MASTER THESIS

“Standardized Security Assessment Framework for ICS Devices and pilot project”

University of Twente

Faculty of Electrical Engineering, Mathematics and Computer Science

Author: Anna Prudnikova (1924818)

Supervisor (University of Twente): Dr. Jeroen Van der Ham

Supervisor (Secura B.V.): Razvan Venter

August 2019

Title page

Student name: Anna Prudnikova

Student number: 1924818

Telephone: +79166907159

E-mail: a.prudnikova@student.utwente.com

Topic of Master Thesis: Standardized Security Assessment Framework for ICS Devices and pilot project

Company: Secura B.V.

Company address: Karspeldreef 8, 1101 CJ Amsterdam, The Netherlands

Acknowledgment

During six months of the research and writing my Master Thesis I received support and help from a lot of different people. I would like to thank everyone involved and give specific acknowledgment to the following people.

First of all, I would like to thank my supervisor Dr. Jeroen van der Ham, who supported me during the whole process of writing my Master Thesis, provided a valuable feedback and recommended me a company which can provide me with an internship position and support me with conducting the research. The company Secura B.V. happened to be a perfect match.

I would also like to thank the company Secura B.V., where I was working on my thesis for six months, especially for providing resources and devices for performing pilot part of my project. My special gratitude goes to my supervisor within the company Razvan Venter who gave me guidance in creating the framework and helped me to outline structure and timeline of my thesis. Moreover, I would like to thank Jos Wetzel, who supported me in technical questions of programming and testing devices during evaluation process.

Moreover, I would also like to show gratitude to my family and friends who supported me from the very beginning of my master studies, believed in my success and were there for me when I needed moral support.

Abstract

The modern world becomes more and more digitalized. The information technologies (IT) keep penetrating all spheres of our life. This major trend of digitalization also changed the industrial sector; Industrial Control Systems (ICS) become more interconnected and the boundaries between classic IT systems and ICS become less clear. IT protocols such as IP or TCP tend to be used within ICS due to their simplicity and widespread. This trend leads to the fact that ICS that originally were not designed to be secure against state of the art cyber-attacks become vulnerable.

One of the main problem within the cyber security domain of ICS is the lack of regulation. Manufactures do not have obligations to make their devices secure. Currently there exist a number of different best practice documents in the domain, but presented requirements overlap or sometimes even contradict each other, which complicates their efficient application. None of the existing documents could be used to perform an in-depth analysis of ICS devices security. To address this problem we created Standardized Security Assessment Framework for ICS Devices, which could be used by all actors involved in industrial processes: industrial companies, certification laboratories and IT integrators or manufacturers of ICS devices to assess and eventually strengthen the cyber security level of ICS devices.

The created framework is based on five different documents related to ICS cyber security that were chosen as the most relevant ones based on specific parameters. From those five documents, we identified more than two hundred requirements (227), performed an overlapping process to identify relevant requirements for ICS devices and eventually presented one hundred forty (140) requirements.

To finalize the created framework, we performed an evaluation process (or so-called pilot project) by testing three different devices, in order to assess compliance with all included requirements. This process allowed to further improve the Framework and revealed that twenty-three of original requirements were either not relevant for single devices (only relevant on system level) and therefore were deleted or partly/completely repeated other requirements and in this case – merged. Thus, the final version of the Framework contains one hundred seventeen requirements (117). Additionally, for every requirement from the Framework we created excessive guidance with description of methods and tools needed to perform the assessing process of compliance.

Moreover, we presented recommendations on how to strengthen security of tested devices on different levels: device-based, system-based and process related. We included in the recommendations the list of possible security solutions that could be used together with the device to reach the compliance with the created framework; based on an example of one device we introduced compensation measures for every requirement that was not fulfilled within this device.

Table of Contents

1. Introduction / Motivation of the topic

1.1. Introduction to ICS

Industrial Control System (ICS) is a general term used to describe different types of control systems that are used for industrial process control. ICS term includes different devices, systems and networks. ICS are normally used in a number of industries such as water, electrical, oil and gas, transportation, chemical, automotive, food and many more [1].

There exist several types of possible ICS systems, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) or Safety Instrumented Systems. Additionally, major parts of ICS are specific devices, such as Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), specific industrial network devices. A PLC is one of the most sophisticated type of ICS devices and is a form of industrial computer that is designed to function in harsh industrial conditions. A PLC is typically used to directly control industrial processes. Moreover, a PLC could be also used in civil applications, such as controlling traffic lights.

The difference between different types of ICS is presented in the Figure 1. Difference between ICS/SCADA/DCS/PLC.

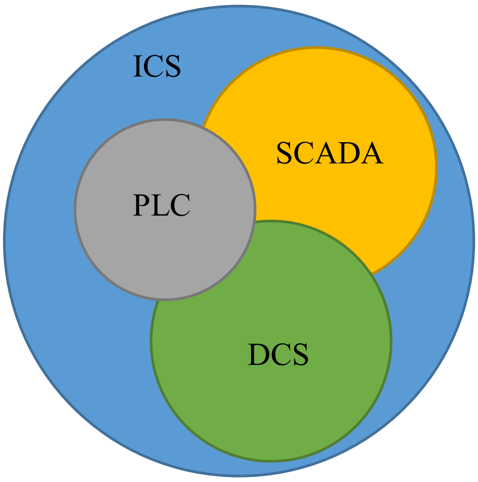

Figure 1. Difference between ICS/SCADA/DCS/PLC.

Industrial control systems in modern understanding have been around since 1950 [2]. The first PLC was developed in USA in 1968. New technologies keep emerging, such as the Internet of Things (IoT), cloud computing or connected cars. This major trend of digitalization can also be referred to as Industry 4.0 or the 4th industrial revolution. Overall, Industry 4.0 refers to manufactory automation ("smart factories"), describes the way we produce goods, and characterizes the industrial sector nowadays. Thus, industrial control systems have also faced major changes in their design – turning into cyber-physical systems instead of simply physical. ICS become more interconnected and the boundaries between classic IT systems and ICS become less clear. IT protocols such as IP, TCP tend to be used within ICS due to their simplicity and widespread.

Historically, there was a separation between Operational Technologies (OT), which could be roughly explained as hardware and software that is used for controlling physical embedded devices, and IT. Therefore, ICS were considered to be "air-gapped" from classical IT and the

Internet and thus were considered to be secure from possible security attacks. Unfortunately, recent cyber security incidents within ICS domain proved this theory to be wrong [3, 4].

1.2. Problem statement

With this rise of IT field, questions of cyber security keep getting more priority. In the recent years, the severity and frequency of cyber-attacks is increasing. All of those trends lead to the fact that ICS, that originally were not designed to be secure against state of the art cyber-attacks and are supposed to be used in place for 10-20 years, become vulnerable. The number of reported incidents in the sphere of ICS rises, the most severe example being the malware Stuxnet [3]. Stuxnet was specifically designed to target PLC and caused major damage to Iran's nuclear program in 2010. This was the first major incident to cause disturbances of ICS. As an example of recent malware specific to ICS, we could refer to TRITON [4]. TRITON was targeting Safety Instrumented Systems (SIS) causing them to falsely enter safe mode and thus shutting down the whole industrial process.

Recent studies [4, 6] show an overall increase of awareness of industrial companies regarding cyber security issues and their preparedness to take actions to prevail them. Unfortunately, the maturity of ICS cybersecurity still remains low, but trending to increase steadily. The experts in [3] claim that "managing risks and compliance is the key" to cybersecurity in the industrial environment. At the same time, the level of compliance to guidance and regulations in the sphere of ICS is relatively low. It could be explained by the fact that currently there exist multiple guidelines, recommendations and standards that often overlap or even contradict each other in their requirements. Thus, there is a clear need of a unified framework that could be used by industrial companies to build their security upon and to be able to test it. Creating such a framework is the goal of this research. By all means, compliance to cyber security guidelines does not always mean high level of cyber security but it could be considered as a first major step, especially for the companies that do not have required expertise in security.

Meanwhile, there is another part of the problem – the lack of mandatory cyber security certification schemes that allows vendors of ICS equipment to keep producing insecure devices. Majority of manufacturers are unaware of any existing standards or recommendations in the domain of ICS cyber security.

To overcome these issues there exists a need of creating a single unified framework for assessing cyber security of ICS that would combine all relevant requirements and provide guidelines on how to assess them. Moreover, this framework should be highly advertised and accepted on a European or even international level. As a starting point for the Master Thesis, it was decided to focus on the security assessment of ICS devices and possible certification schemes. The final name of created framework is "Standardized Security Assessment Framework for ICS Devices" (hereinafter referred to as the Framework or created framework).

1.3. Research questions

Taking into consideration the problem stated in section 1.2, we are going to formulate two main research question as followed:

1. What standards for ICS cyber security could be considered the most relevant and how to merge all requirements from chosen standards into a single framework for assessing the cyber security of ICS devices?

2. How the requirements presented in the created framework could be tested to assess the cyber security for ICS devices?

To be able to answer the main research questions we need to answer a number of subquestions:

1. What are the most relevant standards for ICS cyber security based on country/zone of influence, organization-developer, scope, requirements elaboration?
2. How could the requirements from selected standards be merged together to create a single framework for assessing the cyber security of ICS devices?
3. What types of security levels could be introduced within the framework for the purpose of a certification scheme?
4. How to test all the requirements introduced within the framework?
5. What tools should be used for testing?
6. Is it technically feasible to test all the requirements introduced within the framework?
7. In which way can the framework be used for testing and certification?

1.4. Relevance

1.4.1. Academic relevance

With the rise of awareness in the field of ICS cyber security, more and more new guidelines (recommendation, standards, checklists) keep emerging in different countries. Even though those documents have slightly different focus, they all aim at the same goal – increase maturity of cyber security for industry. The problem here is that not all of those documents work well together, because there is no solid basis to which they can refer and be further adapted to specific needs. Moreover, they all are presented in different formats: recommendations, guidelines, standards. This leads to complication when it comes to choosing which source to implement and to follow. The value of the current research for academic purposes is that we are providing this basis based on already existing standards that proved their value and are currently being used in ICS industry. The ultimate goal is to be able to create a single framework that could be used by different countries and be adapted for their use cases. Current research is a first step towards reaching this goal. By analysing and performing the overlap of more than two hundred requirements from five different documents (guidelines, recommendations, standards) we simplified the future work for academic field and allowed to avoid duplication of work. Additionally, we tried to make all requirements less ambiguous and add more detailed explanation to avoid possible misinterpretations.

1.4.2. Industry relevance

Even though current research is highly relevant for the academic field, it is even more relevant for practical implementation within ICS industry. For industries, the main added advantage of our research is the description of methods and tools that are required to assess compliance. For every requirement, we introduced explanation on how this requirement should be tested, what information could be found in documentation and what possible tools (software of hardware) could be required to perform the technical assessment.

The additional value that framework brings is an opportunity to improve current certification schemes for ICS. Since the certification of ICS is a relatively new topic, most of certification laboratories have not yet reached a high maturity level. The main problem they face is how to correctly interpret requirements and most importantly how to actually test them: should the focus be on documentation review or actual technical testing. That is where the framework comes in hand. It explains what types of tests should be sufficient to assess the compliance of each requirement and how to proceed with the assessment process. Currently Secura B.V. is actively involved in improving the assessment methodology, together with certification bodies.

Moreover, combining of five most complete guidelines allows to address cyber security for ICS devices from all perspectives. The framework has a highly practical approach which has not been introduced before. It is especially relevant to industrial companies that use ICS devices to control industrial processes but are not used to consider cyber security when it comes to introducing new devices within their systems. Following the guidelines presented in the Framework they can assess the security level of ICS devices they currently use without support from IT integrators which will allow to cut financial expenses for those companies. For manufacturers of ICS devices following the created framework during testing process would allow to strengthen overall security of their devices, since it will allow them to identify all possible weak features and identify how they can be improved.

To summarize, the created framework could be used by:

- Testing laboratories and certification bodies for cyber security to provide extensive assessment for the tested devices;
- Industrial companies to assess if certain devices should be introduced within their systems and which risks it could bring;
- Manufacturers (vendors) creating ICS devices to assess their security;

1.5. Structure of the thesis

In chapter two we are going to introduce the literature overview. It contains three main parts: general background on ICS security, discussion about different standards related to ICS security and identification of possible existing certification schemes.

Chapter three provides a description for research methodology and steps that were taken in order to answer stated research questions and all related subquestions.

In chapter four we provide research results, including information regarding choosing of relevant requirements and overlapping them and the final version of Standardized Security Assessment Framework for ICS Devices.

Chapter five reports on evaluation process (pilot project) including results of testing of three different ICS devices in accordance with created framework. Additionally in this chapter we provide comparison of testing results.

In chapter six we discuss the obtained results and provid recommendation for securing the tested ICS devices based on the assessment, by implementing it in cooperation with certain security systems. Moreover, we reflect on limitations that we faced during the research project.

Finally, chapter seven concludes the research project and provides additional outline for possible future work.

2. Literature review

2.1. Brief overview on ICS security

Until recently, ICS were considered secure due to their isolation from internet and classical IT infrastructure, which is why they were not build to be secure and resilient against potential cyber security attacks. Introduction of open standards such as Ethernet, TCP/IP and web-technologies within operation technology to increase connectivity opened the door for attackers to exploit vulnerable systems.

First major researches in the field of ICS security started to emerge in the beginning of 2000th and gained the focus of research society after the incident with Stuxnet [3] together with the first attempts to introduce guidelines. The main topics of research were different: starting from analysing myths and actual facts behind ICS cyber security in [7] and finishing at outlining main challenges that ICS face [8].

The main conclusion that could be derived from the publications is that the ICS field is currently in a transition from being completely closed and isolated, to interconnectivity and that it will take some time for industries to be able to keep up with rising cyber security challenges. The key of doing so is by raising awareness, that cyber threats are real and they need to be addressed.

For our research we are going to focus on identifying and analyzing the most relevant standards for ICS cyber security that support the process of raising awareness and securing ICS.

2.2. ICS security standards

As was mentioned in Part 1 of this document, currently there exist a number of different guidelines, recommendations and regulations in the area of ICS cyber security. The short description of these documents could be found in Table 1. List of all possible standards / guidelines / recommendations for ICS cybersecurity. Further, you can find brief analysis for all eight regulatory documents:

1. IEC62443 series. Industrial communication networks – Network and system security [9].
2. NIST SP800-82. Guide to ICS security [10].
3. NERC-CIP. Version 5 CIP Cyber Security Standards [11].
4. NIST Framework for Improving Critical Infrastructure Cybersecurity [12]
5. UL2900-2-2. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular requirements for ICS [13].
6. ENISA. Indispensable baseline security requirements for the procurement of secure ICT products and services [14].
7. NCSC. Checklist security of ICS/SCADA systems [15].
8. MSB. Guide to increased security in industrial information and control systems [16].

2.2.1. IEC62443 Series

IEC 62443 [9] is a series of standards created by the International Electrotechnical Commission (IEC), the international standards and conformity assessment body for all fields of electro-technology.

This series of standards was originally developed by ISA99 committee, part of the International Society of Automation and later adopted by IEC. The series of Standards consists of fourteen different standards, together providing a flexible framework to secure industrial and automation control systems (IACS). The main security requirements for IACS products are introduced in two of these standards:

1. IEC 62443-4-2, Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components.
2. IEC 62443-3-3, System Security Requirements and Security Level.

For the purpose of creating the Framework we focused on requirements from IEC 62443-4-2 and IEC 62443-3-3. Overall, both standards contain seven categories of basic requirements, defined as Functional Requirements (FR). Requirements include both technical and procedural/process aspects related to the product in scope.

Moreover, the series of standards introduces the concept of security levels (SL). The standards define four security levels for IACS products and systems, which would test the increasing level of security features used to protect against penetration within the system/component. Additionally, they introduce three different types of security levels: target SL, achieved SL and capabilities SL.

2.2.2. NIST SP800-82

NIST SP800-82 [10] is a special publication (SP) "Guide to Industrial Control Systems Security" developed by National Institute of Standards and Technology (NIST) which is responsible for creating guidelines for all spheres of technology from the electronic health records to smart electric power grid for USA.

The publication is based on another publication by NIST "IT Security for Industrial Control Systems" (NISTIR6859), currently withdrawn. NIST SP800-82 outlines guidelines for securing ICS including all possible types such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC). The publication provides information about ICS and their typical topologies, points to specific ICS vulnerabilities and threats and gives recommendations on how to secure ICS.

NIST SP800-82 specifies eighteen control families for possible security measures in correlation with NIST SP800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" [17]. The standard contains both technical and organizational related requirements.

2.2.3. NERC-CIP

NERC-CIP [11] is a series of standards for Critical Infrastructure Protection (CIP) developed by the North-American Reliability Corporation (NERC), which is a non-profit international regulatory authority responsible for developing and enforcing Reliability Standards to secure power grids in the United States, Canada and north Mexico.

NECR-CIP currently consists of eleven different standards that contain recommendations for bulk power systems; nine of those Standards include requirements both process related and technical. Additionally, it outlines physical security requirements. Overall, the series specify more than forty rules and almost one hundred sub-requirements.

Moreover, NERC-CIP introduces the Cyber System Categorization standard, which outlines the basics on how to classify bulk electric systems (BES) to further identify relevant requirements.

2.2.4. NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework for Improving Critical Infrastructure Cybersecurity [12] is a publication created by NIST in 2018.

It describes a recommendatory risk management framework for critical infrastructure of USA to support management of cyber security risks for all involved parties. It outlines the basic guidelines to identify and manage risks and gives recommendation on how those guidelines could be adapted by any organization based on their used technologies. Additionally, it gives references to different widely accepted standards and guidelines for supported technologies.

With support of this framework organizations can:

- outline their current cyber security state;
- specify their target cyber security state;
- identify the processes to continuously improve their state of cyber security;
- assess the progress in reaching the target state;
- raise awareness of different stakeholders about possible cyber security risks.

The document is purely process-related and does not provide any technical recommendations on securing ICS.

2.2.5. UL2900-2-2

UL2900-2-2 [13] is a standard that outlines requirements for Industrial Control Systems developed by a global certification company Underwriters Laboratories (UL).

The goal of the standard is to be able to test and validate ICS. It addresses testing criteria for assessing cyber security of software components of ICS. It contains four main categories of requirements: risk controls, risk management, vulnerabilities and exploits, software weakness analysis with overall more than forty requirements presented.

UL2900-2-2 should be considered together with another standard developed by UL – 2900-1-1 [18] that specifies general requirements for network-connectable devices to receive extra guidance for certain requirements.

2.2.6. ENISA

ENISA “Indispensable baseline security requirements for the procurement of secure ICT products and services” [14] is a paper developed by European Union Agency for Network and Information Security, which is a center of expertise for cyber security in Europe with main focus on network and information security.

The paper outlines basic minimum security requirements for procurement of information and communications technology (ICT) products. The main goal of this paper is to help companies avoid possible “lock-in” to specific vendors of software and hardware and providers of services.

The ENISA paper is based upon best practices and commonly used standards in the field of cyber security chosen by experts. It does not substitute other certification schemes or commonly known standards, instead it should be used as an addition to them. It specifies ten main categories of the requirements with almost forty requirements included. Most of these requirements are process related.

2.2.7. NCSC. Checklist security of ICS/SCADA systems

Checklist security of ICS/SCADA systems [15] was developed by National Cyber Security Center (NCSC) of Ministry of Security and Justice of the Netherlands. NCSC is the central information hub and main center of expertise in the field of cyber security in the Netherlands.

The Checklist was published in 2016 and outlines both organizational and technical measures to ensure cyber security of ICS domain.

It outlines seven main organizational measures, ten technical and operational measures and give brief explanation and references to all of them. The presented measures are introduced on a high level and do not explain how those measures should be tested or implemented.

2.2.8. MSB. Guide to increased security in industrial information and control systems

Guide to increased security in industrial information and control systems was created by Swedish Civil Contingency Agency (MSB). MSB is responsible for preparing society for major accidents and crises, the Director of the Agency is appointed by the Swedish government.

The guide provides seventeen basic recommendations for increasing security of ICS. The provided recommendations are high level and contain both process related and technical recommendations. For each recommendation, the reference to another regulatory document is provided together with some examples and description of possible problems.

The main focus of this guide is to raise awareness about ICS security and provide explanation on why is it important to all actors involved in industrial processes.

2.3. ICS certification schemes

During the research, we additionally studied possible certification schemes for ICS. All certification schemes are based on IEC62443 series of standards, as the only worldwide-recognized ICS cyber security standard. Currently there exist two world recognized certification schemes for ICS:

- ISASecure™ certifications;
- IECEE certifications.

Moreover, there exist independent certification schemes, such as a scheme offered by TÜV SÜD.

The brief overview of existing certification schemes is introduced below.

2.3.1. ISASecure

ISASecure™ is a conformance certification program for independent certification of industrial automation and control products and systems. It is managed by ISCI – non-profit automation controls industry consortium.

ISASecure offers three certification schemes with four security assurance levels based on IEC62443 series of standards:

- ISASecure Embedded Device Security Assurance (EDSA) Certification based on IEC62443-4-2);
- ISASecure System Security Assurance (SSA) Certification (based on IEC62443-3-3);
- ISASecure Security Development Lifecycle Assurance (SDLA) Certification (based on IEC62443-4-1).

ISASecure offers certification for off-the-shelf ICS systems, ICS devices and product development security lifecycle.

Currently there exist three accredited ISASecure Certification bodies from different countries. ISASecure certified thirty five ICS devices and systems. The first certificate was issued in 2017.

2.3.2. IECEE

IECEE is International Electrotechnical Comission (IEC) System of Conformity Assessment Schemes for Electrotechnical Equipment and Components based on IEC International Standards.

IECEE offers five certification schemes according to IEC62443 series of standards:

- IEC 62443-2-4. Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers;
- IEC 62443-2-4/AMD1. Amendment 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers;
- IEC 62443-3-3. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.
- IEC 62443-4-1. Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements ;
- IEC62443-4-2. Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.

The first certification scheme was included in IECEE System in 2017 for IEC 62443-2-4. In total, there are thirty five certification bodies included in the scheme.

2.3.3. TÜV SÜD

TÜV SÜD is a technical service corporation based in Germany and working in the fields of industry, mobility and certification.

The company offers certification for product manufacturers, system integrators and control system operators for three standards of the IEC62443 series:

- IEC 62443-3-3. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.
- IEC 62443-4-1. Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements ;
- IEC62443-4-2. Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.

TÜV SÜD is accredited according to IEC 62443 by the German Accreditation Body (DAkkS).

Table 1. List of all possible standards / guidelines / recommendations for ICS cybersecurity

#	Originating country/ zone	Organization	Name	Field	Description	Number of requirements
1	Worldwide	IEC	**IEC 62443 Series.** Industrial communication networks – Network and system security.	ICS (IACS)	A series of standards, 2 types of main requirements: 3-3. System security requirements; 4-2. Technical security requirements for IACS components.	3-3. System security requirements. Total: 7 categories, 57 requirements + requirement enhancements. 4-2. Technical security requirements for IACS components. Total: 7 categories, 61 requirements + requirement enhancements.
2	USA	NIST	**SP 800-82.** Guide to ICS security.	ICS	Requirements are referenced to a main Standard SP 800-53 with a table of overlays presented. It was created for cyber security of information systems used in the federal government. Often used in non-governmental organizations as a good practice standard.	18 control families. Total: 177 requirements
3	USA	NERC	**NERC-CIP** Critical infrastructure protection. Cyber Security Standards.	Critical Infrastructure (electric sector)	A series of standards. Mandatory for power system operators in USA, Canada and North part of Mexico. Referenced at IEC 62443, that they should work together. The major requirements could be found in Security Management control CIP-003-5. For each category there exists the specific standard with clarification.	9 standards with different requirements. Total: 94 requirements.
4	USA	NIST	**Framework** for Improving Critical Infrastructure Cybersecurity.	Critical Infrastructure	A risk-based approach to managing cybersecurity risk, composed of three parts: Core, Implementation Tiers, Profiles. Each component reinforces the connection between business mission and cybersecurity activities.	5 main categories. Total: 108 requirements
5	Company specific	UL	**2900-2-2.** Outline of Investigation for Software Cybersecurity for Network-Connectable Products,	ICS	The requirements created by a global company UL. Must be used together with global document UL 2900-1. Part 1: General requirements.	4 major categories. Total: 46 requirements

			Part 2-2: Particular requirements for ICS.			
6	EU	ENISA	**Indispensable baseline security requirements** for the procurement of secure ICT products and services.	General ICT	Generic requirements for the procurement of ICT products and services	10 categories. Total: 39 requirements.
7	NL	NCSC (National Cyber Security Center)	**Checklist security** of ICS/SCADA systems.	ICS	Organizational and technical measures that are considered as good practice. Not detailed, high level requirements.	7 organizational measures, 10 technical measures. Total: 17 requirements.
8	Sweden	Swedish Civil Contingency Agency (MSB)	**Guide to increased security** in industrial information and control systems.	ICS	17 general recommendations with references for each and one of them to the standard they are derived from, more like a summary. For each recommendation there are given objectives, that are actual actions to be taken.	17 major recommendations. Total: 17 requirements.

3. Research methodology

3.1. Conceptual model

Considering the nature of formulated research questions, we used Design Science (DS) research methodology to tackle them. This is a research methodology that was specifically designed to perform researches in the area of information technology. For our research we used methodology proposed in [19], the definition they use is as follows:

> *"Design science…creates and evaluates IT artifacts intended to solve identified organizational problems".*

There are six main activities identified in [19]:

1. Problem identification and motivation.
2. Defining the objectives for a solution.
3. Design and development.
4. Demonstration.
5. Evaluation.
6. Communication.

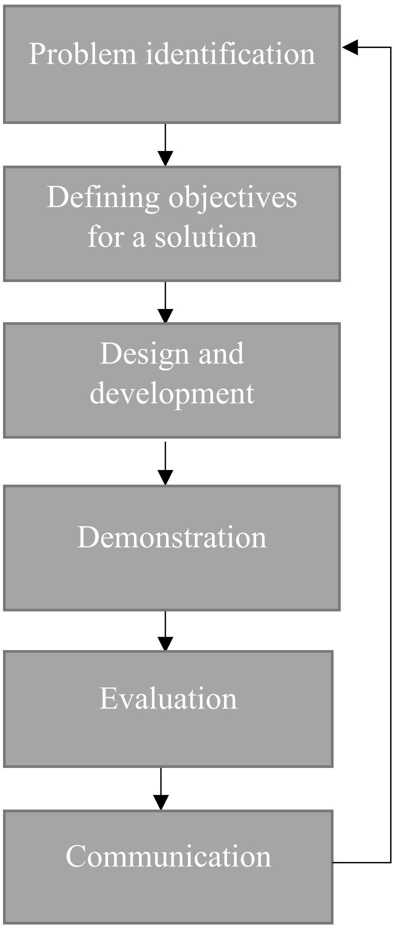

Figure 2. Design Science research methodology

The methodology could be used as a cycle (Figure 2. Design Science research methodology) with iterations that help shaping the final solution and could possibly lead to changing of an original identified problem and objections for the solution.

To adapt the proposed methodology for the identified research questions we performed six following steps presented in Table 2. Correlation between research steps and results presented in the Thesis.

Table 2. Correlation between research steps and results presented in the Thesis

#	Step	Part of the Thesis
1	Problem identification and motivation	1
2	Defining the objectives for creating a framework	1
3	Framework development	2, 4
4	Defining methods/tools for testing process	4
5	Testing process	4
6	Reporting results	5, 6

3.1.1. Correlation of research questions with DS research methodology

The exact research methods of research methodology DS used to answer research questions are presented in Table 3. Correlation of research questions with DS research methodology.

Table 3. Correlation of research questions with DS research methodology

#	Research question	Step of DS research methodology
Main research questions		
1	*What standards for ICS cyber security could be considered most relevant and how to merge all introduced requirements in chosen standards into a single framework for assessing cyber security of ICS devices?*	1-3
2	*How requirements presented in the created framework could be tested to assess cyber security for ICS devices?*	4-5
Sub-questions		
1	*What are the most relevant standards for ICS cyber security based on country/zone of influence, organization-developer, scope, requirements elaboration?*	2-3
2	*How could be requirements from selected standards be merged together to create a single framework for assessing cyber security of ICS devices?*	3
3	*What types of security levels could be introduced within a framework for certification scheme?*	3
4	*How to test all the requirements introduced within the framework?*	4
5	*What tools should be used for testing?*	4
6	*Is it technically feasible to test all the requirements introduced within the framework?*	5
7	*In which way can the framework be used for testing and certification?*	6

4. Research results

4.1. Selection of ICS security standards and relevant requirements

As was discussed in Chapter 3 of the Master Thesis eight different guidelines (standards, recommendations, checklists etc.) regarding ICS security were analyzed. The performed analysis revealed that not all of the selected standards are relevant to the main goal of the Master Thesis. Therefore, we further analyzed the standards and compared them based on a number of parameters. The important parameters for comparison are:

- type of the document (standards, guidelines, recommendations etc.);
- status (mandatory, recommendatory);
- zone of influence (worldwide, USA, Europe);
- type of included requirements (technical, administrative);
- scope (system-related, device-related).

For our Framework we selected the documents that fit at least three of five following criteria:

- type: standard or guidelines;
- status: mandatory;
- zone of influence: worldwide or Europe;
- type of requirements: technical;
- scope: devices-related.

The result of analysis is Presented in Table 4. Comparison analysis of ICS regulatory documents. Underlined are the parameters that follow previously described criteria.

Table 4. Comparison analysis of ICS regulatory documents.

Name of the document	Type of the document	Status	Zone of influence	Type of requirements	Scope
IEC 62443 Series	Standard	Recommendatory	Worldwide	Technical	System-related Device-related
NIST SP 800-82	Guidelines	Recommendatory	USA	Technical Administrative	System-related Device-related
NERC-CIP	Standard	Mandatory	USA, Canada, North Mexico	Technical Administrative	System-related
UL 2900-2-2	Guidelines	Recommendatory	Worldwide	Technical Administrative	Device-related
ENISA Indispensable baseline security requirements for the procurement of secure ICT products and services	Guidelines	Recommendatory	Europe	Technical Administrative	System-related Device-related
NCSC Checklist security of	Guidelines	Recommendatory	NL	Technical Administrative	System-related

ICS/SCADA systems					
Guide to increased security in industrial information and control systems	Guidelines	Recommendatory	Sweden	Administrative	System-related
NIST Framework for Improving Critical Infrastructure Cybersecurity	Framework	Recommendatory	USA	Administrative	System-related

Therefore, this leads us to five final documents that were used to create the Framework:

1. IEC62443 series. Industrial communication networks – Network and system security [9].
2. NIST SP800-82. Guide to ICS security [10].
3. NERC-CIP. Version 5 CIP Cyber Security Standards [11].
4. UL2900-2-2. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular requirements for ICS [12].
5. ENISA. Indispensable baseline security requirements for the procurement of secure ICT products and services [13].

4.2. Design of Standardized Security Assessment Framework

To simplify navigation in the created framework it was decided to create it in the format of an Excel file. To fully represent all collected information during the analysis of related regulatory documents the Framework contains following parts (each represented in a form of separate sheet):

- **Document info.** Basic information about the Framework.
- **Relevant standards.** Description of chosen as relevant standards in part 4.1 of this Thesis.
- **All requirements.** All possible requirements taken from five chosen standards.
- **All requirements (commented).** All possible requirements with extra comments on how they were integrated further.
- **Merged requirements.** The final requirements of the Framework after overlapping process with a comment field to trace the original requirement.
- **Security levels (SL).** Dedicated Security Level (SL) for each of final requirements.
- **Methods/tools.** Description of methods and tools that are used for testing of the final requirements.
- **IEC62443-3-3 checklist.** Correlation between final requirements of the Framework and IEC62443-3-3.
- **Appendix 1.** Requirements for Secure Mechanisms for Storing Sensitive Data and Personally Identifiable data.
- **Appendix 2.** Requirements for Security Functions.

More detailed description of main parts of the Framework is presented in Parts 4.3-4.5 of the Master Thesis.

4.3. Requirements overlapping

As a first step to overlap requirements into a single framework we extracted all possible requirements from five chosen in Part 4.1 standards and included them into a single table. Overall, there were identified sixteen different categories for requirements and in total two hundred twenty seven requirements.

Next, we identified the major document that was going to be used as a basis[1] for our Framework. The only analysed document that has a status of a standard and thus could be considered as a priority to all the rest of the chosen documents is IEC62443-4-2.

As a further step, we analysed all extracted requirements to create a limited number of categories. Based on the selected standard we identified seven possible groups of which all the requirements could be part of (five of those groups completely correlate with the fundamental requirements from IEC62443-4-2). Those groups are as follows:

1. Identification and Authentication control (IAC).
2. Use control (UC).
3. Audit and accountability (AU).
4. System integrity and authenticity (SIA).
5. Data confidentiality (DC).
6. System and communication protection (SCP).
7. Security by design (SD).

Next step was to assign categories for all extracted requirements. First, we started with requirements from IEC62443-4-2 since it was chosen as a basis. After we put all requirements from IEC62443-4-2 into dedicated categories, we started with dividing all the rest of requirements into the same categories. As a result, we received the same amount of requirements but split into seven categories.

Finally, since a lot of requirements overlap each other we performed an integration procedure. Requirements from IEC62443-4-2 were taken as basic requirements. Additionally, some of the requirements have so-called “Requirement Enhancements” that could be used to strengthen the security. Rest of the requirements were processed in three different ways:

- fully overlapping requirements – merged with basic requirements;
- partly overlapping – added as extra part for basic requirement;
- not overlapping – taken as new basic requirements.

Eventually this led us to one hundred seventeen requirements (one hundred thirsty six with enhancements) divided into seven categories. The process of overlapping could be traced back

[1] By basis we mean that all requirements from the chosen document will be considered as main ones, requirements from other documents will be merged with them or added as additional

by following the information from "comment" part in the excel file of the Framework (sheet "Merged requirements").

The whole process of overlapping of the requirements could be presented in a form of simplified logic diagram (Figure 3. Simplified logic diagram for overlapping process of requirements).

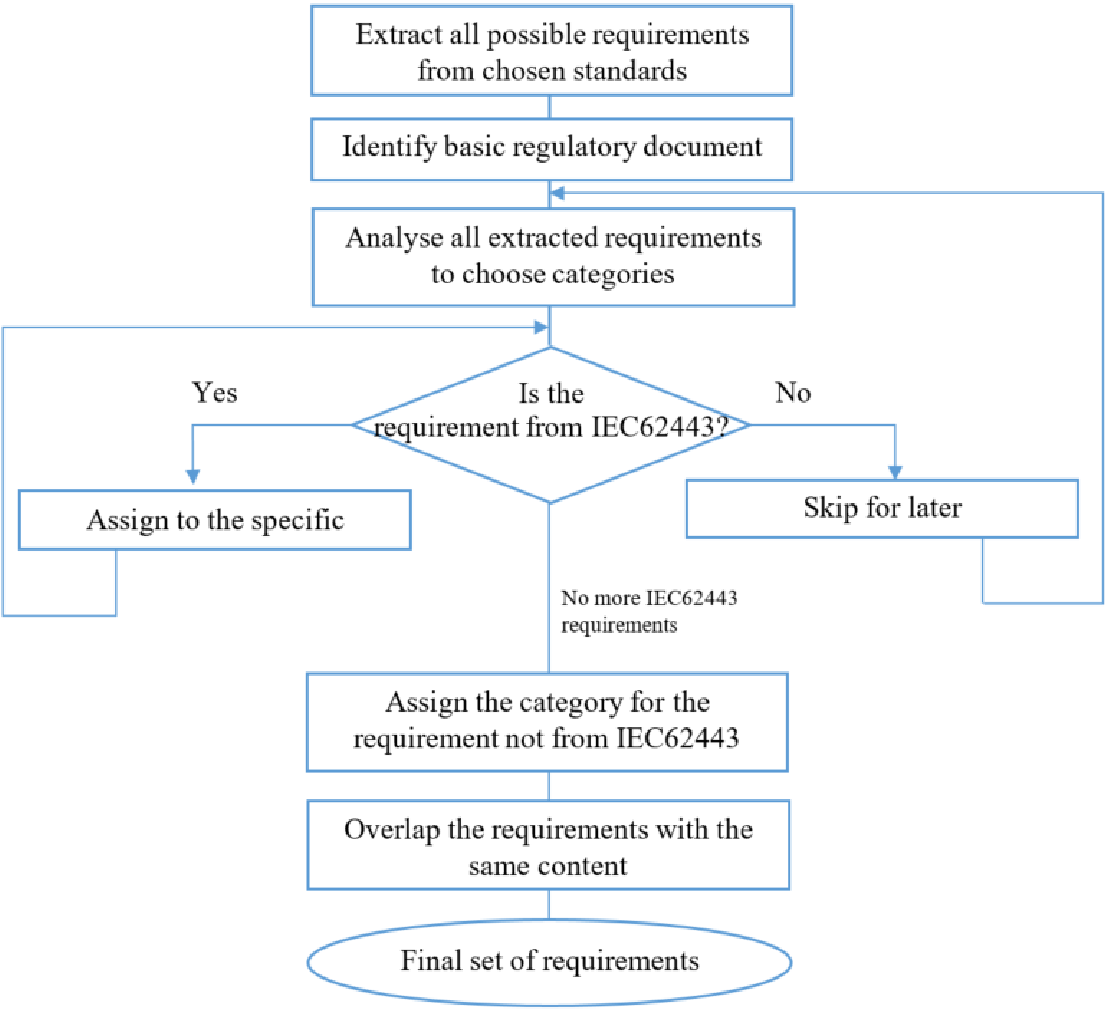
Extract all possible requirements from chosen standards
Identify basic regulatory document
Analyse all extracted requirements to choose categories
Yes
Is the requirement from IEC62443?
No
Assign to the specific
Skip for later
No more IEC62443 requirements
Assign the category for the requirement not from IEC62443
Overlap the requirements with the same content
Final set of requirements

Figure 3. Simplified logic diagram for overlapping process of requirements

4.4. Concept of security levels

Another important part of the Framework is the concept of Security Level (SL). The basic idea of SL was taken from series of standards IEC62443 [9]. The series of standards introduce three different types of SL:

- **Target SL (SL-T).** Represents the necessary level of security that needs to be achieved for a particular IACS or a certain zone. Normally is chosen by industrial company by means of performing risk assessment.
- **Achieved SL (SL-A).** Represents actual level of security for a particular IACS or a component. Could be measured after the system is implemented or in the state of final project. Could be done by industrial company or by system provider. Used to establish whether the goal for target SL was met.

- **Capabilities SL (SL-C).** Represents a maximum possible SL that could be achieved if the component / system is properly configured. Could be done by industrial company or by system provider.

Four possible levels are introduced [9]:

- **SL 1.** Protection against casual or coincidental violation.
- **SL 2.** Protection against intentional violating using simple means with low resources, generic skills and low motivation.
- **SL 3.** Protection against intentional violating using sophisticated means with moderate resources, system specific skills and moderate motivation.
- **SL 4.** Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

The goal of this work is to enable the process of assessing and certifying ICS devices. Usually, any certification process states the level of certification which was achieved; in our case – security level. Thus, for the Framework it was decided to simplify the concept of security levels and leave only one type that could be used for certification purposes. The gradation system of four possible SL stays the same.

For every requirement from the Framework, a correlated SL was assigned. For requirements from IEC62443-4-2 the same level was assigned as used in the standard. Since only this standard introduces the concept of SL, for the rest of the requirements, the SL was chosen based on its content and similarity to requirements from IEC62443-4-2. Most of those requirements are more advanced comparing to requirements from IEC62443-4-2. Taking into consideration that most of the device currently are barely able to meet requirements for SL 1 for more advanced requirements we assigned SL 3 and SL 4 from gradation presented within the Framework.

4.5. Methods and tools used for testing

Additionally to perform the pilot project for the Master Thesis we added to the Framework a separate table with description of methods and tools which shall be used to assess security of ICS devices.

There are three main methods presented:

- reviewing the documentation for the tested device;
- technical verification by testing process;
- analysing the firmware.

Every requirement could be tested either by using one of those methods or a set of methods combined.

For each device, the vendor normally provides extensive documentation that is delivered together with the device or could be accessed via Internet through official vendor web-sites. Additionally, vendor web-sites commonly contain the section with answering users' questions. Analyzing all this documentation and all relevant information found on the Internet is an essential step in assessing security of a device.

Additionally, when possible all information found in the documentation should be verified by actual technical testing. Moreover, often the documentation does not contain all needed information, thus technical testing is the only way to assess whether requirement is met or not met. To simplify testing process on Step 5 we provided brief description on how to proceed with testing for every requirement.

In cases when no information could be found in documentation or on-line and there is no clear way to test any particular requirement we attempted to analyse the devices' firmware. However, in most cases ICS devices have proprietary firmware installed that requires performing reverse-engineering, which is out of scope of current Master Thesis due to complexity and high time consummation.

Different tools could be used to perform technical testing. Most of the tools are typical for penetration testing, the description of tools used for assessment is presented in Part 5. Of the Master Thesis.

Some of the requirements could be tested without a need for external tools but only require established connection with a tested device with a personal computer (PC). Those requirements are usually assessed to verify that some functions of the device are implemented as described in documentation.

4.6. Final Standardized Security Assessment Framework

The final version of the Standardized Security Assessment Framework for ICS [20] in excel file could be provided upon request.

In the Master Thesis we included the merged requirements of the Framework which are presented in Table 5. Framework[1].

The table has following columns:

- **Category**. The name of one of the seven group for requirements.
- **Requirement name**. The name of the requirement.
- **Description.** The full description and explanation what the requirement mean.
- **Possible enhancements.** Additional measures that should be implemented.
- **Type**. There are three main types of requirements: ICS specific (specifically formulated to be relevant to ICS), General (relevant to IT in general), device specific (depend on type of ICS device: HDR, NDR, EDR). ICS specific and General requirements are relevant to all types of devices; device specific depend on the type of the device.
- **Security level**. The reference to SL (in terms of created framework).

[1] The exact source for every requirement is not include in the Master Thesis, since some of the Standards are not available in open access, so were specifically purchased by Secura B.V. Publishing contains of the Standards are prohibited by confidentiality agreement

Table 5. Framework

#	Category	Requirement name	Description	Possible enhancements	Type	Security level
1.	**1. Identification and Authentication control (IAC)**	IAC 1.1. Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	(1) Unique identification and authentication. Components shall provide the capability to uniquely identify and authenticate all human users. (2) Multifactor authentication for all interfaces. Components shall provide the capability to employ multifactor authentication for all human user access to the component.	ICS specific	1,2,3,4 RE(1) - 2,3,4 RE(2) - 3,4
2.		IAC 1.2. Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices). If the component is running in the context of a human user, in addition, the identification and authentication of the human user according to IAC 1.1. may be part of the component identification and authentication process towards other components.	(1) Unique identification and authentication. Components shall provide the capability to uniquely and securely identify and authenticate itself to any other component.	ICS specific	2,3,4 RE(1) - 3,4
3.		IAC 1.3. Account management	Components shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly (management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts).	-	ICS specific	1,2,3,4 RE1 - 3,4
4.		IAC 1.4. Identifier management	Components shall provide the capability to integrate into a system that supports the management or identifiers and/or provide the capability to support the management of identifiers directly (support the management	-	ICS specific	1,2,3,4

			of identifiers by user, group, role or control system interface).			
5.		IAC 1.5. Authenticator management	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	(1) Hardware security for authenticators. The authenticators on which the component rely shall be protected via hardware mechanisms.	ICS specific	1,2,3,4 RE(1) - 3,4
6.		IAC 1.6 Wireless access management	A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	(1) Unique identification and authentication The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Specific (NDR)	1,2,3,4 RE(1) - 2,3,4
7.			Services that are accessible over a wireless interface shall require user authentication prior to access. Exception: Services that report status, do not provide command and control functionality or general use of the component or do not transmit sensitive data or personally identifiable data AND only output status or historical transaction data, etc., may provide unauthenticated access.	-	General	1,2,3,4
8.		IAC 1.7 Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength based on minimum length and variety of character types.	(1) Password generation and lifetime restrictions for human users. Components shall provide, or integrate into a system that provides, the capability to prevent	ICS specific	1,2,3,4 RE(1) - 3,4 RE(2) - 4

			The password complexity must be configurable by the administrator and be either technically or procedurally enforced with following password parameters: - minimal password length at least of eight characters (or the maximum length supported by the component); - maximum password length; - minimum password that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the component); - minimum and maximum usage period; - prevention of re-use of previous passwords; - maximum number of password changes per time (e.g. per day).	any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices. (2) Password lifetime restrictions for all users. Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.		
9.		IAC 1.8 Password protection	If the component uses a user name-and-password mechanism for authenticating users: a) the component shall use a secure mechanism complying with the requirements in Appendix 1 to store the passwords, they shall not be stored in plaintext; b) authentication error messages provided by the component shall not allow for enumerating valid user names; d) the component shall protect against dictionary attacks and brute force attacks; e) the component shall have no hardcoded passwords that cannot be removed or altered.	-	General	3,4
10.		IAC 1.9 Password	For password-only authentication for interactive user access it shall be possible to change the password at any given moment	-	General	1,2,3,4

		changes enforcement	to enforce the policy of password regular update.			
11.		IAC 1.10 Public key infrastructure certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with commonly accepted best practices or obtain public key certificates from an existing PKI.	-	General	2,3,4
12.			For high availability components, the failure of the certificate authority shall not interrupt essential functions.	-	General	1,2,3,4
13.		IAC 1.11 Strength of public key-based authentication	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same ICS environment to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; f) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	(1) Hardware security for public key-based authentication. The component shall provide the capability to protect the relevant private keys via hardware.	General	2,3,4 RE(1) - 3,4

14.			If the component uses other mechanisms for authentication besides username and password, the mechanism used for authentication shall require as many operations to circumvent as determining the actual mechanism.	-	General	3,4
15.		IAC 1.12 Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.	-	General	1,2,3,4
16.		IAC 1.13 Unsuccessful login attempts	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; or b) generate alerts after a threshold of unsuccessful authentication attempts ; c) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.	-	General	1,2,3,4
17.			Accounts used for essential functions shall not be locked out, even temporarily.	-	General	1,2,3,4
18.		IAC 1.14 System use notification	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	-	General	1,2,3,4
19.		IAC 1.15 Access via untrusted networks (remote interface)	Components that are accessible over a remote interface shall require user authentication prior to access. Exception: Services that report status, do not provide command and control functionality or general use of the	-	Specific (NDR)	1,2,3,4

			component or do not transmit sensitive data or personally identifiable data AND only output status or historical transaction data, etc., may provide unauthenticated access but will need to be documented			
20.			The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.	(1) Explicit access request approval. The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.	Specific (NDR)	1,2,3,4 RE(1) - 3,4
21.		IAC 1.16 Strength of symmetric key-based authentication	For components that utilize symmetric keys, the component shall provide the capability to: a) establish the mutual trust using the symmetric key; s) store securely the shared secret (the authentication is valid as long as the shared secret remains secret); t) restrict access to the shared secret; u) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	(1) Hardware security for symmetric key-based authentication. The component shall provide the capability to protect the relevant private keys via hardware mechanisms	General	1,2,3,4 RE(1) - 2,3,4
22.	**2. Use control (UC)**	UC 2.1 Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least privilege. Access to data shall only be given after successful authentication and authorization. Without successful authentication and authorization, the system shall not allow any activities.	(1) Authorization enforcement for all users. Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege. (2) Permission mapping to roles. Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all	General	1,2,3,4 RE(1) - 2,3,4 RE(2) - 2,3,4 RE(3) - 3,4 RE(4) - 3,4

				human users. (3) Supervisor override. Components shall support a supervisor manual override for a configurable time or sequence of events. (4) Dual approval. Components shall support dual approval when action can result in serious impact on the industrial process.		
23.			Authorization enforcement shall not prevent the initiation of the Safety Instruction Function (SIF).	-	General	1,2,3,4
24.		UC 2.2 Usage restriction	Service accounts shall not be usable for interactive logon.	-	ICS specific	3,4
25.		UC 2.3 Wireless use control	The component shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.	-	ICS specific	1,2,3,4
26.		UC 2.4 Mobile code	In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy must allow, at a minimum, the following actions for each mobile code technology used on the software application: a) control execution of mobile code; b) define which users (human, software process, or device) are allowed to transfer mobile code to/from the application; c) perform integrity checks on mobile code prior to the code being executed; d) perform authenticity checks to verify the origin of the mobile code prior to the code being executed.	(1) Mobile code integrity check. The application shall provide the capability to verify the integrity of the mobile code before allowing code execution	Specific (SAR)	1,2,3,4 RE(1) - 2,3,4

27.			In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy must allow, at a minimum, the following actions for each mobile code technology used on the embedded device: a) control execution of mobile code; b) define which users (human, software process, or device) are allowed to upload mobile code to the device; c) perform integrity checks on mobile code prior to the code being executed; d) perform authenticity checks to verify the origin of the mobile code prior to the code being executed.	(1) Mobile code integrity check. The embedded device shall provide the capability to verify the integrity of the mobile code before allowing code execution.	Specific (EDR)	1,2,3,4 RE(1) - 2,3,4
28.			In the event that a host device utilizes mobile code technologies, that host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy must allow, at a minimum, the following actions for each mobile code technology used on the host device: a) control execution of mobile code; b) define which users (human, software process, or device) are allowed to transfer mobile code to/from the host device; c) perform integrity checks on mobile code prior to the code being executed; d) perform authenticity checks to verify the origin of the mobile code prior to the code being executed.	(1) Mobile code integrity check. The embedded device shall provide the capability to verify the integrity of the mobile code before allowing code execution.	Specific (HDR)	1,2,3,4 RE(1) - 2,3,4
29.			In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security	(1) Mobile code integrity check. The embedded device shall provide the capability to verify	Specific (NDR)	1,2,3,4 RE(1) - 2,3,4

			policy for the usage of mobile code technologies. The security policy must allow, at a minimum, the following actions for each mobile code technology used on the network device: a) Control execution of mobile code; b) Define which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; c) Perform integrity checks on mobile code prior to the code being executed; d) Perform authenticity checks to verify the origin of the mobile code prior to the code being executed.	the integrity of the mobile code before allowing code execution.		
30.		UC 2.5 Session lock	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability: a) to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation; b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures; and c) to comply with session locks requested by the underlying infrastructure (operating system, control system).	-	ICS specific	1,2,3,4
31.		UC 2.6 Remote session control	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity , manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	-	ICS specific	2,3,4

32.			At no time shall the use of remote access compromise the integrity of the component or change the intended use of the component.	-	ICS specific	2,3,4
33.			If a component allows remote access, the component shall be able to operate continuously, automatically or remotely without causing a safety hazard and the component shall signal its remote operation visibly on the component.	-	ICS specific	2,3,4
34.			If a local action is initiated on the component, it shall take precedence and priority over a remote action that occurs at the same time.	-	ICS specific	2,3,4
35.			If a communication session over a remote interface is lost or terminated, the component shall require renewed authentication prior to allowing access over the remote interface. Stored data from the previous session shall not be used to initiate the new session.	-	General	2,3,4
36.			The component shall be configurable to allow once a user is authenticated and granted remote access to the component, to reject and record any attempt to setup another remote connection using the same user identity.	-	ICS specific	2,3,4
37.			The transmission of the authentication credential to a component via a remote connection covered on this section cannot be in plaintext or easily intercepted and duplicated unless: a) the information by itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information; b) the transmission path is a trusted path,	-	ICS specific	2,3,4

			for example a directly connected physical cable that is not shared by any other system or components.			
38.		UC 2.7 Concurrent session control	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	-	ICS Specific	3,4
39.		UC 2.8 Use of physical diagnostic and test interfaces	All type of devices shall prevent unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG).	(1) Active monitoring. Embedded devices shall provide active monitoring of the diagnostic and test interface(s) and generate a log entry when attempts to access these interface(s) are detected.	ICS Specific	2,3,4 RE(1) - 3,4
40.		UC 2.9 Control over other ports usage	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by organization, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	-	General	1,2,3,4
41.		UC 2.10 Managing the operators status	The component shall allow the ability for an operator to be disabled, deleted, expired or change of permissions when the component is not in a critical operator-dependent state transition with the operator to be disabled, deleted, expired or permission changed.	-	ICS specific	3,4
42.			If the operator is connected and the operator permissions or status changes, the operator shall be disconnected and a record in the audit log shall be made.	-	ICS specific	3,4
43.	**3. Audit and accountability (AU)**	AU 3.1 Auditable events	Components shall provide the capability to generate audit records relevant to security for the following categories: a) access control (as minimum: successful login attempts, failed access and login	-	ICS specific	3,4

			attempts);
			b) request errors;
			c) control system events;
			d) backup and restore event;
			e) configuration changes (e.g. successful and unsuccessful software updates);
			f) audit log events;
			g) detected malware (if applicable).			

44.			The component shall provide the capability to select which auditable events are to be audited by specific parts of the component by administrator.	-	ICS specific	3,4
45.		AU 3.2 Audit storage capacity	Components shall: a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; b) provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.	(1) Warn when audit record storage capacity threshold reached Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.	ICS specific	1,2,3,4 RE(1)-3,4
46.		AU 3.3 Response to audit processing failures	Components shall a) provide the capability to prevent the loss of essential services and functions in the event of an audit processing failure; b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	-	ICS specific	1,2,3,4
47.		AU 3.4 Timestamps	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	(1) Time synchronization Components shall provide the capability to create timestamps that are synchronized with a system wide time source. (2) Protection of time source integrity The time synchronization mechanism shall provide the capability to detect unauthorized	ICS specific	1,2,3,4 RE(1)-2,3,4 RE(2)-3,4

				alteration and cause an audit event upon alteration		
48.			Incorrectly timestamped audit records shall not adversely affect essential functions.	-	ICS specific	1,2,3,4
49.		AU 3.5 Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	(1) Non-repudiation for all users. Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	ICS specific	1,2,3,4 RE(1)-4
50.			Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time.	-	ICS specific	1,2,3,4
51.		AU 3.6 Protection of audit information	The component shall protect audit information and audit tools (if applicable) from unauthorized access, modification, and deletion.	(1) Audit records on write-once media. Components shall provide the capability to store audit records on hardware-enforced write-once media.	ICS specific	2,3,4 RE(1)-4
52.			Unless and until they are transmitted to an external data storage, the component shall store all security-related logs in non-volatile memory and shall not allow non-privileged users to remove or change them.	-	General	1,2,3,4
53.		AU-3.7 Audit reduction and report generation	The component shall provide an audit reduction and report generation capability that: a) supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; b) does not alter the original content or time ordering of audit records.	-	ICS specific	3,4
54.		AU 3.8 Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	(1) Programmatic access to audit logs. Components shall provide programmatic access to audit	ICS specific	1,2,3,4 RE(1)-3,4

				records by either using an application programming interface (API) or sending the audit logs to a centralized system.		
55.		AU 3.9 Continuous monitoring	When a component provides a security mechanism, that component shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breached in a timely manner.	-	ICS specific	2,3,4
56.	**4. System integrity and authenticity (SIA)**	SIA 4.1 Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	(1) Communication authentication. Components shall provide the capability to authenticate information during communication.	ICS specific	1,2,3,4 RE(1)-2,3,4
57.		SIA 4.2. Remote communication integrity and authenticity	The component shall ensure the integrity and authenticity of all data communicated over any remote interface. For this, the component shall use security functions complying with the requirements in Appendix 2 to the Framework.		General	3,4
58.			Remote connection from different sources shall not disturb the proper function of the component and shall not cause any security flaw.		ICS specific	3,4
59.			Messages sent over a remote connection shall be processed as first in - first out unless a defined message priority or connection is specified by the manufacturer specifications.		ICS specific	3,4
60.			Any remote operation shall be completed before another remote operation can change the operation of the preceding unless specified differently by the manufacturer specifications.	-	ICS specific	3,4

61.		SIA 4.3 Fail-safe mode	The component shall be able to enter a fail-safe mode or an annunciated fail operational mode when a communication failure occurs.		ICS specific	3,4
62.		SIA 4.4 Protection from malicious code	The application component supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.	-	Specific (SAR)	1,2,3,4
63.			The embedded device shall provide the capability to protect from installation, execution of malicious code or unauthorized software.	-	Specific (EDR)	1,2,3,4
64.			There shall be mechanisms on host devices that are qualified by the IACS component supplier to provide protection from malicious code. The IACS component supplier shall document any special configuration requirements related to protection from malicious code.	-	Specific (HDR)	1,2,3,4
65.			The network device shall provide for protection from malicious code.	-	Specific (NDR)	1,2,3,4
66.		SIA 4.5 Security functionality verification	Components shall provide the capability to verify the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	(1) Security functionality verification during normal operation. Components shall provide the capability to support verification of the intended operation of security functions during normal operations.	ICS specific	1,2,3,4 RE(1)-4
67.		SIA 4.6 Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	(1) Authenticity of software and information. Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can	ICS specific	1,2,3,4 RE(1)-2,3,4 RE(2)-3,4

				perform or support authenticity checks. (2) Automated notification of integrity. violations If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.		
68.		SIA 4.7 Input validation	Components shall validate the syntax and content of any input that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	-	ICS specific	1,2,3,4
69.		SIA 4.8 Deterministic output	Components that directly control a process shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.	-	ICS specific	1,2,3,4
70.		SIA 4.9 Error handling	Components shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner that does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	-	ICS specific	1,2,3,4
71.		SIA 4.10 Session integrity and authenticity	Components shall provide mechanisms to protect the integrity and authenticity of communications sessions.	(1) Invalidation of session IDs after session termination. Components shall provide the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions). (2) Unique session ID generation. Components shall provide the	ICS specific	2,3,4

				capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated. (3) Randomness of session IDs. Components shall provide the capability to generate unique session identifiers with commonly accepted sources of randomness.		
72.		SIA 4.11 Physical tamper resistance and detection	All types of devices (EDR, HDR, NDR) shall provide anti-tamper resistance and detection mechanisms for unauthorized physical access into the device.	(1) Notification of a tampering attempt. The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function .	ICS specific	2,3,4 RE(1)-3,4
73.		SIA 4.12 Provisioning component supplier roots of trust	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of component supplier keys and at the time of manufacture of the device.	-	Specific (EDR)	2,3,4
74.			Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of component supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	-	Specific (HDR)	2,3,4
75.			Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of component supplier keys and data to be	-	Specific (NDR)	2,3,4

			used as one or more "roots of trust" at the time of manufacture of the device.			
76.		SIA 4.13 Provisioning asset owner roots of trust	Embedded devices shall: a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and ; and b) support the capability to provision without reliance on components that may be outside of the device s security zone.	-	Specific (EDR)	2,3,4
77.			Host devices shall: c) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; d) support the capability to provision without reliance on components that may be outside of the device security zone.	-	Specific (HDR)	2,3,4
78.			Network devices shall: a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust" and b) support the capability to provision without reliance in components that may be outside of the device's security zone .	-	Specific (NDR)	2,3,4
79.		SIA 4.14 Integrity of the boot process	All types of devices (EDR, HDR, NDR) shall verify the integrity of the firmware, software, and configuration data boot process prior to it being used in the boot process.	(1) Authenticity of the boot process. Embedded devices shall use the component's component supplier roots of trust to verify the authenticity of the firmware, software and configuration data needed for component's boot process prior to it being used in the boot process .	Specific (EDR)	1,2,3,4 RE(1)-2,3,4
80.		SIA 4.15 List of approved integrity mechanisms	The following are approved integrity mechanisms: a) a message authentication code generated on the software and firmware components;	-	General	3,4

			b) a digital signature generated on the software and firmware components; c) a hash generated on the software and firmware components, where the hash is published in such a way that it is difficult for an attacker to change.			
81.		SIA 4.16 Genuinuty of the component	The authenticity checking method of the component shall be capable of tracing back software and/or hardware components to their genuine sources.	-	General	3,4
82.			The authenticity checking method of the component shall protect the properly authorized configuration information assets of the component.	-	General	3,4
83.			Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the component.	-	General	3,4
84.	**5. Data confidentiality (DC)**	DC 5.1 Information confidentiality	Components shall: a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; b) support the protection of the confidentiality of information in transit.	-	ICS specific	1,2,3,4
85.		DC 5.2 Information persistence	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	(1) Erase of shared memory resources Components shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources. (2) Erase verification Components shall provide the capability to verify that the erasure of information occurred.	ICS specific	2,3,4 RE(1)-3,4
86.		DC 5.3 Use of cryptography	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally	-	ICS specific	1,2,3,4

			recognized and proven security practices and recommendations (see Appnedix 1 and Appnedix 2 to the Framework) or in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.			
87.			Sensitive data (e.g. credentials) shall be stored in the component respectively transmitted only in encrypted form.	-	General	3,4
88.			Only established and well-known encryption algorithms shall be used and encryption key lengths, which are considered as safe according to the state-of-art. Proprietary encryption algorithms are not allowed.	-	General	1,2,3,4
89.			The implementation shall be done based on well-established encryption libraries to avoid implementation weaknesses.	-	General	1,2,3,4
90.			The key generation shall create secure keys and keys must be stored securely.	-	General	1,2,3,4
91.	**6. System and communication protection (SCP)**	SCP 6.1 Network segmentation	Components shall support a segmented network as defined in ISA 62443-3-2, as needed, to support the broader network architecture based on logical segmentation and criticality.	-	ICS specific	1,2,3,4
92.		SCP 6.2 Zone boundary protection	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk -based zones and conduits model.	(1) Deny all, permit by exception. The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception). (2) Island mode. The network component shall provide the capability to prevent any communication through the control system boundary (also termed island mode).	Specific (NDR)	1,2,3,4 RE(1)-2,3,4 RE(2)-3,4 RE(3)-3,4

				(3) Fail close. The network component shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms.		
93.			Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode.	-	ICS specific	1,2,3,4
94.		SCP 6.3 General purpose person-to-person communication restrictions	A network device at a zone boundary shall provide the capability to prevent general purpose, person-to-person messages from being received from users or systems external to the control system.	-	Specific (NDR)	1,2,3,4
95.		SCP 6.4 Denial of service protection	Components shall provide the capability to maintain essential functions in a degraded mode during a DoS event.	(1) Manage communication load from component. Components shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information and/or message flooding types of DoS events.	ICS specific	1,2,3,4 RE(1)-2,3,4
96.			A denial of service (DoS) event on the control system or safety instrumented system (SIS) network shall not prevent the SIF from acting.	-	ICS specific	1,2,3,4
97.		SCP 6.5 Resource management	Components shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	-	ICS specific	1,2,3,4
98.		SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	(1) Backup integrity verification. Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information. (2) Local backup	ICS specific	1,2,3,4 RE(1)-2,3,4

				Components shall provide the capability to perform a local backup independent of system functionality.		
99.		SCP 6.7 Control system recovery and reconstitution	Components shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	-	ICS specific	1,2,3,4
100.		SCP 6.8 Network and security configuration settings	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	(1) Machine-readable reporting of current security settings. Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	ICS specific	1,2,3,4 RE(1)-3,4
101.		SCP 6.9 Least functionality	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	-	ICS specific	1,2,3,4
102.		SCP 6.10 Control system component inventory	Components shall provide the capability to support a control system component inventory, that shall provide the capability to report the current list of installed components and their associated properties.	-	ICS specific	2,3,4
103.		SCP 6.11 Security function isolation	Component shall isolate security functions from non-security functions.	-	ICS specific	3,4
104.		SCP 6.12 Network disconnect	The network device shall terminate the network connection associated with a communications session at the end of the session or after a chosen by organization period of inactivity.	-	Specific (NDR)	3,4
105.	**7. Security by design (SD)**	SD 7.1 Update requirements	Component shall be designed and implemented such that it is possible to perform an update of the component's software, and to roll back an update to the current version during the update process if it fails.	-	General	3,4

106.			Component shall verify the authenticity and integrity of any software update cryptographically, before installing the update. component updates shall be possible in an offline environment. This offline component update mode should also still support validation of authenticity and integrity.	-	General	3,4
107.		SD 7.2 Initial operation	Prior to its initial operation in component, the component shall require changes of any system defaults that play a role in component security, such as passwords and keys.	-	General	3,4
108.		SD 7.3 Decomposition requirements	Decommissioning of the component after its use shall allow the ability to completely erase all configuration data, sensitive data and personally identifiable data. Zeroization of this data is acceptable and can be performed as an operation or as a process procedure: a) the operation or procedure shall at least include two steps of overwriting the configuration data, sensitive data and personally identifiable data with data that is not related; b) the operation or procedure shall destroy the configuration data, sensitive data or personally identifiable data from all parts of the component.	-	General	3,4
109.		SD 7.4 Display options	Component shall be able to easily display or communicate the version of the currently installed firmware to the user of the component.	-	ICS Specific	1,2,3,4
110.		SD 7.5 Deployment process	The software deployment process shall follow: a) the new software and firmware components shall be created with an approved software integrity mechanism to generate a factory code or signature for the	-	ICS Specific	3,4

			binary; b) deployment of the software/firmware to the component shall begin with the download of the software/firmware components which can be via a remote connection or directly connected component on a trusted path (for example a crossover cable or a storage unit added to the component); c) download of the software/firmware components to the component shall not interrupt the continued operation of the component as intended and not create a safety hazard unless an indicator is visible that the component is in an upgrade process;. d) the component may allow the erase of the audit log via operator intervention to allow for download of the software only if at a minimum, the component should start the new log with a record of the log erasure including the timestamp, and authenticated means and account.			
111.			After download of the software, the software shall verify the integrity test of the component. a) If the integrity test fails, the component shall stop the download process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The component shall continue to operate as intended. b) The component shall carry out the integrity check only when the component has received the complete software binary. c) The integrity mechanism shall be included in the software binary and shall not be downloaded separately.	-	ICS Specific	3,4

112.		SID 7.6 Uninstalling process	During the process of erasing/uninstalling of the old software, and install of the new software the component shall have an indicator of its current status of firmware installation. This indicator shall be both visual and audible if the component has the capability to have a visual signal.	-	ICS Specific	3,4
113.		SID 7.7 Usage of well-established design and pre-configuration requirements	Functionalities that are not needed shall not be installed.	-	General	1,2,3,4
114.			Functionalities that are installed shall have no undocumented capabilities, especially not those that run against the security and privacy interests of the operator (free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorized data forwarding).	-	General	1,2,3,4
115.			Component shall not utilize technologies, protocols and functionalities that are outdated or already recognized as insecure (e.g. SSL 3.0, MD5, or RC4, among others).	-	General	3,4
116.			The complete component, including extensions and enhancements, must be ready for mitigating known vulnerabilities.	-	General	3,4
117.		SID 7.8 Implementation security	The critical assets used to provide security shall be protected using hardware security. The requirement may be waived if the component's risk and threat analysis shows that these methods are not required or add no additional protection.	-	ICS Specific	3,4

5. Evaluation process

The testing process is a part of the evaluation for the created framework. That is why, during the process of technical testing some requirements from the Framework were either deleted or merged with other requirements. The testing process revealed twenty-three of original requirements were either not relevant for single devices (only relevant for system level) and therefore were deleted or partly/completely repeated other requirements, and in this case – merged. The Master Thesis contains the final version of the Framework that was finalized after performing the pilot project for three tested devices.

5.1. Testing methodology

During our assessment process, we went through all requirements for all SL to verify the compliance. For requirements that have extra Requirement Enhancements (RE) we at first evaluated compliance of the basic ones. If it is not met, we did not further check compliance of RE, since logically enhancements require stronger security mechanisms than the basic requirements.

Since this is a research project, evaluation was performed without having direct contact with manufacturers (vendors) of tested ICS devices. As a result, no support or extra documentation (not freely accessible) was provided which led to a number of limitation in assessment process, specifically some requirements received assessment status “Unknown”.

According to the created framework, there exist four types of possible devices (components): embedded devices (ED), host devices (HD), network devices (ND) and software application (SA). During testing process, we evaluated security level for three different devices of two different types:

- PLC 1[1] – embedded device;
- PLC 2 – embedded device
- Switch – network device.

This allowed us to evaluate created framework from two different angles: two devices of the same type with same requirements but different functionality and a device of a different type with different requirements.

The process of assessment of every requirement follows four steps presented below.

5.1.1. Analysing the requirement to assess the relevance for the device.

Some of the requirements presented in the Framework are not relevant due to exact functionalities presented within a device (e.g. the absence of wireless communication). Additionally, a number of requirements depend on a type of tested device, thus will not be relevant for particular types of devices (e.g. embedded devices).

5.1.2. Analysing the documentation to find relevant information regarding the requirement.

[1] Since the research was conducted without the support from the vendors of the devices, we are not going to reveal information about the exact tested models due to possible confidentiality issues

The list of documentation to be reviewed depends on the exact device but normally includes user manuals, getting started guides, quick references and information from official vendor web-site. Additional information could be obtained via communication with the vendor.

5.1.3. Technical verification if feasible by testing process.

For technical testing of a device there is a number of free software tools available that are commonly used for penetration testing such as:

- Nmap – network scanning tool;
- Wireshark – ttaffic analyser;
- Denial-of-Service (DoS) attack tools (hping3, LOIC).

Additionally, free software tools specifically designed for testing of ICS could be used:

- Modbus fuzzing – fuzzing testing tool for Modbus protocol;
- SMOD – penetration testing framework for exploiting vulnerabilities of ICS, created based on Metasploit Framework.

Some requirements could be tested without help of external tools; testing could be performed by connecting to the device with a dedicated method trough a PC.

5.1.4. Assessing the final compliance.

For every tested requirement there could be following types of results:

- met (the requirement is completely fulfilled);
- not met (the requirements is not fulfilled or partially fulfilled);
- unknown (no information found regarding needed functionality)[1];
- not relevant (no functional capability is present within the device).

The final results of assessment are introduced in a form of compliance score X met requirements of Y relevant requirements.

In the current Master Thesis we presented final assessment results in a form of a table for all tested devices. For one of the tested devices (PLC 1) we additionally presented a table in Appendix A with full assessment results, including description for used methods of assessment and explanation on results[2].

5.2. Testing results of PLC 1

5.2.1. Description of the device

The first tested device is a PLC, that could be used for controlling large stand-alone machine control application that require flexible communications and vast I/O capabilities. A PLC is an industrial digital computer which was adapted to be used for the control of manufacturing processes that requires high reliability control and ease of programming and process fault diagnosis.

The product presents the following input/output features:

[1] Due to limitation of the research with no communication with manufacturers of tested devices

[2] Due to time limitation of the research this table was created for one tested device

- Digital input type: 24V DC/V AC;
- Number of input points available: 14;
- Digital output type: 24V DC Source;
- Number of output points available: 10.

The device has the following features:

- includes 100 kHz speed high-speed counter (HSC) inputs;
- provides embedded communications via USB programming port, non-isolated serial port (for RS-232 and RS-485 communications) and Ethernet port;
- supports up to five Plug-in Modules;
- supports up to four Expansion I/O Modules, up to 132 I/O points;
- provides embedded motion capabilities by supporting as many as three axes with Pulse Train Outputs (PTO);
- communicates via Ethernet/IP;
- operates in -20…65 °C (-4…149 °F) temperature ranges.

. The device has the following communication ports:

- USB port: Type B connector USB port;
- Serial port: RS232/RS485 non-isolated combo serial port;
- Ethernet port: RJ-45 Ethernet connector.

The device has a proprietary firmware by developed by the vendor installed.

5.2.2. Assessment results

The final results of assessment for PLC 1 could be found in Table 6. Testing results for PLC 1. Since the main goal of testing process for different devices is to compare performance of these devices after being tested on the framework (and not to actually detail the assessment results for each of them), we provide the full results for only one device PLC 1 as an example. The full results of testing for PLC 1 could be found in Appendix A.

For the purpose of testing we listed every Requirement Enhancement (RE) as a separate requirement. For original requirements that are not met, RE were automatically considered as not met, no testing process was involved.

For a number of requirements, final result of assessment is unknown, since no information was found in documentation available in open access. The questions were sent to the vendor of the tested device, but no answer was received.

Table 6. Testing results for PLC 1.

#	Security requirement name	Security requirement	Result
1. Identification and Authentication control (IAC)			
1.	IAC 1.1.1 Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Not met.

2.	RE (1)	Components shall provide the capability to uniquely identify and authenticate all human users.	Not met.
3.	RE (2)	Components shall provide the capability to employ multifactor authentication for all human user access to the component	Not met.
4.	IAC 1.1.2	Identification and authentication shall not prevent the initiation of the Safety Instrumented Function (SIF).	Not relevant[1].
5.	IAC 1.2.1 Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices). If the component is running in the context of a human user, in addition, the identification and authentication of the human user according to IAC 1.1. may be part of the component identification and authentication process towards other components.	Unknown.
6.	RE (1)	Components shall provide the capability to uniquely and securely identify and authenticate itself to any other component.	Unknown.
7.	IAC 1.3 Account management	Components shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly (management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts).	Not met.
8.	IAC 1.4 Identifier management	Components shall provide the capability to integrate into a system that supports the management or identifiers and/or provide the capability to support the management of identifiers directly (support the management of identifiers by user, group, role or control system interface).	Not met.
9.	IAC 1.5 Authenticator management	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	a) Met. b) Not relevant. c) Met. d)Unknown.
10.	RE (1)	The authenticators on which the component rely shall be protected via hardware mechanisms.	Not met.
11.	IAC 1.7 Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength based on minimum length and variety of character types. The password complexity must be configurable by the administrator and be either technically or procedurally enforced with following password parameters: - minimal password length at least of eight characters (or the maximum length supported by the component); - maximum password length; - minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the component); - minimum and maximum usage period; - prevention of re-use of previous passwords; - maximum number of password changes per time (e.g. per day).	Not met.
12.	RE (1)	Components shall provide, or integrate into a system that provides, the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	Not met.

[1] Could only be tested within the system that includes SIF

13.	RE (2)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	Not met.
14.	IAC 1.8 Password protection	If the component uses a user name-and-password mechanism for authenticating users: a) The component shall use a secure mechanism to store the passwords, they shall not be stored in plaintext. b) Authentication error messages provided by the component shall not allow for enumerating valid user names. d) The component shall protect against dictionary attacks and brute force attacks. e) The component shall have no hardcoded passwords that cannot be removed or altered.	a) Unknown. b) Not relevant. c) Not met. d) Met.
15.	IAC 1.9 Password changes enforcements	For password-only authentication for interactive user access it shall be possible to change the password at any given to enforce the policy of password regular update	**Met.**
16.	IAC 1.10.1 Public key infrastructure certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance commonly accepted best practices or obtain public key certificates from an existing PKI.	Not relevant.
17.	IAC 1.10.2	For high availability control systems, the failure of the certificate authority shall not interrupt essential functions	Not relevant.
18.	IAC 1.11.1 Strength of public key-based authentication	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same ICS environment to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; f) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	Not relevant.
19.	RE (1)	The control system shall provide the capability to protect the relevant private keys via hardware.	Not relevant.
20.	IAC 1.11.2	If the component uses other mechanisms for authentication besides username and password, the mechanism used for authentication shall require as many operations to circumvent as determining the actual mechanism.	Not relevant.
21.	IAC 1.12 Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.	Not met.
22.	IAC 1.13.1 Unsuccessful login attempts	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; or b) generate alerts after a threshold of unsuccessful authentication attempts; c) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.	Not met.
23.	IAC 1.13.2	Accounts used for essential functions shall not be locked out, even temporarily.	Not met.

24.	IAC 1.14 System use notification	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	Not relevant.
25.	IAC 1.16 Strength of symmetric key-based authentication	For components that utilize symmetric keys, the component shall provide the capability to: a) establish the mutual trust using the symmetric key; s) store securely the shared secret (the authentication is valid as long as the shared secret remains secret); t) restrict access to the shared secret; u) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	Not relevant.
26.	RE (1)	Component shall provide the capability to protect the relevant private keys via hardware mechanisms.	Not relevant.
2. Use control (UC)			
27.	UC 2.1.1 Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least privilege. Access to data shall only be given after successful authentication and authorization. Without successful authentication and authorization, the system shall not allow any activities.	Not met.
28.	RE (1)	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	Not met.
29.	RE (2)	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.	Not met.
30.	RE (3)	Components shall support a supervisor manual override for a configurable time or sequence of events.	Not met.
31.	RE (4)	Components shall support dual approval when action can result in serious impact on the industrial process.	Not met.
32.	UC 2.1.2	Authorization enforcement shall not prevent the initiation of the SIF	Not relevant[1].
33.	UC 2.2 Usage restriction	Service accounts shall not be usable for interactive logon.	Not relevant.
34.	UC 2.3 Wireless use control	The component shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.	Not relevant.
35.	UC 2.4 Mobile code	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device: a) control execution of mobile code; b) control which users (human, software process, or device) are allowed to upload mobile code to the device; c) control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Not relevant.
36.	RE(1)	The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Not relevant.
37.	UC 2.5 Session lock	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability: a) to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation; b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes	Not met.

[1] Could only be tested within the system that includes SIF

		access using appropriate identification and authentication procedures; c) to comply with session locks requested by the underlying infrastructure (operating system, control system).	
38.	UC 2.6.1 Remote session control	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity , manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	Not relevant.
39.	UC 2.6.2	At no time shall the use of remote access compromise the integrity of the component or change the intended use of the component.	Not relevant.
40.	UC 2.6.3	If a component allows remote access, the component shall be able to operate continuously, automatically or remotely without causing a safety hazard and the component shall signal its remote operation visibly on the component.	Not relevant.
41.	UC 2.6.4	If a local action is initiated on the component, it shall take precedence and priority over a remote action that occurs at the same time.	Not relevant.
42.	UC 2.6.5	If a communication session over a remote interface is lost or terminated, the component shall require renewed authentication prior to allowing access over the remote interface. Stored data from the previous session shall not be used to initiate the new session.	Not relevant.
43.	UC 2.6.6	The component shall be configurable to allow once a user is authenticated and granted remote access to the component, the component shall reject and record any attempt to setup another remote connection using the same user identity.	Not relevant.
44.	UC 2.6.7	The transmission of the authentication credential to a component via a remote connection covered on this section cannot be in plaintext or easily intercepted and duplicated unless: a) the information by itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information; b) the transmission path is a trusted path, for example a directly connected physical cable that is not shared by any other system or components.	Not relevant.
45.	UC 2.7 Concurrent session control	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	**Met.**
46.	UC 2.8 Use of physical diagnostic and test interfaces	Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	Not relevant
47.	RE (1)	Embedded devices shall provide active monitoring of the device’s diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	Not relevant
48.	UC 2.9.1 Control over other ports usage	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by organization, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	**Met.**
49.	UC 2.10 Managing the operators status	The component shall allow the ability for an operator to be disabled, deleted, expired or change of permissions when the component is not in a critical operator-dependent state transition with the operator to be disabled, deleted, expired or permission changed.	Not met.
50.	UC 2.10.2	If the operator is connected and the operator permissions or status changes, the operator shall be disconnected and a record in the audit log shall be made.	Not met.
3. Audit and accountability (AU)			

51.	AU 3.1.1 Auditable events	Components shall provide the capability to generate audit records relevant to security y for the following categories: a) access control (as minimum: successful login attempts, failed access and login attempts); b) request errors; c) control system events; d) backup and restore event; e) configuration changes (e.g. successful and unsuccessful software updates); f) audit log events; g) detected malware (if applicable).	Not met.
52.	AU 3.1.2	The component shall provide the capability to select which auditable events are to be audited by specific parts of the component by administrator.	Not met.
53.	AU 3.2 Audit storage capacity	Components shall: a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; b) provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.	Not met.
54.	RE (1)	Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.	Not met.
55.	AU 3.3 Response to audit processing failures	Components shall: a) provide the capability to prevent the loss of essential services and functions in the event of an audit processing failure; b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Not met.
56.	AU 3.4.1 Timestamps	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	**Met.**
57.	RE (1)	Components shall provide the capability to create timestamps that are synchronized with a system wide time source.	Not met.
58.	RE (2)	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	Not met.
59.	AU 3.4.2	Incorrectly timestamped audit records shall not adversely affect essential functions.	Unknown.
60.	AU 3.5 Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	Not met.
61.	RE (1)	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Not met.
62.	AU 3.5.2	Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time.	Not met.
63.	AU 3.6.1 Protection of audit information	The component shall protect audit information and audit tools (if applicable) from unauthorized access, modification, and deletion.	Not met.
64.	RE(1)	Components shall provide the capability to store audit records on hardware-enforced write-once media.	Not met.
65.	AU 3.6.2	Unless and until they are transmitted to an external data storage, the component shall store all security-related logs in non-volatile memory and shall not allow non-privileged users to remove or change them.	Not met.
66.	AU 3.7 Audit reduction and report generation	The component shall provide an audit reduction and report generation capability that: a) supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; b) does not alter the original content or time ordering of audit records.	Not met.

67.	AU 3.8 Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Not met.
68.	RE(1)	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system	Not met.
69.	AU 3.9 Continuous monitoring	When a component provides a security mechanism, that component shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breached in a timely manner.	Not met.
4. System integrity and authenticity (SIA)			
70.	SIA 4.1 Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Not met.
71.	RE(1)	Components shall provide the capability to authenticate information during communication.	Not met.
72.	SIA 4.2.1 Remote communication integrity and authenticity	The component shall ensure the integrity and authenticity of all data communicated over any remote interface. For this, the component shall use security functions complying with the requirements for use of cryptography. Exception: Remote interfaces that report status, do not provide command and control functionality or do not transmit sensitive data, etc., may not ensure integrity and authenticity but will need to be documented.	Not relevant.
73.	SIA 4.2.2	Remote connection from different sources shall not disturb the proper function of the component and shall not cause any security flaw.	Not relevant.
74.	SIA 4.2.3	Messages sent over a remote connection shall be processed as first in, first out unless a defined message priority or connection is specified by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	Not relevant.
75.	SIA 4.2.4	Any remote operation shall be completed before another remote operation can change the operation of the preceding unless specified differently by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	Not relevant.
76.	SIA 4.3 Fail-safe mode	The component shall be able to enter a fail-safe mode or an annunciated fail operational mode when a communication failure occurs.	Not met.
77.	SIA 4.4 Protection from malicious code	The embedded device shall provide the capability to protect from installation and execution of unauthorized software.	Unknown.
78.	SIA 4.5 Security functionality verification	Components shall provide the capability to verify the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Not met.
79.	RE(1)	Components shall provide the capability to support verification of the intended operation of security functions during normal operations.	Not met.
80.	SIA 4.6 Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Not met.
81.	RE(1)	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or	Not met.

		be integrated into a system that can perform or support authenticity checks.	
82.	RE(2)	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	Not met.
83.	SIA 4.7 Input validation	Components shall validate the syntax and content of any input that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	**Met.**
84.	SIA 4.8 Deterministic output	Components that directly control a process shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack	**Met.**
85.	SIA 4.9 Error handling	Components shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner that does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	Not met.
86.	SIA 4.10 Session integrity and authenticity	Components shall provide mechanisms to protect the integrity and authenticity of communications sessions.	Not met.
87.	RE(1)	Components shall provide the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions).	Not met.
88.	RE(2)	Components shall provide the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.	Not met.
89.	RE(3)	Components shall provide the capability to generate unique session identifiers with commonly accepted sources of randomness.	Not met.
90.	SIA 4.11 Physical tamper resistance and detection	The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Not met.
91.	RE (1)	The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Not met.
92.	SIA 4.12 Provisioning component supplier roots of trust	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.	Not relevant.
93.	SIA 4.13 Provisioning asset owner roots of trust	Embedded devices shall: a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; b) support the capability to provision without reliance on components that may be outside of the device security zone.	Not relevant.
94.	SIA 4.14 Integrity of the boot process	Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component’s boot and runtime processes prior to use.	Not met.
95.	SIA 4.15 List of approved integrity mechanisms	The following are approved integrity mechanisms: a) A message authentication code generated on the software and firmware components. b) A digital signature generated on the software and firmware components. c) A hash generated on the software and firmware components, where the hash is published in such a way that it is difficult for an attacker to change.	Not met.
96.	SIA 4.16.1 Genuinuty of the component	The authenticity checking method of the component shall be capable of tracing back software and/or hardware components to their genuine sources.	Not met.

97.	SIA 4.16.2	The authenticity checking method of the component shall protect the properly authorized configuration information assets of the system	Not met.
98.	SIA 4.16.3	Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the system.	Not met.
5. Data confidentiality (DC)			
99.	DC 5.1 Information confidentiality	Components shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and b) support the protection of the confidentiality of information in transit.	Not relevant.
100.	DC 5.2 Information persistence	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	Not relevant.
101.	RE(1)	Components shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.	Not relevant.
102.	RE(2)	Components shall provide the capability to verify that the erasure of information occurred.	Not relevant.
103.	DC 5.3.1 Use of cryptography	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations or in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Unknown.
104.	DC 5.3.2	Sensitive data (e.g. credentials) may be stored in the component respectively transmitted only in encrypted form.	Unknown.
105.	DC 5.3.3	Only established and well-known encryption algorithms may be used and encryption key lengths, which are considered as safe according to the state-of-art. Proprietary encryption algorithms are not allowed.	Unknown.
106.	DC 5.3.4	The implementation must be done based on well-established encryption libraries to avoid implementation weaknesses.	Unknown.
107.	DC 5.3.5	The key generation must create secure keys and keys must be stored securely.	Unknown.
6. System and communication protection (SCP)			
108.	SCP 6.1 Network segmentation	Components shall support a segmented network as defined in ISA 62443-3-2, as needed, to support the broader network architecture based on logical segmentation and criticality.	Not relevant[1].
109.	SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	Not relevant.
110.	RE(1)	Backup integrity verification. Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Not relevant.
111.	RE(2)	Local backup. Components shall provide the capability to perform a local backup independent of system functionality.	Not relevant.
112.	SCP 6.4.1 Denial of service protection	Components shall provide the capability to maintain essential functions in a degraded mode during a DoS event.	**Met.**
113.	SCP 6.4.2	A denial of service (DoS) event shall not prevent the SIF from acting.	Not relevant[2].

[1] Could only be tested within a system with different network zones

[2] Could only be tested within the system that includes SIF

114.	SCP 6.5 Resource management	Components shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	**Met.**
115.	SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	Not met.
116.	RE(1)	Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Not met.
117.	RE(2)	Components shall provide the capability to perform a local backup independent of system functionality.	Not met.
118.	SCP 6.7 Control system recovery and reconstitution	Components shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	**Met.**
119.	SCP 6.8 Network and security configuration settings	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	**Met.**
120.	RE(1)	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Not met.
121.	SCP 6.9 Least functionality	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	**Met.**
122.	SCP 6.10 Control system component inventory	Components shall provide the capability to support a control system component inventory, that shall provide the capability to report the current list of installed components and their associated properties.	Not relevant[1].
123.	SCP 6.11 Security function isolation	The component shall isolate security functions from nonsecurity functions.	Unknown.
7. Security by design (SD)			
124.	SD 7.1.1 Update requirements	Component shall be designed and implemented such that it is possible to perform an update of the component's software, and to roll back an update to the current version during the update process if it fails.	**Met.**
125.	SD 7.1.2	Component shall verify the authenticity and integrity of any software update cryptographically, before installing the update. Component updates shall be possible in an offline environment. This offline component update mode should also still support validation of authenticity and integrity.	Unknown.
126.	SD 7.2 Initial operation	Prior to its initial operation, the component shall require changes of any system defaults that play a role in component security, such as passwords and keys.	Not relevant.
127.	SD 7.3 Decomposition requirements	Decommissioning of the component after its use shall allow the ability to completely erase all configuration data, sensitive data and personally identifiable data. Zeroization of this data is acceptable and can be performed as an operation or as a process procedure: a) The operation or procedure shall at least include two steps of overwriting the configuration data, sensitive data and personally identifiable data with data that is not related); b) The operation or procedure shall destroy the configuration data, sensitive data or personally identifiable data from all parts of the component.	**Met.**
128.	SD 7.4 Display options	Component shall be able to easily display or communicate the version of the currently installed firmware to the user of the component.	**Met.**

129.	SD 7.5.1 Deployment process	The software deployment process shall follow: a) The new software and firmware components shall be created with an approved software integrity mechanism to generate a factory code or signature for the binary. b) Deployment of the software/firmware to the component shall begin with the download of the software/firmware components which can be via a remote connection or directly connected component on a trusted path (for example a crossover cable or a storage unit added to the component). c) Download of the software/firmware components to the component shall not interrupt the continued operation of the component as intended and not create a safety hazard unless an indicator is visible that the component is in an upgrade process. d) The component may allow the erase of the audit log via operator intervention to allow for download of the software only if at a minimum, the component should start the new log with a record of the log erasure including the timestamp, and authenticated means and account.	a) Not met. b) Met. c) Met. d) Not met.
130.	SD 7.5.2	After download of the software, the software shall verify the integrity test of the component. a) If the integrity test fails, the component shall stop the download process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The component shall continue to operate as intended. b) The component shall carry out the integrity check only when the component has received the complete software binary. c) The integrity mechanism shall be included in the software binary and shall not be downloaded separately.	Not met.
131.	SD 7.6 Uninstalling process	During the process of erasing/uninstalling of the old software, and install of the new software the component shall have an indicator of its current status of firmware installation. This indicator shall be both visual and audible if the component has the capability to have a visual signal.	Not met.
132.	SD 7.7.1 Usage of well-established design and pre-configuration requirements	Functionalities that are not needed shall not be installed.	**Met.**
133.	SD 7.7.2	Functionalities that are installed shall have no undocumented capabilities, especially not those that run against the security and privacy interests of the operator (free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorized data forwarding).	**Met.**
134.	SD 7.7.3	The component shall not utilize technologies, protocols and functionalities that are outdated or already recognized as insecure (e.g. SSL 3.0, MD5, or RC4, among others)	**Met.**
135.	SD 7.7.4	The complete component, including extensions and enhancements, must be ready for mitigating known vulnerabilities.	Not met.
136.	SD 7.8 Implementation security	The critical assets used to provide security shall be protected using hardware security. Exception: the requirement may be waived if the component's risk and threat analysis shows that these methods are not required or add no additional protection.	Not relevant[1].

To evaluate overall compliance of the device with the Framework we use compliance score which represents a number of met requirements amongst relevant to a particular device

[1] Could only be tested after installing within a system and performing the risk analysis

requirements. Additionally, we can use the concept of security levels introduced within the Framework to evaluate if the device could be certified for a certain security level.

- *The overall compliance score with the Framework is **17 of 95**[1].*
- *The final SL assigned to the device is **0**.*

5.3. Testing results of PLC 2

5.3.1. Description of the device

The second tested device is a PLC that is commonly used to control compact machines, including wide positioning capabilities, such as robots. The embedded Ethernet port allows connection for monitoring, flexible operation, logging and remote access.

The product presents following input/output features:

- Digital input type: 24V DC/V AC;
- Number of input points available: 12;
- Digital output type: 24V DC Source;
- Number of output points available: 8.

The device has following features:

- memory capacity: 5K steps;
- high-speed counters: 100 kH, 4 axes;
- pulse outputs: 100 kHz, 2 axes;
- includes 100 kHz speed high-speed counter (HSC) inputs;
- provides embedded communication via Ethernet port;
- 6 interrupt inputs are built in;
- supports structured text (ST) language;
- ambient operating temperature: 0…55 °C (-4…149 °F) temperature ranges;
- ambient operating humidity: 10 – 90% (with no condensation);
- power holding time: 2 ms min.

. The device has following communication ports:

- Ethernet port: RJ-45 Ethernet connector;
- Backplane databus.

No information was found regarding installed firmware. Update of the device is only possible by sending the device to the manufacturer.

5.3.2. Assessment results

The final assessment results for PLC 2 could be found in Table 7. Testing results for PLC 2.

For a number of requirements, result is unknown, since no information was found in documentation available in open access. The questions were sent to the vendor of the device, no answer was received.

[1] For the sake of calculating the compliance score we assume that requirements that are “Unknown” are “Not met”, since no information was found in the documentation or through testing process

Table 7. Testing results for PLC 2

#	Security requirement name	Security requirement	Result
1. Identification and Authentication control (IAC)			
1.	IAC 1.1.1 Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Not met.
2.	RE (1)	Components shall provide the capability to uniquely identify and authenticate all human users.	Not met.
3.	RE (2)	Components shall provide the capability to employ multifactor authentication for all human user access to the component	Not met.
4.	IAC 1.1.2	Identification and authentication shall not prevent the initiation of the Safety Instrumented Function (SIF).	Not relevant[1].
5.	IAC 1.2.1 Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices). If the component is running in the context of a human user, in addition, the identification and authentication of the human user according to IAC 1.1. may be part of the component identification and authentication process towards other components.	Unknown.
6.	RE (1)	Components shall provide the capability to uniquely and securely identify and authenticate itself to any other component.	Unknown.
7.	IAC 1.3 Account management	Components shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly (management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts).	Not met.
8.	IAC 1.4 Identifier management	Components shall provide the capability to integrate into a system that supports the management or identifiers and/or provide the capability to support the management of identifiers directly (support the management of identifiers by user, group, role or control system interface).	Not met.
9.	IAC 1.5 Authenticator management	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	a) Met. b) Not relevant. c) Met. d)Unknown.
10.	RE (1)	The authenticators on which the component rely shall be protected via hardware mechanisms.	Not met.
11.	IAC 1.7 Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength based on minimum length and variety of character types. The password complexity must be configurable by the administrator and be either technically or procedurally enforced with following password parameters: - minimal password length at least of eight characters (or the maximum length supported by the component); - maximum password length; - minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase	Not met.

[1] Could only be tested within the system that includes SIF

		alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the component); - minimum and maximum usage period; - prevention of re-use of previous passwords; - maximum number of password changes per time (e.g. per day).	
12.	RE (1)	Components shall provide, or integrate into a system that provides, the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	Not met.
13.	RE (2)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	Not met.
14.	IAC 1.8 Password protection	If the component uses a user name-and-password mechanism for authenticating users: a) The component shall use a secure mechanism to store the passwords, they shall not be stored in plaintext. b) Authentication error messages provided by the component shall not allow for enumerating valid user names. d) The component shall protect against dictionary attacks and brute force attacks. e) The component shall have no hardcoded passwords that cannot be removed or altered.	a) Unknown. b) Not met. c) Not met. d) Met.
15.	IAC 1.9 Password changes enforcements	For password-only authentication for interactive user access it shall be possible to change the password at any given to enforce the policy of password regular update.	**Met.**
16.	IAC 1.10.1 Public key infrastructure certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance commonly accepted best practices or obtain public key certificates from an existing PKI.	Not relevant.
17.	IAC 1.10.2	For high availability control systems, the failure of the certificate authority shall not interrupt essential functions	Not relevant.
18.	IAC 1.11.1 Strength of public key-based authentication	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same ICS environment to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; f) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	Not relevant.
19.	RE (1)	The control system shall provide the capability to protect the relevant private keys via hardware.	Not relevant.
20.	IAC 1.11.2	If the component uses other mechanisms for authentication besides username and password, the mechanism used for authentication shall require as many operations to circumvent as determining the actual mechanism.	Not relevant.
21.	IAC 1.12 Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.	Not met.

22.	IAC 1.13.1 Unsuccessful login attempts	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; or b) generate alerts after a threshold of unsuccessful authentication attempts; c) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.	Not met.
23.	IAC 1.13.2	Accounts used for essential functions shall not be locked out, even temporarily.	Not met.
24.	IAC 1.14 System use notification	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	Not relevant.
25.	IAC 1.16 Strength of symmetric key-based authentication	For components that utilize symmetric keys, the component shall provide the capability to: a) establish the mutual trust using the symmetric key; s) store securely the shared secret (the authentication is valid as long as the shared secret remains secret); t) restrict access to the shared secret; u) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	Not relevant.
26.	RE (1)	Component shall provide the capability to protect the relevant private keys via hardware mechanisms.	Not relevant.
2. Use control (UC)			
27.	UC 2.1.1 Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least privilege. Access to data shall only be given after successful authentication and authorization. Without successful authentication and authorization, the system shall not allow any activities.	Not met.
28.	RE (1)	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	Not met.
29.	RE (2)	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.	Not met.
30.	RE (3)	Components shall support a supervisor manual override for a configurable time or sequence of events.	Not met.
31.	RE (4)	Components shall support dual approval when action can result in serious impact on the industrial process.	Not met.
32.	UC 2.1.2	Authorization enforcement shall not prevent the initiation of the SIF	Not relevant[1].
33.	UC 2.2 Usage restriction	Service accounts shall not be usable for interactive logon.	Not relevant.
34.	UC 2.3 Wireless use control	The component shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.	Not relevant.
35.	UC 2.4 Mobile code	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device: a) control execution of mobile code;	Not relevant.

[1] Could only be tested within the system that includes SIF

		b) control which users (human, software process, or device) are allowed to upload mobile code to the device; c) control the execution of mobile code based on the results of an integrity check prior to the code being executed.	
36.	RE(1)	The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Not relevant.
37.	UC 2.5 Session lock	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability: a) to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation; b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures; c) to comply with session locks requested by the underlying infrastructure (operating system, control system).	Not met.
38.	UC 2.6.1 Remote session control	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity , manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	Not relevant.
39.	UC 2.6.2	At no time shall the use of remote access compromise the integrity of the component or change the intended use of the component.	Not relevant.
40.	UC 2.6.3	If a component allows remote access, the component shall be able to operate continuously, automatically or remotely without causing a safety hazard and the component shall signal its remote operation visibly on the component.	Not relevant.
41.	UC 2.6.4	If a local action is initiated on the component, it shall take precedence and priority over a remote action that occurs at the same time.	Not relevant.
42.	UC 2.6.5	If a communication session over a remote interface is lost or terminated, the component shall require renewed authentication prior to allowing access over the remote interface. Stored data from the previous session shall not be used to initiate the new session.	Not relevant.
43.	UC 2.6.6	The component shall be configurable to allow once a user is authenticated and granted remote access to the component, the component shall reject and record any attempt to setup another remote connection using the same user identity.	Not relevant.
44.	UC 2.6.7	The transmission of the authentication credential to a component via a remote connection covered on this section cannot be in plaintext or easily intercepted and duplicated unless: a) the information by itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information; b) the transmission path is a trusted path, for example a directly connected physical cable that is not shared by any other system or components.	Not relevant.
45.	UC 2.7 Concurrent session control	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	**Met.**
46.	UC 2.8 Use of physical diagnostic and test interfaces	Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	Not relevant
47.	RE (1)	Embedded devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	Not relevant

48.	UC 2.9.1 Control over other ports usage	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by organization, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	**Met.**
49.	UC 2.10 Managing the operators status	The component shall allow the ability for an operator to be disabled, deleted, expired or change of permissions when the component is not in a critical operator-dependent state transition with the operator to be disabled, deleted, expired or permission changed.	Not met.
50.	UC 2.10.2	If the operator is connected and the operator permissions or status changes, the operator shall be disconnected and a record in the audit log shall be made.	Not met.
3. Audit and accountability (AU)			
51.	AU 3.1.1 Auditable events	Components shall provide the capability to generate audit records relevant to security y for the following categories: a) access control (as minimum: successful login attempts, failed access and login attempts); b) request errors; c) control system events; d) backup and restore event; e) configuration changes (e.g. successful and unsuccessful software updates); f) audit log events; g) detected malware (if applicable).	Not met.
52.	AU 3.1.2	The component shall provide the capability to select which auditable events are to be audited by specific parts of the component by administrator.	Not met.
53.	AU 3.2 Audit storage capacity	Components shall: a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; b) provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.	Not met.
54.	RE (1)	Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.	Not met.
55.	AU 3.3 Response to audit processing failures	Components shall: a) provide the capability to prevent the loss of essential services and functions in the event of an audit processing failure; b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Not met.
56.	AU 3.4.1 Timestamps	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	Not met.
57.	RE (1)	Components shall provide the capability to create timestamps that are synchronized with a system wide time source.	Not met.
58.	RE (2)	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	Not met.
59.	AU 3.4.2	Incorrectly timestamped audit records shall not adversely affect essential functions.	Unknown.
60.	AU 3.5 Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	Not met.
61.	RE (1)	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Not met.
62.	AU 3.5.2	Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time.	Not met.

63.	AU 3.6.1 Protection of audit information	The component shall protect audit information and audit tools (if applicable) from unauthorized access, modification, and deletion.	Not met.
64.	RE(1)	Components shall provide the capability to store audit records on hardware-enforced write-once media.	Not met.
65.	AU 3.6.2	Unless and until they are transmitted to an external data storage, the component shall store all security-related logs in non-volatile memory and shall not allow non-privileged users to remove or change them.	Not met.
66.	AU 3.7 Audit reduction and report generation	The component shall provide an audit reduction and report generation capability that: a) supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; b) does not alter the original content or time ordering of audit records.	Not met.
67.	AU 3.8 Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Not met.
68.	RE(1)	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system	Not met.
69.	AU 3.9 Continuous monitoring	When a component provides a security mechanism, that component shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breached in a timely manner.	Not met.
4. System integrity and authenticity (SIA)			
70.	SIA 4.1 Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Not met.
71.	RE(1)	Components shall provide the capability to authenticate information during communication.	Not met.
72.	SIA 4.2.1 Remote communication integrity and authenticity	The component shall ensure the integrity and authenticity of all data communicated over any remote interface. For this, the component shall use security functions complying with the requirements for use of cryptography. Exception: Remote interfaces that report status, do not provide command and control functionality or do not transmit sensitive data, etc., may not ensure integrity and authenticity but will need to be documented.	Not relevant.
73.	SIA 4.2.2	Remote connection from different sources shall not disturb the proper function of the component and shall not cause any security flaw.	Not relevant.
74.	SIA 4.2.3	Messages sent over a remote connection shall be processed as first in, first out unless a defined message priority or connection is specified by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	Not relevant.
75.	SIA 4.2.4	Any remote operation shall be completed before another remote operation can change the operation of the preceding unless specified differently by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	Not relevant.
76.	SIA 4.3 Fail-safe mode	The component shall be able to enter a fail-safe mode or an annunciated fail operational mode when a communication failure occurs.	Not met.
77.	SIA 4.4 Protection from malicious code	The embedded device shall provide the capability to protect from installation and execution of unauthorized software.	Unknown.

78.	SIA 4.5 Security functionality verification	Components shall provide the capability to verify the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Not met.
79.	RE(1)	Components shall provide the capability to support verification of the intended operation of security functions during normal operations.	Not met.
80.	SIA 4.6 Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Not met.
81.	RE(1)	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Not met.
82.	RE(2)	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	Not met.
83.	SIA 4.7 Input validation	Components shall validate the syntax and content of any input that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	**Met.**
84.	SIA 4.8 Deterministic output	Components that directly control a process shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack	**Met.**
85.	SIA 4.9 Error handling	Components shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner that does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	**Met.**
86.	SIA 4.10 Session integrity and authenticity	Components shall provide mechanisms to protect the integrity and authenticity of communications sessions.	Not met.
87.	RE(1)	Components shall provide the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions).	Not met.
88.	RE(2)	Components shall provide the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.	Not met.
89.	RE(3)	Components shall provide the capability to generate unique session identifiers with commonly accepted sources of randomness.	Not met.
90.	SIA 4.11 Physical tamper resistance and detection	The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Not met.
91.	RE (1)	The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Not met.
92.	SIA 4.12 Provisioning component supplier roots of trust	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.	Not relevant.
93.	SIA 4.13 Provisioning asset owner roots of trust	Embedded devices shall: a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; b) support the capability to provision without reliance on components that may be outside of the device security zone.	Not relevant.

94.	SIA 4.14 Integrity of the boot process	Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component’s boot and runtime processes prior to use.	Not met.
95.	SIA 4.15 List of approved integrity mechanisms	The following are approved integrity mechanisms: a) A message authentication code generated on the software and firmware components. b) A digital signature generated on the software and firmware components. c) A hash generated on the software and firmware components, where the hash is published in such a way that it is difficult for an attacker to change.	Not met.
96.	SIA 4.16.1 Genuinuty of the component	The authenticity checking method of the component shall be capable of tracing back software and/or hardware components to their genuine sources.	Not met.
97.	SIA 4.16.2	The authenticity checking method of the component shall protect the properly authorized configuration information assets of the system	Not met.
98.	SIA 4.16.3	Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the system.	Not met.
5. Data confidentiality (DC)			
99.	DC 5.1 Information confidentiality	Components shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and b) support the protection of the confidentiality of information in transit.	Not relevant.
100.	DC 5.2 Information persistence	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	Not relevant.
101.	RE(1)	Components shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.	Not relevant.
102.	RE(2)	Components shall provide the capability to verify that the erasure of information occurred.	Not relevant.
103.	DC 5.3.1 Use of cryptography	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations or in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Unknown.
104.	DC 5.3.2	Sensitive data (e.g. credentials) may be stored in the component respectively transmitted only in encrypted form.	Unknown.
105.	DC 5.3.3	Only established and well-known encryption algorithms may be used and encryption key lengths, which are considered as safe according to the state-of-art. Proprietary encryption algorithms are not allowed.	Unknown.
106.	DC 5.3.4	The implementation must be done based on well-established encryption libraries to avoid implementation weaknesses.	Unknown.
107.	DC 5.3.5	The key generation must create secure keys and keys must be stored securely.	Unknown.
6. System and communication protection (SCP)			
108.	SCP 6.1 Network segmentation	Components shall support a segmented network as defined in ISA 62443-3-2, as needed, to support the broader network architecture based on logical segmentation and criticality.	Not relevant[1].
109.	SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	Not relevant.
110.	RE(1)	Backup integrity verification. Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Not relevant.

[1] Could only be tested within a system with different network zones

111.	RE(2)	Local backup. Components shall provide the capability to perform a local backup independent of system functionality.	Not relevant.
112.	SCP 6.4.1 Denial of service protection	Components shall provide the capability to maintain essential functions in a degraded mode during a DoS event.	**Met.**
113.	SCP 6.4.2	A denial of service (DoS) event shall not prevent the SIF from acting.	Not relevant[1].
114.	SCP 6.5 Resource management	Components shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	**Met.**
115.	SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	**Met.**
116.	RE(1)	Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Not met.
117.	RE(2)	Components shall provide the capability to perform a local backup independent of system functionality.	**Met.**
118.	SCP 6.7 Control system recovery and reconstitution	Components shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	Not met.
119.	SCP 6.8 Network and security configuration settings	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	**Met.**
120.	RE(1)	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Not met.
121.	SCP 6.9 Least functionality	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	**Met.**
122.	SCP 6.10 Control system component inventory	Components shall provide the capability to support a control system component inventory, that shall provide the capability to report the current list of installed components and their associated properties.	Not relevant[1].
123.	SCP 6.11 Security function isolation	The component shall isolate security functions from nonsecurity functions.	Unknown.
7. Security by design (SD)			
124.	SD 7.1.1 Update requirements	Component shall be designed and implemented such that it is possible to perform an update of the component's software, and to roll back an update to the current version during the update process if it fails.	Not met.
125.	SD 7.1.2	Component shall verify the authenticity and integrity of any software update cryptographically, before installing the update. Component updates shall be possible in an offline environment. This offline component update mode should also still support validation of authenticity and integrity.	Unknown.
126.	SD 7.2 Initial operation	Prior to its initial operation, the component shall require changes of any system defaults that play a role in component security, such as passwords and keys.	Not relevant.
127.	SD 7.3 Decomposition requirements	Decommissioning of the component after its use shall allow the ability to completely erase all configuration data, sensitive data and personally identifiable data. Zeroization of this data is acceptable and can be performed as an operation or as a process procedure:	**Met.**

[1] Could only be tested within the system that includes SIF

		a) The operation or procedure shall at least include two steps of overwriting the configuration data, sensitive data and personally identifiable data with data that is not related); b) The operation or procedure shall destroy the configuration data, sensitive data or personally identifiable data from all parts of the component.	
128.	SD 7.4 Display options	Component shall be able to easily display or communicate the version of the currently installed firmware to the user of the component.	**Met.**
129.	SD 7.5.1 Deployment process	The software deployment process shall follow: a) The new software and firmware components shall be created with an approved software integrity mechanism to generate a factory code or signature for the binary. b) Deployment of the software/firmware to the component shall begin with the download of the software/firmware components which can be via a remote connection or directly connected component on a trusted path (for example a crossover cable or a storage unit added to the component). c) Download of the software/firmware components to the component shall not interrupt the continued operation of the component as intended and not create a safety hazard unless an indicator is visible that the component is in an upgrade process. d) The component may allow the erase of the audit log via operator intervention to allow for download of the software only if at a minimum, the component should start the new log with a record of the log erasure including the timestamp, and authenticated means and account.	a) Not met. b) Met. c) Not met. d) Not met.
130.	SD 7.5.2	After download of the software, the software shall verify the integrity test of the component. a) If the integrity test fails, the component shall stop the download process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The component shall continue to operate as intended. b) The component shall carry out the integrity check only when the component has received the complete software binary. c) The integrity mechanism shall be included in the software binary and shall not be downloaded separately.	Not met.
131.	SD 7.6 Uninstalling process	During the process of erasing/uninstalling of the old software, and install of the new software the component shall have an indicator of its current status of firmware installation. This indicator shall be both visual and audible if the component has the capability to have a visual signal.	Not met.
132.	SD 7.7.1 Usage of well-established design and pre-configuration requirements	Functionalities that are not needed shall not be installed.	**Met.**
133.	SD 7.7.2	Functionalities that are installed shall have no undocumented capabilities, especially not those that run against the security and privacy interests of the operator (free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorized data forwarding).	**Met.**
134.	SD 7.7.3	The component shall not utilize technologies, protocols and functionalities that are outdated or already recognized as insecure (e.g. SSL 3.0, MD5, or RC4, among others)	**Met.**
135.	SD 7.7.4	The complete component, including extensions and enhancements, must be ready for mitigating known vulnerabilities.	Not met.

136.	SD 7.8 Implementation security	The critical assets used to provide security shall be protected using hardware security. Exception: the requirement may be waived if the component's risk and threat analysis shows that these methods are not required or add no additional protection.	Not relevant[1].

Final results of assessment are presented below.

- *The overall compliance score with the Framework is **16 of 95**[2].*
- *The final SL assigned to the device is **0**.*

5.4. Testing results of the Switch

5.4.1. Description of the device

The third tested device is an Industrial Ethernet Switch suitable for PROFINET and Ethernet/IP networks. The Switch is specifically designed to be used in ICS.

The product has following interfaces:

- Interface: Ethernet (RJ45);
- No. of ports: 8 (RJ45 ports);
- Note on the connection method: Auto negotiation and autocrossing;
- Transmission physics: Copper;
- Transmission speed: 10/100 Mbps;
- Transmission length: 100 m (per segment).

The device supports following functions:

- Basic functions: Store-and-forward switch, complies with IEEE 802.3;
- Management: Web-based management (HTTP/HTTPS):
  - SNMPv1/v2/v3;
  - Command-line interface (Telnet, SSH);
- Diagnostic functions: RMON History:
  - LLDP (Link Layer Discovery Protocol);
  - SNMP-Traps;
  - N:1-Portmirroring;
  - ACD (Address Conflict Detection);
- Filter functions: Quality of Service (8 priority classes):
  - Port-Priorisierung;
  - VLAN (up to 8 VLANs);
  - IGMP Snooping (32 groups);
  - IGMP Query;
  - Auto-Query-Port;
  - Extended Multicast Filtering;
- Redundancy: MRP (Media Redundancy Protocol):
  - RSTP (Rapid Spanning Tree Protocol);
- Additional functions: Transmission of MMS and GOOSE (IEC 61850-8-1)

[1] Could only be tested after installing within a system and performing the risk analysis

[2] For the sake of calculating the compliance score we assume that requirements that are “Unknown” are “Not met”, since no information was found in the documentation or through testing process

- MAC address table: 8k
- IP parameterization: DHCP-Client;
    - DHCP server (port based);
    - BootP;
- PROFINET conformance class: Conformance-Class A;
- Time synchronization: SNTP (Simple Network Time Protocol);
- Status and diagnostic indicators LEDs: US (power supply), 2 LEDs per Ethernet port (Link/Activity and Speed).

The device has a proprietary firmware developed by the vendor installed.

The device has the operating system (OS) Linux 3.14.61-rt64 installed. The central processing unit (CPU) installed in the device is unknown, no information was found. The architecture is MIPS32r2.

5.4.2. Assessment results

The testing results for the Switch are presented in Table 8. Testing results of the Switch.

Information about compliance for a number of requirements was received from the vendor. As was stated by the vendor they are aware of the need to comply with the security requirements, specifically requirements in IEC62443-4-2 and currently are working on securing their devices accordingly. Unfortunately, currently existing devices (including the tested device) were not designed to include specific security features stated in the standard.

Table 8. Testing results of the Switch

#	Security requirement name	Security requirement	Result
1. Identification and Authentication control (IAC)			
1.	IAC 1.1.1 Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	**Met.**
2.	RE (1)	Components shall provide the capability to uniquely identify and authenticate all human users.	Not met.
3.	RE (2)	Components shall provide the capability to employ multifactor authentication for all human user access to the component	Not met.
4.	IAC 1.1.2	Identification and authentication shall not prevent the initiation of the Safety Instrumented Function (SIF).	Not relevant[1].
5.	IAC 1.2.1 Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices). If the component is running in the context of a human user, in addition, the identification and authentication of the human user according to IAC 1.1. may be part of the component identification and authentication process towards other components.	Not met.
6.	RE (1)	Components shall provide the capability to uniquely and securely identify and authenticate itself to any other component.	Not met.
7.	IAC 1.3	Components shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly	Not met.

[1] Could only be tested with the system that includes SIF

	Account management	(management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts).	
8.	IAC 1.4 Identifier management	Components shall provide the capability to integrate into a system that supports the management or identifiers and/or provide the capability to support the management of identifiers directly (support the management of identifiers by user, group, role or control system interface).	Not met.
9.	IAC 1.5 Authenticator management	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	a) Met. b) Met. c) Met. d) Not met.
10.	RE (1)	The authenticators on which the component rely shall be protected via hardware mechanisms.	Not met.
11.	IAC 1.6.1 Wireless access management	A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication	Not relevant.
12.	RE (1)	The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Not relevant.
13.	IAC 1.6.2	Services that are accessible over a wireless interface shall require user authentication prior to access. Exception: Services that report status, do not provide command and control functionality or general use of the component or do not transmit sensitive data or personally identifiable data AND only output status or historical transaction data, etc., may provide unauthenticated access	Not relevant.
14.	IAC 1.7 Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength based on minimum length and variety of character types. The password complexity must be configurable by the administrator and be either technically or procedurally enforced with following password parameters: - minimal password length at least of eight characters (or the maximum length supported by the component); - maximum password length; - minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the component); - minimum and maximum usage period; - prevention of re-use of previous passwords; - maximum number of password changes per time (e.g. per day).	Not met.
15.	RE (1)	Components shall provide, or integrate into a system that provides, the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	Not met.
16.	RE (2)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	Not met.
17.	IAC 1.8 Password protection	If the component uses a user name-and-password mechanism for authenticating users: a) The component shall use a secure mechanism to store the passwords, they shall not be stored in plaintext. b) Authentication error messages provided by the component shall not allow for enumerating valid user names.	a) Not met. b) Met. c) Not met. d) Met.

		d) The component shall protect against dictionary attacks and brute force attacks. e) The component shall have no hardcoded passwords that cannot be removed or altered.	
18.	IAC 1.9 Password changes enforcements	For password-only authentication for interactive user access it shall be possible to change the password at any given to enforce the policy of password's regular update.	**Met.**
19.	IAC 1.10.1 Public key infrastructure certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance commonly accepted best practices or obtain public key certificates from an existing PKI.	Not relevant.
20.	IAC 1.10.2	For high availability control systems, the failure of the certificate authority shall not interrupt essential functions	Not relevant.
21.	IAC 1.11.1 Strength of public key-based authentication	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same ICS environment to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; f) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	Not relevant.
22.	RE (1)	The control system shall provide the capability to protect the relevant private keys via hardware.	Not relevant.
23.	IAC 1.11.2	If the component uses other mechanisms for authentication besides username and password, the mechanism used for authentication shall require as many operations to circumvent as determining the actual mechanism.	Not relevant.
24.	IAC 1.12 Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.	Not met.
25.	IAC 1.13.1 Unsuccessful login attempts	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; or b) generate alerts after a threshold of unsuccessful authentication attempts; c) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.	Not met.
26.	IAC 1.13.2	Accounts used for essential functions shall not be locked out, even temporarily.	Not met.
27.	IAC 1.14 System use notification	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	Not relevant.
28.	IAC 1.15.1 Access via untrusted networks	Components that are accessible over a remote interface shall require user authentication prior to access. Exception: Services that report status, do not provide command and control functionality or general use of the component or do not transmit sensitive data or personally identifiable data AND only output status or	**Met.**

	(remote interface)	historical transaction data, etc., may provide unauthenticated access but will need to be documented asper Section 12, Vendor component Risk Management Process.	
29.	IAC 1.15.2	The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks	Not met.
30.	RE (1)	The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.	Not met.
31.	IAC 1.16 Strength of symmetric key-based authentication	For components that utilize symmetric keys, the component shall provide the capability to: a) establish the mutual trust using the symmetric key; s) store securely the shared secret (the authentication is valid as long as the shared secret remains secret); t) restrict access to the shared secret; u) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	Not relevant.
32.	RE (1)	Component shall provide the capability to protect the relevant private keys via hardware mechanisms.	Not relevant.
2. Use control (UC)			
33.	UC 2.1.1 Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least privilege. Access to data shall only be given after successful authentication and authorization. Without successful authentication and authorization, the system shall not allow any activities.	Not met.
34.	RE (1)	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	Not met.
35.	RE (2)	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.	Not met.
36.	RE (3)	Components shall support a supervisor manual override for a configurable time or sequence of events.	Not met.
37.	RE (4)	Components shall support dual approval when action can result in serious impact on the industrial process.	Not met.
38.	UC 2.1.2	Authorization enforcement shall not prevent the initiation of the SIF.	Not relevant[1].
39.	UC 2.2 Usage restriction	Service accounts shall not be usable for interactive logon.	Not relevant.
40.	UC 2.3 Wireless use control	The component shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.	Not relevant.
41.	UC 2.4 Mobile code	In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy must allow, at a minimum, the following actions for each mobile code technology used on the network device: a) control execution of mobile code; b) define which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; c) perform integrity checks on mobile code prior to the code being executed; d) perform authenticity checks to verify the origin of the mobile code prior to the code being executed.	Not relevant.
42.	UC 2.5 Session lock	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability: a) to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation;	**Met.**

[1] Could only be tested with the system that includes SIF

		b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures; c) to comply with session locks requested by the underlying infrastructure (operating system, control system).	
43.	UC 2.6.1 Remote session control	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity , manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	**Met.**
44.	UC 2.6.2	At no time shall the use of remote access compromise the integrity of the component or change the intended use of the component.	**Met.**
45.	UC 2.6.3	If a component allows remote access, the component shall be able to operate continuously, automatically or remotely without causing a safety hazard and the component shall signal its remote operation visibly on the component.	**Met.**
46.	UC 2.6.4	If a local action is initiated on the component, it shall take precedence and priority over a remote action that occurs at the same time.	**Met.**
47.	UC 2.6.5	If a communication session over a remote interface is lost or terminated, the component shall require renewed authentication prior to allowing access over the remote interface. Stored data from the previous session shall not be used to initiate the new session.	**Met.**
48.	UC 2.6.6	The component shall be configurable to allow once a user is authenticated and granted remote access to the component, the component shall reject and record any attempt to setup another remote connection using the same user identity.	Not met.
49.	UC 2.6.7	The transmission of the authentication credential to a component via a remote connection covered on this section cannot be in plaintext or easily intercepted and duplicated unless: a) the information by itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information; b) the transmission path is a trusted path, for example a directly connected physical cable that is not shared by any other system or components.	**Met.**
50.	UC 2.7 Concurrent session control	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	**Met.**
51.	UC 2.8 Use of physical diagnostic and test interfaces	Components shall prevent unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG).	Not relevant
52.	RE (1)	Components shall provide active monitoring of the diagnostic and test interface(s) and generate a log entry when attempts to access these interface(s) are detected.	Not relevant
53.	UC 2.9.1 Control over other ports usage	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by organization, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	**Met.**
54.	UC 2.10 Managing the operators status	The component shall allow the ability for an operator to be disabled, deleted, expired or change of permissions when the component is not in a critical operator-dependent state transition with the operator to be disabled, deleted, expired or permission changed.	Not met.
55.	UC 2.10.2	If the operator is connected and the operator permissions or status changes, the operator shall be disconnected and a record in the audit log shall be made.	Not met.

3. Audit and accountability (AU)			
56.	AU 3.1.1 Auditable events	Components shall provide the capability to generate audit records relevant to security y for the following categories: a) access control (as minimum: successful login attempts, failed access and login attempts); b) request errors; c) control system events; d) backup and restore event; e) configuration changes (e.g. successful and unsuccessful software updates); f) audit log events; g) detected malware (if applicable).	Not met.
57.	AU 3.1.2	The component shall provide the capability to select which auditable events are to be audited by specific parts of the component by administrator.	Not met.
58.	AU 3.2 Audit storage capacity	Components shall: a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; b) provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.	Unknown.
59.	RE (1)	Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.	Unknown.
60.	AU 3.3 Response to audit processing failures	Components shall: a) provide the capability to prevent the loss of essential services and functions in the event of an audit processing failure; b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Unknown.
61.	AU 3.4.1 Timestamps	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	**Met.**
62.	RE (1)	Components shall provide the capability to create timestamps that are synchronized with a system wide time source.	Not met.
63.	RE (2)	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	Not met.
64.	AU 3.4.2	Incorrectly timestamped audit records shall not adversely affect essential functions.	**Met.**
65.	AU 3.5 Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	Not met.
66.	RE (1)	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Not met.
67.	AU 3.5.2	Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time.	Not met.
68.	AU 3.6.1 Protection of audit information	The component shall protect audit information and audit tools (if applicable) from unauthorized access, modification, and deletion.	**Met.**
69.	RE(1)	Components shall provide the capability to store audit records on hardware-enforced write-once media.	Not met.
70.	AU 3.6.2	Unless and until they are transmitted to an external data storage, the component shall store all security-related logs in non-volatile memory and shall not allow non-privileged users to remove or change them.	Not met.
71.	AU 3.7 Audit reduction and report generation	The component shall provide an audit reduction and report generation capability that: a) supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; b) does not alter the original content or time ordering of audit records.	**Met.**

72.	AU 3.8 Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Not met.
73.	RE(1)	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system	Not met.
74.	AU 3.9 Continuous monitoring	When a component provides a security mechanism, that component shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breached in a timely manner.	Not met.
4. System integrity and authenticity (SIA)			
75.	SIA 4.1 Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Not met.
76.	RE(1)	Components shall provide the capability to authenticate information during communication.	Not met.
77.	SIA 4.2.1 Remote communication integrity and authenticity	Components shall ensure the integrity and authenticity of all data communicated over any remote interface. For this, the component shall use security functions complying with the requirements for use of cryptography. Exception: Remote interfaces that report status, do not provide command and control functionality or do not transmit sensitive data, etc., may not ensure integrity and authenticity but will need to be documented.	**Met.**
78.	SIA 4.2.2	Remote connection from different sources shall not disturb the proper function of the component and shall not cause any security flaw.	**Met.**
79.	SIA 4.2.3	Messages sent over a remote connection shall be processed as first in, first out unless a defined message priority or connection is specified by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	**Met.**
80.	SIA 4.2.4	Any remote operation shall be completed before another remote operation can change the operation of the preceding unless specified differently by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	**Met.**
81.	SIA 4.3 Fail-safe mode	Components shall be able to enter a fail-safe mode or an annunciated fail operational mode when a communication failure occurs.	Not met.
82.	SIA 4.4 Protection from malicious code	The network device shall provide for protection from malicious code.	Not met.
83.	SIA 4.5 Security functionality verification	Components shall provide the capability to verify the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Not met.
84.	RE(1)	Components shall provide the capability to support verification of the intended operation of security functions during normal operations.	Not met.
85.	SIA 4.6 Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Not met.
86.	RE(1)	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Not met.

87.	RE(2)	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	Not met.
88.	SIA 4.7 Input validation	Components shall validate the syntax and content of any input that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	**Met.**
89.	SIA 4.8 Deterministic output	Components that directly control a process shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack	**Met.**
90.	SIA 4.9 Error handling	Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.	**Met.**
91.	SIA 4.10 Session integrity and authenticity	Components shall provide mechanisms to protect the integrity and authenticity of communications sessions.	Not met.
92.	RE(1)	Components shall provide the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions).	Not met.
93.	RE(2)	Components shall provide the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.	Not met.
94.	RE(3)	Components shall provide the capability to generate unique session identifiers with commonly accepted sources of randomness.	Not met.
95.	SIA 4.11 Physical tamper resistance and detection	Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Not met.
96.	RE (1)	Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Not met.
97.	SIA 4.12 Provisioning component supplier roots of trust	Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Not relevant.
98.	SIA 4.13 Provisioning asset owner roots of trust	Network devices shall: a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; b) support the capability to provision without reliance on components that may be outside of the device's security zone.	Not relevant.
99.	SIA 4.14 Integrity of the boot process	Network devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	Not met.
100.	SIA 4.15 List of approved integrity mechanisms	The following are approved integrity mechanisms: a) A message authentication code generated on the software and firmware components. b) A digital signature generated on the software and firmware components. c) A hash generated on the software and firmware components, where the hash is published in such a way that it is difficult for an attacker to change.	Not met.
101.	SIA 4.16.1 Genuinuty of the component	The authenticity checking method of the component shall be capable of tracing back software and/or hardware components to their genuine sources.	Not met.
102.	SIA 4.16.2	The authenticity checking method of the component shall protect the properly authorized configuration information assets of the system	Not met.

103.	SIA 4.16.3	Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the system.	Not met.
5. Data confidentiality (DC)			
104.	DC 5.1 Information confidentiality	Components shall: a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; b) support the protection of the confidentiality of information in transit.	Not relevant.
105.	DC 5.2 Information persistence	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	Not relevant.
106.	RE(1)	Components shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.	Not relevant.
107.	RE(2)	Components shall provide the capability to verify that the erasure of information occurred.	Not relevant.
108.	DC 5.3.1 Use of cryptography	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations or in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	**Met.**
109.	DC 5.3.2	Sensitive data (e.g. credentials) may be stored in the component respectively transmitted only in encrypted form.	Unknown.
110.	DC 5.3.3	Only established and well-known encryption algorithms may be used and encryption key lengths, which are considered as safe according to the state-of-art. Proprietary encryption algorithms are not allowed.	**Met.**
111.	DC 5.3.4	The implementation must be done based on well-established encryption libraries to avoid implementation weaknesses.	**Met.**
112.	DC 5.3.5	The key generation must create secure keys and keys must be stored securely.	**Met.**
6. System and communication protection (SCP)			
113.	SCP 6.1 Network segmentation	Components shall support a segmented network as defined in ISA 62443-3-2, as needed, to support the broader network architecture based on logical segmentation and criticality.	**Met.**
114.	SCP 6.1.2	The component enforces approved authorizations for controlling the flow of information within its boundaries and between interconnected systems based on organization-defined information flow control policies.	Not met.
115.	SCP 6.2.1 Zone boundary protection	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk -based zones and conduits model.	Not met.
116.	RE(1)	Deny all, permit by exception. The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).	Not met.
117.	RE(2)	Island mode. The network component shall provide the capability to prevent any communication through the control system boundary (also termed island mode).	Not met.
118.	RE(3)	Fail close. The network component shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).	Not met.
119.	SCP 6.2.2	Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode.	Not met.
120.	SCP 6.3 – General purpose person-to-person communication restrictions	A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.	Not met.

121.	SCP 6.4.1 Denial of service protection	Components shall provide the capability to maintain essential functions in a degraded mode during a DoS event.	**Met.**
122.	SCP 6.4.2	A denial of service (DoS) event shall not prevent the SIF from acting.	Not relevant.[1]
123.	SCP 6.5 Resource management	Components shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	**Met.**
124.	SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	**Met.**
125.	RE(1)	Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Not met.
126.	RE(2)	Components shall provide the capability to perform a local backup independent of system functionality.	**Met.**
127.	SCP 6.7 Control system recovery and reconstitution	Components shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	**Met.**
128.	SCP 6.8 Network and security configuration settings	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	**Met.**
129.	RE(1)	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Not met.
130.	SCP 6.9 Least functionality	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	**Met.**
131.	SCP 6.10 Control system component inventory	Components shall provide the capability to support a control system component inventory, that shall provide the capability to report the current list of installed components and their associated properties.	Not relevant.
132.	SCP 6.11 Security function isolation	The component shall isolate security functions from nonsecurity functions.	Not met.
133.	SCP 6.14 Network disconnect	The network device terminates the network connection associated with a communications session at the end of the session or after a chosen by organization period of inactivity.	Not relevant[2].
7. Security by design (SD)			
134.	SD 7.1.1 Update requirements	Component shall be designed and implemented such that it is possible to perform an update of the component's software, and to roll back an update to the current version during the update process if it fails.	**Met.**
135.	SD 7.1.2	Component shall verify the authenticity and integrity of any software update cryptographically, before installing the update. Component updates shall be possible in an offline environment. This offline component update mode should also still support validation of authenticity and integrity.	Unknown.
136.	SD 7.2 Initial operation	Prior to its initial operation, the component shall require changes of any system defaults that play a role in component security, such as passwords and keys.	**Met.**
137.	SD 7.3 Decomposition requirements	Decommissioning of the component after its use shall allow the ability to completely erase all configuration data, sensitive data and	**Met.**

[1] Could only be tested as a part of the system that includes SIF

[2] Could only be tested as a part of the system with a stated time of inactivity that leads to end of session

		personally identifiable data. Zeroization of this data is acceptable and can be performed as an operation or as a process procedure: a) The operation or procedure shall at least include two steps of overwriting the configuration data, sensitive data and personally identifiable data with data that is not related); b) The operation or procedure shall destroy the configuration data, sensitive data or personally identifiable data from all parts of the component.	
138.	SD 7.4 Display options	Component shall be able to easily display or communicate the version of the currently installed firmware to the user of the component.	**Met.**
139.	SD 7.5.1 Deployment process	The software deployment process shall follow: a) The new software and firmware components shall be created with an approved software integrity mechanism to generate a factory code or signature for the binary. b) Deployment of the software/firmware to the component shall begin with the download of the software/firmware components which can be via a remote connection or directly connected component on a trusted path (for example a crossover cable or a storage unit added to the component). c) Download of the software/firmware components to the component shall not interrupt the continued operation of the component as intended and not create a safety hazard unless an indicator is visible that the component is in an upgrade process. d) The component may allow the erase of the audit log via operator intervention to allow for download of the software only if at a minimum, the component should start the new log with a record of the log erasure including the timestamp, and authenticated means and account.	a) Not met. b) Met. c) Met. d) Met.
140.	SD 7.5.2	After download of the software, the software shall verify the integrity test of the component. a) If the integrity test fails, the component shall stop the download process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The component shall continue to operate as intended. b) The component shall carry out the integrity check only when the component has received the complete software binary. c) The integrity mechanism shall be included in the software binary and shall not be downloaded separately.	Not met.
141.	SD 7.6 Uninstalling process	During the process of erasing/uninstalling of the old software, and install of the new software the component shall have an indicator of its current status of firmware installation. This indicator shall be both visual and audible if the component has the capability to have a visual signal.	**Met**
142.	SD 7.7.1 Usage of well-established design and pre-configuration requirements	Functionalities that are not needed shall not be installed.	**Met.**
143.	SD 7.7.2	Functionalities that are installed shall have no undocumented capabilities, especially not those that run against the security and privacy interests of the operator (free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorized data forwarding).	**Met.**
144.	SD 7.7.3	The component shall not utilize technologies, protocols and functionalities that are outdated or already recognized as insecure (e.g. SSL 3.0, MD5, or RC4, among others)	**Met.**
145.	SD 7.7.4	The complete component, including extensions and enhancements, must be ready for mitigating known vulnerabilities.	Not met.

146.	SD 7.9 Implementation security	The critical assets used to provide security shall be protected using hardware security. Exception: the requirement may be waived if the component's risk and threat analysis shows that these methods are not required or add no additional protection.	Not relevant[1].

Final results of assessment are presented below.

- *The overall compliance score with the Framework is **40 of 123**[2].*
- *The final SL assigned to the device is **0**.*

5.5. Comparison of testing results

The testing results for all tested devices are presented in Table 9. Comparison of final compliance scores.

Table 9. Comparison of final compliance scores

Device	PLC 1	PLC 2	Switch
Compliance score[3]	17 of 95	16 of 95	40 of 123

According to received results of compliance, we can conclude that the Switch is the device with the highest level of security amongst the three tested devices. It has a compliance score 40 of 123. Moreover, the vendor of the device was able to provide additional information about security features and confirmed that they are aware of existing IEC62443 certification schemes and currently working on the compliance process. The strongest aspects of the device's security are Use Control and Security by Design.

5.5.1. Results of compliance with IEC62443-4-2

The only official existing certification schemes for ICS devices are based on IEC62443 series. That is why, we additionally evaluate the compliance of tested devices with IEC62443-4-2 standard (contains component level requirements). Unlike concept of SL introduced in the Framework (a single number), IEC62443 recommends to represent assessment results in a form of SL vector. The security vector is introduced to avoid compressing SL to a single number and use the concept of seven foundational requirements. Each element in the vector represents separate SL for every foundational requirement, thus it has seven elements in total. Security vector is represented in a form: {X X X X X X X}. By using security vector, we can separate SL for different groups of requirements, which helps to understand better weak and strong points of the device from a security perspective.

Final testing results according to IEC62443-4-2 in the form of security vectors for all tested devices are presented in Table 10. SL for IEC62443-4-2.

Table 10. SL for IEC62443-4-2

Device	PLC 1	PLC 2	Switch
Security vector	{0 0 0 0 0 0 0}	{0 0 0 0 0 0 0}	{0 0 0 0 0 0 1}

[1] Could only be tested after installing within a system and performing the risk analysis

[2] For the sake of calculating the compliance score we assume that requirements that are "Unknown" are "Not met", since no information was found in the documentation or through testing process

[3] The number of relevant requirements is different due to different types of devices, originally network devices have more applicable requirements. Moreover, the switch has additional functional capabilities, that are not presented in other tested devices

As we can see, the majority of foundational requirements from IEC62443-4-2 are not fulfilled for all tested devices. However, we can still conclude that the Switch has the highest level of security with at least one foundational requirement completely fulfilled.

The idea of SL vector is presented to support the vendors in assigning the devices to different security zones with different security requirements. The zero level of security means that the device should be either put in the zone where no requirements for security are presented or should be used only in combination with additional security measures that will fulfill the requirements of IEC62443-4-2. The recommendations for possible security measures for the devices are presented in Part 6 of the Master Thesis.

When we combine together in a system devices with different SL vectors, the whole system will automatically inherit the minimum SL vector amongst the devices. For example, if we combine the Switch with SL vector {0 0 0 0 0 0 1} and PLC 1 or PLC 2 with SL vector {0 0 0 0 0 0 0} the overall SL vector for the system will be {0 0 0 0 0 0 0}. This means, that it is not recommended to put in the same security zone the Switch with any of the tested PLC; it is encouraged to put it in a zone with devices with the same SL vector to avoid extra costs for additional security measures that are already in place for the device. At the same time, both tested PLCs could be put in the same security zone with either no requirements for security assigned or in combination with additional security measures in place.

The compliance scores for each device with IEC62443-4-2 are presented in Table 11. Compliance scores with IEC62443-4-2.

Table 11. Compliance scores with IEC62443-4-2

Device	PLC 1	PLC 2	Switch
Compliance score	10 of 70	9 of 70	19 of 75

As we can see, the number of relevant requirements for all three devices is almost the same; at the same time, number of met requirements is almost two times higher for the Switch than for both PLCs. This supports our theory that the Switch has the highest level of security amongst tested devices.

6. Discussion

6.1. Analysis of the results and recommendations

The testing results for three devices showed the overall low level of security. As was discussed in Part 1.2 of the Master Thesis there is a number of reasons for the explanation. Additionally, we discovered, that Majority of ICS devices vendors are still unaware of the need to secure their devices and continue to manufacture unsecure devices. The only vendor of three contacted who replied to answers regarding security features of the device was the manufacturer of the Switch. Moreover, they admitted that they are aware of a security standard IEC62443 and are currently in process of compliance. Unsurprisingly, the device produced by them has the highest compliance score amongst three tested devices and the highest level of security accordingly.

To strengthen security of devices extra measures should be implemented when installing within ICS. Extra security measures could be implemented in a form of dedicated cyber security systems (security solutions), such as identity management systems (IdM), antivirus protection systems or firewalls. Those systems could be implemented in the form of software solutions (e.g. antivirus protection) or hardware solutions (e.g. firewall). To understand what type of security solutions would be sufficient to bring the security level of the devices up to at least SL 1 we need to analyze which requirements are not met for every tested device.

Originally, we have seven groups of requirements in the Framework. For most of those groups one security solution would be enough to cover all included requirements.

The correlation between the groups of the requirements and the possible security solutions is presented in Table 12. Possible security solutions. There exists a number of different solutions offered by different vendors that cover the same security functionality and represent the same class of security solutions. For each suggested class of security solutions we included a possible example; some of them are specifically designed to work within ICS (e.g. industrial firewalls).

Table 12. Possible security solutions

#	**Security solution**	**Example of possible solution**[1]	**Group of the requirement**
1	Identity and access management system (IAM).	SailPoint	1. Identification and Authentication Control (IAC), 2. Use control (UC)
2	Antivirus system	Symantec	2. Use control (UC)
3	Security information and event management (SIEM)	AlienVault Unified Security Management[2]	3. Audit and accountability (AU)
4	File integrity monitoring (FIM)	Tripwire	4. System integrity and authenticity (SIA)
5	Industrial Firewall	Cisco Industrial Security Appliance 3000[1]	6. System and communication protection (SCP)

Some of requirement groups such as Data Confidentiality and Security by Design could not be fulfilled by external systems and can only by implemented within the devices. This means that improvement of security features should be a responsibility of the vendors. As another solution,

[1] The solution has to be assessed to understand if it fully covers the requirements

[2] Specifically designed for ICS

those requirements could be covered within the companies utilizing ICS devices by introducing dedicated policies and procedures. Some of the requirement could be disregarded based on performed by those companies risk analysis (with certain low-level risks being accepted).

6.1.1. Recommendation for the Swotch

To show how additional measures could be implemented to strengthen cyber security of an ICS device, we took as an example the tested device with highest level of security; in our research this is the Switch. We performed analysis of all requirements that are not met for the device to understand what additional measures could be used to cover those requirements. Result of this analysis is presented in Table 13. Recommendations for the Switch. We introduced three types of possible measures:

- system-related (usage of extra security systems) for companies that utilize ICS devices;
- process-related (performing risk analysis, introducing policies and procedures) for companies that utilize ICS devices;
- device-based (changing firmware/hardware of the device) for vendors.

Device-based requirements are only introduced, when there are no possible system- or process-related requirements. As a best practise, usage of all security systems should be supported by related security policies. However, for some requirements we additionally specify the need of enforcing security policies, since the usage of security systems will only be valid with the support of processes within the company.

Table 13. Recommendations for the Switch

#	Name of the requirement	Requirement	Type of the measure	Comment
1. Identification and Authentication control (IAC)				
1.	IAC 1.1.1 RE 1 Human user identification and authentication	Components shall provide the capability to uniquely identify and authenticate all human users.	System-related	IAM system
2.	IAC 1.1.1 RE 2	Components shall provide the capability to employ multifactor authentication for all human user access to the component	System-related + device-based	IAM system + include support within the device
3.	IAC 1.2.1 Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices). If the component is running in the context of a human user, in addition, the identification and authentication of the human user according to IAC 1.1. may be part of the component identification and authentication process towards other components.	System-related	IAM system
4.	IAC 1.2.1 RE 1	Components shall provide the capability to uniquely and securely identify and authenticate itself to any other component.	System-related	IAM system
5.	IAC 1.3 Account management	Components shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly (management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts).	System-related	IAM system
6.	IAC 1.4 Identifier management	Components shall provide the capability to integrate into a system that supports the management or identifiers and/or provide the capability to support the management of identifiers directly (support the management of identifiers by user, group, role or control system interface).	System-related	IAM system
7.	IAC 1.5 Authenticator management	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	Device-based	Include mechanisms to protect authenticators
8.	IAC 1.7 Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength based on minimum	System-related + process-related	IAM system + create and enforce Password Policies

		length and variety of character types. The password complexity must be configurable by the administrator and be either technically or procedurally enforced with following password parameters: - minimal password length at least of eight characters (or the maximum length supported by the component); - maximum password length; - minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the component); - minimum and maximum usage period; - prevention of re-use of previous passwords; - maximum number of password changes per time (e.g. per day).		
9.	IAC 1.7 RE 1	Components shall provide, or integrate into a system that provides, the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	System-related + process-related	IAM system + create and enforce Password Policies
10.	IAC 1.7 RE 2	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	System-related + process-related	IAM system + create and enforce Password Policies
11.	IAC 1.8 Password protection	If the component uses a user name-and-password mechanism for authenticating users: a) The component shall use a secure mechanism to store the passwords, they shall not be stored in plaintext. b) Authentication error messages provided by the component shall not allow for enumerating valid user names. d) The component shall protect against dictionary attacks and brute force attacks. e) The component shall have no hardcoded passwords that cannot be removed or altered.	System-related	IAM system
12.	IAC 1.12 Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.	System-related	IAM system
13.	IAC 1.13.1 Unsuccessful login attempts	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access	System-related	IAM system

		attempts by any user (human, software process or device) during a configurable time period; or b) generate alerts after a threshold of unsuccessful authentication attempts; c) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.		
14.	IAC 1.13.2	Accounts used for essential functions shall not be locked out, even temporarily.	System-related	IAM system
15.	IAC 1.15.2 Access via untrusted networks (remote interface)	The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks	Device-based	Include mechanisms to monitor remote connection
16.	IAC 1.15.1 RE 1	The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.	Device-based	Include mechanisms to provide approval for the remote connection
2. Use control (UC)				
17.	UC 2.1.1 Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least privilege. Access to data shall only be given after successful authentication and authorization. Without successful authentication and authorization, the system shall not allow any activities.	System-related + process related	IAM system + create and enforce Account Management Policies
18.	UC 2.1.1 RE 1	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	System-related	IAM system
19.	UC 2.1.1 RE 2	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.	System-related	IAM system
20.	UC 2.1.1 RE 3	Components shall support a supervisor manual override for a configurable time or sequence of events.	System-related	IAM system
21.	UC 2.1.1 RE 4	Components shall support dual approval when action can result in serious impact on the industrial process.	System-related	IAM system
22.	UC 2.6.6 Remote session control	The component shall be configurable to allow once a user is authenticated and granted remote access to the component, the component shall reject and record any attempt to setup another remote connection using the same user identity.	Device-based	Include mechanisms to be able to reject double connection
23.	UC 2.10 Managing the operators status	The component shall allow the ability for an operator to be disabled, deleted, expired or change of permissions when the component is not in a critical operator-dependent state transition with the operator to be disabled, deleted, expired or permission changed.	System-related	IAM system

24.	UC 2.10.2	If the operator is connected and the operator permissions or status changes, the operator shall be disconnected and a record in the audit log shall be made.	System-related	IAM system
3. Audit and accountability (AU)				
25.	AU 3.1.1 Auditable events	Components shall provide the capability to generate audit records relevant to security y for the following categories: a) access control (as minimum: successful login attempts, failed access and login attempts); b) request errors; c) control system events; d) backup and restore event; e) configuration changes (e.g. successful and unsuccessful software updates); f) audit log events; g) detected malware (if applicable).	Device-based + system-related	Include mechanisms to collect all necessary event +SIEM
26.	AU 3.1.2	The component shall provide the capability to select which auditable events are to be audited by specific parts of the component by administrator.	Device-based + system-related	Include mechanisms to collect all necessary event +SIEM
27.	AU 3.4.1 RE 1 Timestamps	Components shall provide the capability to create timestamps that are synchronized with a system wide time source.	Device-based + system-related	Include mechanisms to collect all necessary event +SIEM
28.	AU 3.4.1 RE 2	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	System-related	SIEM
29.	AU 3.5 Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	System-related	SIEM
30.	AU 3.5 RE 1	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	System-related	SIEM
31.	AU 3.5.2	Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time.	System-related	SIEM
32.	AU 3.6.1 RE 1 Protection of audit information	Components shall provide the capability to store audit records on hardware-enforced write-once media.	Device-based	Include support for hardware storage for logs
33.	AU 3.6.2	Unless and until they are transmitted to an external data storage, the component shall store all security-related logs in non-volatile memory and shall not allow non-privileged users to remove or change them.	Device-based	Include support for storage of logs in non-volatile memory
34.	AU 3.8 Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	System-related	SIEM

35.	RE(1)	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system	System-related	SIEM
36.	AU 3.9 Continuous monitoring	When a component provides a security mechanism, that component shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breached in a timely manner.	System-related	SIEM
4. System integrity and authenticity (SIA)				
37.	SIA 4.1 Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Device-based	Include support for communication protocols that provide integrity of transmitted information
38.	SIA 4.1 RE1	Components shall provide the capability to authenticate information during communication.	Device-based	Include support for communication protocols that provide authenticity of transmitted information
39.	SIA 4.3 Fail-safe mode	Components shall be able to enter a fail-safe mode or an annunciated fail operational mode when a communication failure occurs.	Device-based	Include capability to switch to fail-safe mode during communication failure
40.	SIA 4.4 Protection from malicious code	The network device shall provide for protection from malicious code.	System-related	Antivirus
41.	SIA 4.5 Security functionality verification	Components shall provide the capability to verify the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Device-based + process-related	Include support for verification of security functions + create and enforce Policy for Maintainance
42.	SIA 4.5 RE 1	Components shall provide the capability to support verification of the intended operation of security functions during normal operations.		
43.	SIA 4.6 Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	System-related	FIM
44.	SIA 4.6 RE 1	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	System-related	FIM

45.	SIA 4.6 RE 2	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	System-related	FIM
46.	SIA 4.10 Session integrity and authenticity	Components shall provide mechanisms to protect the integrity and authenticity of communications sessions.	Device-based	Include support for communication protocols that provide integrity and authenticity of communication sessions
47.	SIA 4.10 RE 1	Components shall provide the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions).		
48.	SIA 4.10 RE 2	Components shall provide the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.		
49.	SIA 4.10 RE 3	Components shall provide the capability to generate unique session identifiers with commonly accepted sources of randomness.		
50.	SIA 4.11 Physical tamper resistance and detection	Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Device-based	Include hardware physical tamper resistance and detection mechanisms
51.	SIA 4.11 RE 1	Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Device-based	Include software physical tamper detection mechanisms
52.	SIA 4.14 Integrity of the boot process	Network devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	System-related	FIM
53.	SIA 4.15 List of approved integrity mechanisms	The following are approved integrity mechanisms: a) A message authentication code generated on the software and firmware components. b) A digital signature generated on the software and firmware components. c) A hash generated on the software and firmware components, where the hash is published in such a way that it is difficult for an attacker to change.	System-related	FIM
54.	SIA 4.16.1 Genuinuty of the component	The authenticity checking method of the component shall be capable of tracing back software and/or hardware components to their genuine sources.	System-related	FIM
55.	SIA 4.16.2	The authenticity checking method of the component shall protect the properly authorized configuration information assets of the system	System-related	FIM
56.	SIA 4.16.3	Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the system.	System-related	FIM

6. System and communication protection (SCP)				
57.	SCP 6.1.2 Network segmentation	The component enforces approved authorizations for controlling the flow of information within its boundaries and between interconnected systems based on organization-defined information flow control policies.	System-related	Industrial Firewall
58.	SCP 6.2.1 Zone boundary protection	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk -based zones and conduits model.	System-related	Industrial Firewall
59.	SCP 6.2.1 RE 1	Deny all, permit by exception. The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).	System-related	Industrial Firewall
60.	SCP 6.2.1 RE 2	Island mode. The network component shall provide the capability to prevent any communication through the control system boundary (also termed island mode).	System-related	Industrial Firewall
61.	SCP 6.2.1 RE 3	Fail close. The network component shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).	System-related	Industrial Firewall
62.	SCP 6.2.2	Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode.	System-related	Industrial Firewall
63.	SCP 6.3 – General purpose person-to-person communication restrictions	A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.	System-related	Industrial Firewall
64.	SCP 6.6 RE 1 Control system backup	Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	System-related	FIM
65.	SCP 6.8 RE 1 Network and security configuration settings	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Device-based; or process related	Introduce mechanisms to generate report about currently deployed security settings; or create and enforce Document specifying deployed security settings, include regular update
66.	SCP 6.11 Security function isolation	The component shall isolate security functions from nonsecurity functions.	Device-based	Include support for separation security functions from non-security
7. Security by design (SD)				
67.	SD 7.5.1 Deployment process	The software deployment process shall follow: a) The new software and firmware components shall be created with an approved software integrity mechanism to generate a factory code or signature for the binary.	Device-based	Adjust the firmware deployment process according to the requirement

		b) Deployment of the software/firmware to the component shall begin with the download of the software/firmware components which can be via a remote connection or directly connected component on a trusted path (for example a crossover cable or a storage unit added to the component). c) Download of the software/firmware components to the component shall not interrupt the continued operation of the component as intended and not create a safety hazard unless an indicator is visible that the component is in an upgrade process. d) The component may allow the erase of the audit log via operator intervention to allow for download of the software only if at a minimum, the component should start the new log with a record of the log erasure including the timestamp, and authenticated means and account.		
68.	SD 7.5.2	After download of the software, the software shall verify the integrity test of the component. a) If the integrity test fails, the component shall stop the download process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The component shall continue to operate as intended. b) The component shall carry out the integrity check only when the component has received the complete software binary. c) The integrity mechanism shall be included in the software binary and shall not be downloaded separately.	Device-based	Adjust the firmware deployment process according to the requirement
69.	SD 7.7.4	The complete component, including extensions and enhancements, must be ready for mitigating known vulnerabilities.	Device-based	Include capabilities to mitigate vulnerabilities

6.2. Limitations

During the research project we met a number of limitations that did not allow us to fully explore the topic.

First of all, we started the research by identifying e different regulatory documents within the ICS security field but proceeded further with only five of them as they were considered the most relevant to the research. The choice was made based on the number of criteria, such as the scope, zone of influence, type of requirements and the status of the document. We decided to start with a limited number of standards to have a solid foundation. This foundation will allow us in the future to easily expand the framework with requirements from other standards including the original ones from the list and also emerging ones.

Another major limitation we faced was the lack of support from the vendors of the tested devices. During our research we tried to contact all three vendors to receive some additional information about the security features of the devices, which we could not find in the available documentation, but only one of the vendors replied back. Therefore, we had a “black box”[1] testing approach, leading to the fact that compliance of some requirements is in the status “unknown”.

Additionally, some of the requirement in the Framework even though refer to a single device could only be tested within a larger scope on a system level. This type of testing is out of the scope of the current Master Thesis, since the goal of the testing is to be able to assess separately the compliance of each separate device.

Finally, we had a time limitation for the research of six months. That is why, we were only able to test three devices. Given more time, the research could be expended to evaluate more devices of different types. Additionally, it would provide an opportunity to include more standards in the Framework and build a system to test some of the requirements on the system level.

[1] By “black-box” testing we mean the testing without the knowledge of the exact internal structure of the device and no support from the vendor

7. Conclusion and Future work

7.1. Conclusion

Within the Master Thesis we introduced the Framework for assessing security of ICS devices and evaluated this Framework by performing testing of three different ICS devices within a so-called pilot project. The created framework combines requirements from five different regulatory documents and could be easily expanded further to add requirements from additional documents. The pilot project allowed us to adapt the Framework to real life scenarios and finalize the Framework in a way that it could be used by different actors, such as manufactures of ICS devices, companies utilizing ICS, consultancy companies performing audits for ICS and finally for certification laboratories. To add further value for the Framework we specified what type of documentation and tools are needed to perform assessment of the ICS devices and for each requirement described the testing process.

Originally, to perform our research we identified the main problem we need to address and specified the research question we need to tackle. During our research we answered all stated research question, correlation between research questions and parts of the Master Thesis is presented in Table 2. Correlation between research steps and results presented in the Thesis.

In Part 1 of the Master Thesis we presented motivation and relevance of the research topic, stated the problem that needs to be addressed, introduced main research question and all related sub-question and outlined the structure of the Thesis. We justified the need of creating a single standardized assessment framework by the low maturity level of cyber security within ICS field.

In Part 2 we provided literature overview for ICS cyber security topic and analyzed nine most relevant standards, guidelines and recommendation in the field.

The description of chosen research methodology to answer stated research questions is given in Part 3 of the Master Thesis. The chosen methodology is Design Science research methodology as one of the most common methodologies specifically developed to tackle research questions in the field of Information Technology. Moreover, Part 3 gives the description for six steps that are necessary to perform to answer research questions and develop a solution for a stated problem.

The research results including the final version of the Framework are presented in Part 4. In this part we include the justification of choosing five documents (guidelines, regulations, standards) to create the Framework, description of the overlapping process for the requirements, introduce concept of security levels and methods and tools used for testing process.

In Part 5 we provide the results of the pilot project performed to evaluate the created framework. We present the results of testing for three different ICS devices. Evaluation process allowed us to finalize the Framework by identifying through testing procedure which requirements are not relevant to single devices and could be deleted and requirements with similar meaning that could be merged together.

Finally, in Part 6 we discuss the results of our research and provide recommendation on how to strengthen the security of tested devices by introducing additional security systems and extra measures to be used within the system. Moreover, in this part we analyze the possible limitation that we met during the research process.

7.2. Future research

Possible future work could be identified based on results of discussion and limitations provided in Part 6 of the Master Thesis. As a first step of future research, we could recommend to include in the Framework more requirements from documents that were originally rejected. Three originally identified documents were disregarded as part of research limitation. Even though we can expect that many of the requirements from those document will overlap already included into the Framework ones, it will still increase the value of the Framework. Additionally, new regulatory documents keep emerging on a regular basis, so the Framework should be updated regularly by including new requirements into it.

The documents that we decided not to use for the basic Framework are following:

- NIST Framework for improving Critical Infrastructure Cybersecurity;
- NCSC Checklist security of ICS/SCADA systems.
- Swedish Civil Contingency Agency Guide to increased security in industrial information and control systems.

Moreover, the Framework could be expanded not only for testing ICS devices but for systems in general. In this case, additional requirements on system level could be introduced. Furthermore, to assess whole industrial sites process-related requirements could be added into the Framework. Some of those requirements could be found in the documents mentioned above. This will switch focus of the Framework from being purely relevant for single devices to be used within organizations utilizing ICS in general.

As a further recommendation, additional devices could be tested. For example, another network device (such as a switch) to further compare results of two devices of same type. Additionally, we have not tested any device of host type, this could be done to have testing results for all possible types of devices. This could increase legitimacy of the Framework and suggest new improvements to strengthen the base of the Framework.

Overall, we consider created framework not as a finished work but as a work in progress. The Framework should be treated as a process, and as any process, it needs constant analysis and improvement on a regular basis.

References

1. Definition from https://csrc.nist.gov/glossary/term/industrial-control-system.
2. An abbreviated history of automation & industrial control systems and cybersecurity. E. Hayden, M. Assante, T. Conway (2014). White paper by SANS.
3. W32.Stuxnet Dossier. N. Falliere, L. O Murchu, E. Chien (2011). White Paper by Symantec.
4. TRITON: The first ICS Cyber Attack on Safety Instruments systems. Understanding the Malware, its communications and OT payload. A. Di Pinto, Y. Dragoni, A. Carcano (2018). Black Hat USA 2018 - Research Paper.
5. The State of Industrial Cybersecurity (2018). W. Schwab, M. Poujol. Trend study by Kaspersky.
6. ICS Security: 2017 in Review (2018). White paper by Positive Technologies.
7. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. E. Byres (2004). British Columbia Institute of Technology – Research Paper.
8. Challenges for Securing Cyber Physical Systems. A. A. Cardenas, S. Amin, B.Sinopoli (2013). Department of Electrical Engineering and Computer Sciences. University of California, Berkeley – Research Paper.
9. IEC62443 series. Industrial communication networks – Network and system security. Series of standards (2013-2018). International Electrotechnical Commission.
10. NIST Special Publication 800-82. Revision 2. Guide to Industrial Control Systems Security (2015). National Institute of Standards and Technology.
11. NERC-CIP. Version 5 Critical Infrastructure Protection. Cyber Security Standards. (2011-2018). North American Electric Reliability Corporation.
12. NIST Framework for improving Critical Infrastructure Cybersecurity (2018). National Institute of Standards and Technology.
13. UL2900-2-2. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular requirements for ICS. (2016). Underwriter Laboratories.
14. ENISA. Indispensable baseline security requirements for the procurement of secure ICT products and services (2017). European Union agency for Network and Information Security.
15. Checklist security of ICS/SCADA systems (2018). National Cyber Security Center of the Netherlands.
16. Guide to increased security in industrial information and control systems (2017). Swedish civil contingencies agency.
17. NIST Special Publication 800-53. Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations (2013). National Institute of Standards and Technology.
18. UL 2900-1-1. Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements (2016). Underwriter Laboratories.
19. A Design Science Research Methodology for Information Systems Research. K. Peffers, T. Tuunanen, M. A. Rothenberger (2007). Journal of Management Information Systems. Volume 24 Issue 3, Winter 2007-8, pp. 45-78.
20. Standardized Security Assessment Framework for ICS Devices and pilot project.

Appendix A. Complete testing results for PLC 1

Table 14. Full testing results for PLC 1.

#	Security requirement name	Security requirement	Testing process	Tools/methods used	Result	Explanation
1. Identification and Authentication control (IAC)						
1	IAC 1.1.1 Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Verify that any human interaction with the device via any interface is not possible without prior identification and authentication by trying to connect to the system with the help of specific cable and check if prior identification/ authentication is needed.	Reviewing the documentation. Technical testing.	Not met.	There is password authentication to communicate with the device but no identification. Additionally only one user can work at a time with the device.
2.	RE (1)	Components shall provide the capability to uniquely identify and authenticate all human users.	If the mechanisms for identification and authentication are in place verify that it is possible to log into the device with different user accounts.	Reviewing the documentation. Technical testing.	Not met.	No identifications mechanisms are in place.
3.	RE (2)	Components shall provide the capability to employ multifactor authentication for all human user access to the component	If the mechanisms for identification and authentication are in place verify that it is possible to add the second factor (e.g. SMS code for a mobile phone) to log into the device.	Reviewing the documentation. Technical testing.	Not met.	No identifications mechanisms are in place.

4.	IAC 1.1.2	Identification and authentication shall not prevent the initiation of the Safety Instrumented Function (SIF).	If tested within system verify that during identification and authentication process it is still possible to initiate SIF according to documentation.	Technical testing.	Not relevant[1].	Not tested within the system.
5.	IAC 1.2.1 Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices). If the component is running in the context of a human user, in addition, the identification and authentication of the human user according to IAC 1.1. may be part of the component identification and authentication process towards other components.	Verify in the documentation that the device provides the capability to identify and authenticate itself to other devices. When possible, try to connect to the system a new device and verify that a prior identification/authentication is needed.	Reviewing the documentation. Technical testing.	Unknown.	No information regarding the list of permitted processes was found in the documentation. Could only be technically tested within the system.
6.	RE (1)	Components shall provide the capability to uniquely and securely identify and authenticate itself to any other component.	If the device provides the capability to identify to identify itself and authenticate with any other component, verify that it has a unique identifier for different components by connecting two different devices and verifying that identificators are different.	Reviewing the documentation. Technical testing.	Unknown.	No information regarding the list of permitted processes was found in the documentation. Could only be technically tested within the system.
7.	IAC 1.3 Account management	Components shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly (management of all	Verify if the device provides the capability to manage all user accounts. If it does, try to disable or remove any account using account management and verify if the account was	Reviewing the documentation. Technical testing.	Not met.	There is no identification of the users, only one user can work at a time with the device.

[1] Could only be tested within the system that includes SIF

		accounts by authorized users, including adding, activating, modifying, disabling and removing accounts).	indeed disabled or removed (by trying to connect again using its credentials).			
8.	IAC 1.4 Identifier management	Components shall provide the capability to integrate into a system that supports the management or identifiers and/or provide the capability to support the management of identifiers directly (support the management of identifiers by user, group, role or control system interface).	Verify if the device provides the capability to manage identifiers. I fit does verify that it is possible to manage identifiers by users, roles, interfaces by attempting to assign new capabilities to any role (e.g. restricting any functionality) and verify if the new capabilities were indeed implemented by attempting to perform restricted functions.	Reviewing the documentation. Technical testing.	Not met.	There is no identification of the users, only one user can work at a time with the device.
9.	IAC 1.5 Authenticator management	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	Verify if the device provides the capability to manage authenticators by: a) verifying the existence of authentication settings within the device; b) attempting to change all default authenticators upon installation; c) attempting to change/refresh all authenticators; d) checking how the authenticators are stored within the device and transmitted.	Reviewing the documentation. Technical testing. Analyzing firmware	a) Met. b) Not relevant. c) Met. d)Unknown.	a) initial password can be set after first connection to the device; b) there is no initial password set on the device. c) password can be changed. d) password is transmitted in encrypted form, but it is unknown how it is stored.
10.	RE (1)	The authenticators on which the component rely shall be protected via hardware mechanisms.	Verify that the device provides the capability to use hardware mechanisms for authenticators' protection by reviewing the documentation	Reviewing the documentation.	Not met.	No hardware mechanisms to protect authenticators are in place.
11.	IAC 1.7	For components that utilize password-based	If the device uses password-based authentication verify	Reviewing the documentation.	Not met.	The password requirements are set within the device with minimum 8

	Strength of password-based authentication	authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength based on minimum length and variety of character types.	that the password strength requirements are either set in the device or can be configured by trying to change the password for the weak one.	Technical testing.		characters, no requirements for different types of characters are set. They cannot be changed. The short passwords are not accepted.
12.	RE (1)	Components shall provide, or integrate into a system that provides, the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	If the device uses password-based authentication verify that device does not allow to set as a new password previously used one.	Reviewing the documentation. Technical testing.	Not met.	The device allows to use the previously used password.
13.	RE (2)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	If the device uses password-based authentication verify that it is possible to configure password expiration period.	Reviewing the documentation. Technical testing.	Not met.	The device does not allow to set password expiration period.
14.	IAC 1.8 Password protection	If the component uses a user name-and-password mechanism for authenticating users: a) the component shall use a secure mechanism to store the passwords, they shall not be stored in plaintext; b) authentication error	If the device uses password-based authentication verify that: a) mechanisms to secure the password storage are in place; b) no information regarding usernames is shown during incorrect login process;	Reviewing the documentation. Technical testing.	a) Unknown. b) Not relevant. c) Not met. d) Met.	a) no information found regarding storage of the password; b) no identification mechanisms are in place; c)

		messages provided by the component shall not allow for enumerating valid user names; c) the component shall protect against dictionary attacks and brute force attacks; d) the component shall have no hardcoded passwords that cannot be removed or altered.	c) the password is strong enough to protect against dictionary and brute-force attacks; d) all password could be changed upon installation.			
15.	IAC 1.9 Password changes enforcements	For password-only authentication for interactive user access it shall be possible to change the password at any given to enforce the policy of password regular update	Verify by technical testing by connecting with administrator account that it is possible to change all possible passwords of the component at a given moment.	Technical testing.	**Met**	It is possible to change the password at any moment.
16.	IAC 1.10.1 Public key infrastructure certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance commonly accepted best practices or obtain public key certificates from an existing PKI.	If the system supports PKI certificates, verify in the documentation that PKI functions according to commonly accepted best practices or that key certificates are obtained from existing PKI.	Reviewing the documentation.	Not relevant.	No PKI infrastructure is utilized.
17.	IAC 1.10.2	For high availability control systems, the failure of the certificate authority shall not interrupt essential functions.	Verify by technical testing that if the certificate authority is failed the component continues functioning as programmed.	Technical testing.	Not relevant.	No PKI infrastructure is utilized.
18.	IAC 1.11.1 Strength of public key-based authentication	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same ICS environment to: a) validate certificates by	If the component utilizes public key authentication, verify that: a) all certificates have valid signatures and that the component detects invalid signatures;	Reviewing the documentation. Technical testing.	Not relevant.	No PKI infrastructure is utilized.

		checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; f) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	b) all certificates are issued by trusted CA or with self-signed certificated; c) the component identifies and reports the attempts to provide revoked certificates; d) the component allows the connection with a valid certificate and accepts data from this connection; e) it is possible to map identity to a certain user by checking common or distinguished name; f) check what type of cryptography is used by reviewing the documentation and verify that it is in compliance with DC 5.3.			
19.	RE (1)	The control system shall provide the capability to protect the relevant private keys via hardware.	If the component utilizes public key authentication, verify that it has hardware mechanisms to protect the keys.	Reviewing the documentation.	Not relevant.	No PKI infrastructure is utilized.
20.	IAC 1.11.2	If the component uses other mechanisms for authentication besides username and password, the mechanism used for	If the component is capable of utiliing additional types of authentication rather than password, verify in the documentation that those	Reviewing the documentation.	Not relevant.	No additional authentication mechanisms are in place.

		authentication shall require as many operations to circumvent as determining the actual mechanism.	mechanisms are at least as strong as password protection (e.g. no PIN-code protection).			
21.	IAC 1.12 Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.	If the device uses password-based authentication verify that the password is obfuscated during entering. Attempt to enter wrong credentials to verify that no information that could be used for a brute-force attack on the credentials is revealed.	Technical testing.	Not met.	By default inserted password is obfuscated. But there is an option to show the password by clicking dedicated checkbox.
22.	IAC 1.13.1 Unsuccessful login attempts	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; or b) generate alerts after a threshold of unsuccessful authentication attempts; c) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.	Verify that limited number of failed login attempts lead to a lock of the account / device by performing at least 10 login attempts with incorrect credentials.	Technical testing.	Not met.	After 10 attempts to enter the incorrect password the device becomes blocked and does not allow connecting to it even with a valid password. Meanwhile, turning off and turning back on the power of the device resets it and allow new attempts.
23.	IAC 1.13.2	Accounts used for essential functions shall not be locked out, even temporarily.	Verify that accounts used for essential functions cannot be locked out after trying to insert the incorrect password for 10 times.	Technical testing.	Not met.	We have only one account to connect to the device and it could be locked out after 10 incorrect attempts to provide the password. It is only possible to unlock by turning off and turning back on the power.

24.	IAC 1.14 System use notification	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	If the device provides local human access, verify that there exists a notification about the use of the device prior authentication. Verify that those messages could be changed by the administrator.	Reviewing the documentation. Technical testing.	Not relevant.	No local human access/HMI is possible.
25.	IAC 1.16 Strength of symmetric key-based authentication	For components that utilize symmetric keys, the component shall provide the capability to: a) establish the mutual trust using the symmetric key; s) store securely the shared secret (the authentication is valid as long as the shared secret remains secret); t) restrict access to the shared secret; u) ensure that the algorithms and keys used for the symmetric key authentication comply with DC 5.3 Use of cryptography.	If the device utilizes symmetric key-based authentication, verify that all the requirements are met by reviewing the documentation.	Reviewing the documentation.	Not relevant.	Symmetric key-based authentication is not utilized.
26.	RE (1)	Component shall provide the capability to protect the relevant private keys via hardware mechanisms.	If the device utilizes symmetric key-based authentication, verify that hardware protection mechanisms are in place for private keys.	Reviewing the documentation.	Not relevant.	Symmetric based authentication is not utilized.
2. Use control (UC)						
27.	UC 2.1.1 Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least	If there exist accounts with different access right verify that those differences are actually implemented by logging into the device with 2 different accounts with	Reviewing the documentation. Technical testing.	Not met.	There is no support for creating accounts with different privileges.

		privilege. Access to data shall only be given after successful authentication and authorization. Without successful authentication and authorization, the system shall not allow any activities.	different privileges and trying to perform actions that are allowed for one account and restricted to another.			
28.	RE (1)	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	If there exist accounts with different access right verify that the access policy is implemented within the device correctly by assigning to one of the roles the specific set of responsibilities (by connecting with privileged account) and check if other functionality fort hat user is unavailable.	Reviewing the documentation. Technical testing.	Not met.	There is no support for creating accounts with different privileges.
29.	RE (2)	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.			Not met.	There is no support for creating accounts with different privileges.
30.	RE (3)	Components shall support a supervisor manual override for a configurable time or sequence of events.	Verify that documentation for the device states the authentication mechanisms for a supervisor. Verify that those operations can be manually overridden in the device.	Reviewing the documentation.	Not met.	There is no support for creating accounts with different privileges.
31.	RE (4)	Components shall support dual approval when action can result in serious impact on the industrial process.	Verify in the documentation that there exist functionality that requires dual approval. Verify by technical testing that it is indeed implemented.	Reviewing the documentation. Technical testing.	Not met.	There is no support for dual approval mechanisms.
32.	UC 2.1.2	Authorization enforcement shall not prevent the initiation of the SIF.	If tested within system verify that during authorization process it is still possible to	Technical testing.	Not relevant[1].	Not tested within the system.

[1] Could only be tested within the system that includes SIF

			initiate SIF according to documentation.			
33.	UC 2.2 Usage restriction	Service accounts shall not be usable for interactive logon.	If there exist distinction between user and service accounts, verify by connecting through service account that it is not possible to program the process for the device	Reviewing the documentation. Technical testing.	Not relevant.	There is no support for creating accounts with different privileges.
34.	UC 2.3 Wireless use control	The component shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.	Verify that if the component has the capability to provide an access via wireless communication channels it is possible to monitor this type of access by attempting to login into the device via supported wireless protocol and check that in the logs it is possible to monitor successful and unsuccessful login attempts. Additionally verify that there are restriction in place for password strength and usage of wireless communication by checking the wireless communication settings in the system.	Reviewing the documentation. Technical testing.	Not relevant.	The device does not provide support for wireless communication.
35.	UC 2.4 Mobile code	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device:	Verify that if the device supports the use of mobile code the restrictions are in place: a) check that it is possible to restrict the execution of mobile code by first configuring the device accordingly and next actually attempting to execute any mobile code (e.g. JavaScript);	Reviewing the documentation. Technical testing.	Not relevant.	The device does not support any type of mobile code.

		a) control execution of mobile code; b) control which users (human, software process, or device) are allowed to upload mobile code to the device; c) control the execution of mobile code based on the results of an integrity check prior to the code being executed.	b) check in the documentation that proper mechanisms for checking the origin of the code are in place; c) check that it is possible to restrict mobile code transfer to/from portable and mobile devices by attempting to configure the device accordingly; d) check that all activities regarding usage of mobile code are written in logs.			
36.	RE(1)	The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	If the device supports mobile code, verify that it also supports the integrity check prior execution of the code.	Reviewing the documentation.	Not relevant.	No support for mobile code is presented.
37.	UC 2.5 Session lock	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability: a) to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation; b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures;	Verify that the device provides session lock out after a certain time of inactivity (if no information found in documentation – 30 minutes) or / and after the request of the user.	Reviewing the documentation. Technical testing.	Not met.	The documentation for the device doesn’t contain any information about session lock. The testing showed, that after 1 hour of inactivity the session with the device is not locked.

		c) to comply with session locks requested by the underlying infrastructure (operating system, control system).				
38.	UC 2.6.1 Remote session control	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity , manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	Verify that the device provides the capability to terminate remote session after a certain timer period by attempting to specify time period of 2 minutes of inactivity and check that the session is actually terminated after that period of inactivity. Verify that the session indeed terminates after you perform the termination session activities (e.g. press the certain button). Additionally, verify by monitoring network traffic that in both cases remote sessions are indeed terminated.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote access is presented.
39.	UC 2.6.2	At no time shall the use of remote access compromise the integrity of the component or change the intended use of the component.	If the device supports remote connection, verify by establishing remote connection that while being connected the device keeps functioning as programmed.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote access is presented.
40.	UC 2.6.3	If a component allows remote access, the component shall be able to operate continuously, automatically or remotely without causing a safety hazard and the component shall signal its remote	If the device supports remote connection, verify by establishing remote connection that the device has a visual signal that remote connection is established.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote access is presented.

		operation visibly on the component.				
41.	UC 2.6.4	If a local action is initiated on the component, it shall take precedence and priority over a remote action that occurs at the same time.	If the device supports remote connection, verify by establishing at the same time local and remoted connection and performing simultaneously actions, that action performed from local connection is prioritized. If technical test is not possible, review the documentation for the certain information.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote access is presented.
42.	UC 2.6.5	If a communication session over a remote interface is lost or terminated, the component shall require renewed authentication prior to allowing access over the remote interface. Stored data from the previous session shall not be used to initiate the new session.	If the device supports remote connection, verify after establishing remote connection that it is not possible to connect fot the second time without providing again the authentication information.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote access is presented.
43.	UC 2.6.6	The component shall be configurable to allow once a user is authenticated and granted remote access to the component, the component shall reject and record any attempt to setup another remote connection using the same user identity.	If the device supports remote connection, verify after establishing remote connection that it is not possible to connect with another session with same user credentials.	Reviewing the documentation. Technical testing	Not relevant.	No support for remote access is presented.
44.	UC 2.6.7	The transmission of the authentication credential to a component via a remote connection covered on this	If the device supports remote connection verify in the documentation that	Reviewing the documentation. Technical testing	Not relevant.	No support for remote access is presented.

		section cannot be in plaintext or easily intercepted and duplicated unless: a) the information by itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information; b) the transmission path is a trusted path, for example a directly connected physical cable that is not shared by any other system or components.	credentials are not sent to the device not encrypted.			
45.	UC 2.7 Concurrent session control	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	Verify in the documentation that there is a limited number of concurrent sessions possible for a single user. If possible, verify by network traffic simulation that in case when the limit of possible concurrent sessions (specified in the documentation) is reached the next attempted session is getting blocked.	Reviewing the documentation. Technical testing.	**Met.**	Only one connection session is possible to the device at a time.
46.	UC 2.8 Use of physical diagnostic and test interfaces	Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	If the device has physical factory diagnostic of test interfaces (e.g. JTAG debugging) verify that it is not possible to connect to the device through that interface without providing certain authentication credentials.	Reviewing the documentation. Technical testing.	Not relevant	No physical factory diagnostic and test interfaces are presented.
47.	RE (1)	Embedded devices shall provide active monitoring of	If the device has physical factory diagnostic of test	Reviewing the documentation.	Not relevant	No physical factory diagnostic and test interfaces are presented.

		the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	interfaces (e.g. JTAG debugging) verify by connecting through this interface to the device that information regarding that connection is written in the logs.	Technical testing.		
48.	UC 2.9.1 Control over other ports usage	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by organization, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Analyze the documentation to understand which ports are presented within device and for which functionality they are needed. Verify by port scanning that only necessary ports are actually available.	Reviewing the documentation. Technical testing.	**Met.**	It is possible at any moment to disable any ports within the device by accessing it locally.
3. Audit and accountability (AU)						
49.	AU 3.1.1 Auditable events	Components shall provide the capability to generate audit records relevant to security y for the following categories: a) access control (as minimum: successful login attempts, failed access and login attempts); b) request errors; c) control system events; d) backup and restore event; e) configuration changes (e.g. successful and unsuccessful software updates); f) audit log events; g) detected malware (if applicable).	Verify that the device can create logs with the security events by trying to access it and verify that all the necessary events are written down in the logs.	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
50.	AU 3.1.2	The component shall provide the capability to select which			Not met.	

		auditable events are to be audited by specific parts of the component by administrator.				
51.	AU 3.2 Audit storage capacity	Components shall: a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; b) provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.	Verify that the device has dedicated memory allocation for audit storage by reviewing the documentation. Verify that even after maximum capacity for the logs is reached that the device continues functioning normally by either reviewing the documentation or by technical testing	Reviewing the documentation. Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
52.	RE (1)	Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.			Not met.	
53.	AU 3.3 Response to audit processing failures	Components shall: a) provide the capability to prevent the loss of essential services and functions in the event of an audit processing failure; b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Verify that in case of audit processing failures the device can continue functioning normally by either reviewing the documentation or by technical testing. Verify that the device react to audit processing failures according to accepted industry practices and recommendations by either reviewing the documentation or by technical testing.	Reviewing the documentation. Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
54.	AU 3.4.1 Timestamps	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	Verify that the device provides timestamps for all recorded events by checking out the logs of the device.	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
55.	RE (1)	Components shall provide the capability to create timestamps	If the device provides timestamps for recorded	Technical testing.	Not met.	

		that are synchronized with a system wide time source.	events verify that it is possible to synchronize time with a system time by checking the dedicated settings.			
56.	RE (2)	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	If the device provides timestamps for recorded events verify that it is not possible to change the original timestamp of the event by attempting to perform a change and check how the device behaves.	Technical testing.	Not met.	
57.	AU 3.4.2	Incorrectly timestamped audit records shall not adversely affect essential functions.		Technical testing.	Not met.	
58.	AU 3.5 Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	Verify that the device records the usernames of responsible users for all the events in the logs by checking out the logs of the system.	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
59.	RE (1)	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Verify that the device records the usernames of responsible users for all the events in the logs by checking out the logs of the system.	Technical testing.	Not met.	
60.	AU 3.5.2	Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time.	Verify that the device functions without delays while performing simultaneously a number of actions to generate a lot of records to logs.	Technical testing.	Not met.	
61.	AU 3.6.1 Protection of audit information	The component shall protect audit information and audit tools (if applicable) from unauthorized access, modification, and deletion.	Verify that it is not possible to access the logs with prior authorization process. Verify that even with accessing the logs with a high privileged	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.

			account (administrator) it is not possible to delete or modify the records in the logs.			
62.	RE(1)	Components shall provide the capability to store audit records on hardware-enforced write-once media.	If the device provides protection mechanisms for audit records verify in the documentation that it is possible to store the records on separate media source.	Reviewing the documentation.	Not met.	
63.	AU 3.6.2	Unless and until they are transmitted to an external data storage, the component shall store all security-related logs in non-volatile memory and shall not allow non-privileged users to remove or change them.	If the device provides protection mechanisms for audit records verify in the documentation that audit records are stored in non-volatile memory and cannot be altered by attempting to change the records with a user account.	Reviewing the documentation.	Not met.	
64.	AU 3.7 Audit reduction and report generation	The component shall provide an audit reduction and report generation capability that: a) supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; b) does not alter the original content or time ordering of audit records.	Verify that the device is capable of generating the reports with different parameters by reviewing the settings. Attempt to generate any report and verify that the information in the report correlates with the actual events.	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
65.	AU 3.8 Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Verify that the logs created by the device can only be viewed with read rights and can only be accessed after the authentication process by attempting to view the logs without prior authorization. Verify that it is possible to configure the logs to read-only access rights for all users	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.

			and check if this configuration is indeed implemented by accessing the logs from any legitimate user account and attempting to change/delete any records.			
66.	RE(1)	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system.	Verify that the device is capable of sending the logs to the centralized system by reviewing the documentation.	Reviewing the documentation.	Not met.	
67.	AU 3.9 Continuous monitoring	When a component provides a security mechanism, that component shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breached in a timely manner.	Verify that the device is capable of continuous monitoring of the events by attempting to perform any different actions (that are supposed to be recorded according to documentation) with different accounts and checking that all those events were correctly written down in the logs.	Reviewing the documentation. Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
4. System integrity and authenticity (SIA)						
68.	SIA 4.1 Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Verify by reviewing the documentation that the device supports the capability to protect the integrity of data in transit (e.g. supports secure communication protocols).	Reviewing the documentation.	Not met.	The main communication protocols used in the device are CIP and Modbus, which do not provide extra integrity protection for transmitted information. The specific protocols responsible for providing extra communication integrity are CIP Security and Modbus Security that are not supported by the tested device.
69.	RE(1)	Components shall provide the capability to authenticate information during communication.	Verify by reviewing the documentation that the device is capable of authenticating the information during communication.	Reviewing the documentation.	Not met.	
70.	SIA 4.2.1 Remote communication	The component shall ensure the integrity and authenticity of all data communicated	Verify in the documentation what type of protocols are supported for remoted	Reviewing the documentation.	Not relevant.	No support for remote communication is presented.

	integrity and authenticity	over any remote interface. For this, the component shall use security functions complying with the requirements for use of cryptography. Exception: Remote interfaces that report status, do not provide command and control functionality or do not transmit sensitive data, etc., may not ensure integrity and authenticity but will need to be documented.	communication and check if those protocols are capable of ensuring integrity and authenticity of transmitted data.			
71.	SIA 4.2.2	Remote connection from different sources shall not disturb the proper function of the component and shall not cause any security flaw.	If the device supports remote connection, verify by connecting remotely to the device and performing a number of commands that the device continues to work as programmed and no security incidents occur.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote communication is presented.
72.	SIA 4.2.3	Messages sent over a remote connection shall be processed as first in, first out unless a defined message priority or connection is specified by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	If the device supports remote connection, verify by connecting remotely to the device and performing a number of legitimate commands (e.g. change password, close the connection) that those actions are performed in the order in which they were entered.	Reviewing the documentation. Technical testing.	Not relevant.	No support for remote communication is presented.
73.	SIA 4.2.4	Any remote operation shall be completed before another remote operation can change the operation of the preceding	If the device supports remote connection, verify by connecting remotely to the device and performing a		Not relevant.	No support for remote communication is presented.

		unless specified differently by the manufacturer specifications. Exception: If a remote connection is used for a critical operation in a machine to machine connection, then the remote connection does not have to comply.	number of legitimate commands (e.g. change password, close the connection) that those actions are performed in the order in which they were entered.			
74.	SIA 4.3 Fail-safe mode	The component shall be able to enter a fail-safe mode or an annunciated fail operational mode when a communication failure occurs.	Verify in the documentation, that there is exist a pre-configured fail-safe mode within the device in case of operational or communication failure. Verify by technical testing that in case of communication failure (e.g. disconnecting of Ethernet cable), the device goes to a described fail-safe mode.	Reviewing the documentation. Technical testing	Not met.	No information about possible fail-safe mode was found in the documentation.
75.	SIA 4.4 Protection from malicious code	The embedded device shall provide the capability to protect from installation and execution of unauthorized software.	Verify that the device has any protection mechanisms against malicious code (e.g. code & data integrity mechanisms) by reviewing the documentation for the device.	Reviewing the documentation.	Unknown.	There is no information found in the documentation for the device regarding any possible countermeasures against malicious code execution.
76.	SIA 4.5 Security functionality verification	Components shall provide the capability to verify the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Verify in the documentation that the device is capable of reporting anomalies discovered during FAT, SAT and maintenance.	Reviewing the documentation.	Not met.	No information was found in the documentation about verification process of security functions. No alerts / messages were shown about correctness of security mechanisms during the testing process.

77.	RE(1)	Components shall provide the capability to support verification of the intended operation of security functions during normal operations.	Verify in the documentation that the device is capable of reporting anomalies discovered during normal operations.	Reviewing the documentation.	Not met.	No information was found in the documentation about verification process of security functions. No alerts / messages were shown about correctness of security mechanisms during the testing process.
78.	SIA 4.6 Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Verify that the device supports integrity checks of software and information by reviewing the documentation. Verify that information about those checks is written down into logs.	Reviewing the documentation. Technical testing.	Not met.	Since it is not possible to connect to a password protected device without prior inserting the correct authentication credentials (password), the device is considered to be able to protect against unauthorized changes to software and information at rest. At the same time, since the logs and auditing tools are not supported within the device it is not possible to detect, record and report the attempts to make unauthorized changes.
79.	RE(1)	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Verify that it the device supports authenticity checks of software, information and configuration by reviewing the documentation. Verify that it the device integrity checks of software and information by reviewing the documentation	Reviewing the documentation. Technical testing.	Not met.	No support for integrity checks is presented.
80.	RE(2)	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	If the device supports integrity checks verify in the documentation that it is capable of providing a notification about attempts to make unauthorized changes.	Reviewing the documentation.	Not met.	No support for authenticity checks is presented.
81.	SIA 4.7 Input validation	Components shall validate the syntax and content of any input that is used as an	Review the documentation to analyze the correct possible syntax, length etc. for input	Reviewing the documentation.	**Met.**	The device supports the only type of input – a program that can be uploaded into the device. Prior to

		industrial process control input or input via external interfaces that directly impacts the action of the component.	information. Verify that it is not possible to provide the incorrect input (not according to stated in the documentation) by attempting to provide input with incorrect syntax (e.g. command) and see how the device behaves.	Technical testing.		uploading the program the device verifies its syntax with the hehp of build-in function and reports on found errors.
82.	SIA 4.8 Deterministic output	Components that directly control a process shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack	Verify that there exist predetermined values for outputs of the device when normal operation cannot be maintained.	Reviewing the documentation.	**Met.**	The documentation for the device specifies the variables retention mechanism and the states of outputs while changing from Run to Program mode of the device. In general, all analog and digital output variables hold their last state, but only the analog outputs hold their last state while the digital outputs are off (set to zero). Additionally while downloading the project to the device it is possible to choose to download it with or without project variables.
83.	SIA 4.9 Error handling	Components shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner that does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	Verify by reviewing the documentation that the device is capable of triggering alarms about possible errors. Attempt to trigger all possible errors alarms specified in the documentation to see what information is revealed about the errors and verify that no sensitive information is shown.	Reviewing the documentation. Technical testing.	Not met.	No information was found in the documentation about error handling. During testing process incorrect entering of wrong password (short one) triggered an error message, that revealed that the password should be at least 8 characters.
84.	SIA 4.10 Session integrity and authenticity	Components shall provide mechanisms to protect the integrity and authenticity of communications sessions.	Verify in the documentation what type of protocols are supported for communication and check if those protocols are capable of ensuring	Reviewing the documentation.	Not met.	Supported protocols do not provide integrity and authenticity of communication sessions.

			integrity and authenticity of communication sessions.			
85.	RE(1)	Components shall provide the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions).	If the supported protocols provide integrity and authenticity for communication session additionally check if they invalidate sessions upon user logout.	Reviewing the documentation.	Not met.	Supported protocols do not provide integrity and authenticity of communication sessions.
86.	RE(2)	Components shall provide the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.	If the supported protocols provide integrity and authenticity for communication session additionally check that identifiers for that are system-generated.	Reviewing the documentation.	Not met.	Supported protocols do not provide integrity and authenticity of communication sessions.
87.	RE(3)	Components shall provide the capability to generate unique session identifiers with commonly accepted sources of randomness.	If the supported protocols provide integrity and authenticity for communication session additionally check that identifiers for sessions are generated randomly.	Reviewing the documentation.	Not met.	Supported protocols do not provide integrity and authenticity of communication sessions.
88.	SIA 4.11 Physical tamper resistance and detection	The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Verify that it is not possible to physically penetrate the device without triggering tamper reaction (depending on specific physical tampering protection mechanisms in place).	Reviewing the documentation. Technical testing.	Not met.	No physical tamper resistance and detection mechanisms are in place.
89.	RE (1)	The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall	Verify after attempting to physically tamper the device that the information about this attempt was recorded by checking the logs.	Technical testing.	Not met.	No physical tamper resistance and detection mechanisms are in place.

		be logged as part of the overall audit logging function.				
90.	SIA 4.12 Provisioning component supplier roots of trust	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.	Verify in the documentation what type of key management architecture is in place and are there any protection mechanisms for product supplier keys and “roots of trust”(e.g. secure boot process).	Reviewing the documentation.	Not relevant.	No product suppliers keys or roots of trust are stored within the device.
91.	SIA 4.13 Provisioning asset owner roots of trust	Embedded devices shall: a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; b) support the capability to provision without reliance on components that may be outside of the device security zone.	Verify in the documentation is there a process described for the secure loading of asset owner keys and roots of trust.	Reviewing the documentation.	Not relevant.	No asset owner keys and roots of trust are stored within the device.
92.	SIA 4.14 Integrity of the boot process	Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component’s boot and runtime processes prior to use.	Verify by reviewing the documentation that the device is capable of performing integrity checks of firmware during boot process.	Reviewing the documentation.	Not met.	The device does not perform integrity checks during boot process.
93.	SIA 4.15 List of approved integrity mechanisms	The following are approved integrity mechanisms: a) a message authentication code generated on the software and firmware components; b) a digital signature generated on the software and firmware components; c) a hash generated on the software and firmware	Verify in the documentation if integrity checks are supported, what types of mechanisms are in place and whether they are in compliance with allowed types according to the requirement.	Reviewing the documentation.	Not met.	The device does not perform integrity checks.

		components, where the hash is published in such a way that it is difficult for an attacker to change.				
94.	SIA 4.16.1 Genuinuty of the component	The authenticity checking method of the component shall be capable of tracing back software and/or hardware components to their genuine sources.	Verify in the documentation that the device performs authenticity checks for software and hardware parts and that it is possible to trace back the original source.	Reviewing the documentation.	Not met.	The device does not perform authenticity checks.
95.	SIA 4.16.2	The authenticity checking method of the component shall protect the properly authorized configuration information assets of the component.	If the device supports authenticity checks, verify in the documentation that it is capable of protecting the properly authorized configuration information.	Reviewing the documentation.	Not met.	The device does not perform authenticity checks.
96.	SIA 4.16.3	Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the component.	If the device supports authenticity checks, verify that it is capable of detecting any unauthorized changes in the configuration information.	Reviewing the documentation.	Not met.	The device does not perform authenticity checks.
5. Data confidentiality (DC)						
97.	DC 5.1 Information confidentiality	Components shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and b) support the protection of the confidentiality of information in transit.	Verify by reviewing the documentation that there exist information with explicit read authorization rights and that for this information there exist mechanisms to protect this information. Check that those mechanisms are indeed in place by technical testing.	Reviewing the documentation.	Not relevant.	The device does not support the different access rights.
98.	DC 5.2 Information persistence	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	Verify by reviewing the documentation that there exist information with explicit read authorization rights and that it is possible to remove all this information from the system.	Reviewing the documentation. Technical testing	Not relevant.	The device does not support the different access rights.

			Verify that after removing information with explicit read authorization it cannot be recreated by attempting to delete if first and then attempting to recreate it.			
99.	RE(1)	Components shall provide the capability to prevent unauthorized and unintended information (with explicit read authorization) transfer via volatile shared memory resources.	Verify by reviewing the documentation that there exist information with explicit read authorization, that this type of information is not stored in volatile memory (e.g. RAM chip).	Reviewing the documentation.	Not relevant.	The device does not support the different access rights.
100.	RE(2)	Components shall provide the capability to verify that the erasure of information (with explicit read authorization) occurred.	Verify by reviewing the documentation that there exist information with explicit read authorization. Verify by technical testing that after erasing this type of information from the component, the record is made in the logs by checking the logs.	Reviewing the documentation. Technical testing	Not relevant.	The device does not support the different access rights.
101.	DC 5.3.1 Use of cryptography	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations or in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Verify that traffic out/into the device is encrypted in accordance with requirements of the standard. Verify that documentation includes information about used cryptography: algorithms, key sizes etc.	Reviewing the documentation.	Unknown.	There is no information about what types of cryptographic algorithms are used within the device.
102.	DC 5.3.2	Sensitive data (e.g. credentials) may be stored in the component respectively transmitted only in encrypted form.	Identify by reviewing documentation what types of sensitive data is stored within the device. Verify that it is	Reviewing the documentation.	Unknown.	There is no information about what types of cryptographic algorithms are used within the device.

			stored and transmitted only in encrypted form.			
103.	DC 5.3.3	Only established and well-known encryption algorithms may be used and encryption key lengths, which are considered as safe according to the state-of-art. Proprietary encryption algorithms are not allowed.	Check in the documentation what type of encryption algorithms are used within the device. Verify that those mechanisms are well known and considered safe according to best practices.	Reviewing the documentation.	Unknown.	There is no information about what types of cryptographic algorithms are used within the device.
104.	DC 5.3.4	The implementation must be done based on well-established encryption libraries to avoid implementation weaknesses.	Check in the documentation what type of encryption algorithms are used within the device. Verify that the libraries used for implementation are chosen according to best practices.	Reviewing the documentation.	Unknown.	There is no information about what types of cryptographic algorithms are used within the device.
105.	DC 5.3.5	The key generation must create secure keys and keys must be stored securely.	Check in the documentation what type of encryption algorithms are used within the device. Verify that the keys are created and stored securely.	Reviewing the documentation.	Unknown.	There is no information about what types of cryptographic algorithms are used within the device.
6. System and communication protection (SCP)						
106.	SCP 6.1 Network segmentation	Components shall support a segmented network as defined in ISA 62443-3-2, as needed, to support the broader network architecture based on logical segmentation and criticality.	Verify that it is not possible to access a separated zone of the network from another zone by connecting the testing PC to one zone and trying to ping any device located in another network zone. The prior network configuration is required to perform network segmentation.	Technical testing.	Not relevant[1].	Could not be tested for a single device.
107.	SCP 6.4.1	Components shall provide the capability to maintain essential	Verify that the device can function in a degraded mode	Reviewing the documentation.	**Met.**	The results of stress testing are presented in the Part 5.2 of the

[1] Could only be tested within a system with different network zones

	Denial of service protection	functions in a degraded mode during a DoS event.	in case of DoS attack either by reviewing the documentation or by performing different types of stress testing.	Technical testing.		Report. For all performed tests the device was able to continue functioning as programmed (with some tests leading to a drop of connection).
108.	SCP 6.4.2	A denial of service (DoS) event shall not prevent the SIF from acting.	If tested within system verify that during DoS testing it is still possible to activate SIF according to documentation.	Technical testing.	Not relevant[1].	Not tested within the system.
109.	SCP 6.5 Resource management	Components shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	Review the documentation to identify all the possible security functions supported by the device. Verify by technical testing that the usage of those security functions (e.g. a large number of unsuccessful login attempts) does not interfere with the normal functioning of the device.	Technical testing.	**Met.**	The only security function provided by the device is authentication (password protection), which is not affecting normal functioning of the device and do not lead to resource exhaustion. Technical testing showed, that even 100 failed access attempts within a limited period of time didn't cause crushing of the device.
110.	SCP 6.6 Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	Verify that this is possible to perform a backup for the device and that the backup could be successfully restored. Verify that during process of creating / uploading existing backups the device keeps functioning in normal state without errors. If tested within the system verify that it is possible to set the device to participate in a level-system backup.	Technical testing.	Not met.	The device only supports the logging and auditing functionality with the support of external hardware plug-in that is out of scope of current assessment.
111.	RE(1)	Components shall provide the capability to validate the integrity of backed up information prior to the	If it is possible to perform backup for he device, verify in the documentation that the	Reviewing the documentation.	Not met.	

[1] Could only be tested within the system that includes SIF

		initiation of a restore of that information.	device performs prior integrity checks for backups.			
112.	RE(2)	Components shall provide the capability to perform a local backup independent of system functionality.	Verify that this is possible to perform a backup for the device and that the backup could be successfully restored. Verify that during process of creating / uploading existing backups the device keeps functioning in normal state without errors.	Technical testing.	Not met.	
113.	SCP 6.7 Control system recovery and reconstitution	Components shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	Verify that the device keep previous configuration after possible failures by first pre-configuring the device (e.g. uploading user program, setting static IP address and password protection), switching off the power, turning power back on and ensuring that the device keeps a pre-configured state.	Technical testing.	**Met.**	After turning off and turning on power from a functioning device it was able to recover the previous uploaded user program and configuration (including authentication requirements).
114.	SCP 6.8 Network and security configuration settings	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	Verify that documentation for the device specifies default network settings. Verify that those settings are actually implemented on the device by connecting through a dedicated network port (e.g. Ethernet).	Reviewing the documentation. Technical testing.	**Met.**	The documentation states that there exist out-of-the box network settings for the device ("obtain IP address automatically using DHCP", "detect duplicate IP addresses" checked). The testing process showed that default requirements are as specified and could be changed.
115.	RE(1)	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Verify that it is possible to generate report with current deployed security setting by connecting to the component, checking the settings and	Technical testing.	Not met.	

			attempting to generate the report.			
116.	SCP 6.9 Least functionality	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	Verify that documentation for the device specifies what ports and protocols are necessary for normal functioning of the device. Verify that no other ports are open by performing a port scanning of the device. Verify that ports that are not needed can be disabled.	Reviewing the documentation. Technical testing.	**Met.**	The documentation for the device states that there are 2 ports open within the device which is confirmed by scanning process.
117.	SCP 6.10 Control system component inventory	Components shall provide the capability to support a control system component inventory, that shall provide the capability to report the current list of installed components and their associated properties.	Verify by reviewing the documentation for the system is capable of reporting the current list of all installed components. Check by technical testing that the system is indeed capable of providing this information and that this information is sufficient.	Reviewing the documentation.	Not relevant[1].	Could only be tested within the system.
118.	SCP 6.11 Security function isolation	The component shall isolate security functions from nonsecurity functions.	Verify in the documentation that the device separates security functions from nonsecurity functions.	Reviewing the documentation.	Unknown.	No information was found regrading isolation of non-security functions.
7. Security by design (SD)						
119.	SD 7.1.1 Update requirements	Component shall be designed and implemented such that it is possible to perform an update of the component's software, and to roll back an update to the current version during the update process if it fails.	Verify in the documentation that it is possible to update the device firmware without the external help of the vendor. Attempt to perform update of the firmware and verify that it is possible to roll back the update during the process in case of fails.	Reviewing the documentation. Technical testing.	**Met.**	It is possible to update the device firmware with the support of an external software. No errors were triggered during the update process.
120.	SD 7.1.2	Component shall verify the authenticity and integrity of any software update	If it possible to perform an update of the firmware, verify in the documentation that the	Reviewing the documentation.	Unknown.	No information was found regarding integrity and authenticity checks before installing the updates.

		cryptographically, before installing the update. Component updates shall be possible in an offline environment. This offline component update mode should also still support validation of authenticity and integrity.	device is capable of checking the integrity and authenticity of the update prior to installation.			
121.	SD 7.2 Initial operation	Prior to its initial operation, the component shall require changes of any system defaults that play a role in component security, such as passwords and keys.	Check in the documentation if the device has initial If the device has initial defaults (such as passwords or keys) verify by technical testing that it is possible to change them by checking the device settings.	Reviewing the documentation. Technical testing.	Not relevant.	The device does not have any defaults, such as passwords or keys.
122.	SD 7.3 Decomposition requirements	Decommissioning of the component after its use shall allow the ability to completely erase all configuration data, sensitive data and personally identifiable data. Zeroization of this data is acceptable and can be performed as an operation or as a process procedure: a) The operation or procedure shall at least include two steps of overwriting the configuration data, sensitive data and personally identifiable data with data that is not related); b) The operation or procedure shall destroy the configuration data, sensitive data or personally identifiable data	Check in the documentation that it is possible to delete all information from the device. Attempt to erase all possible information from the device to verify that it was indeed deleted.	Reviewing the documentation. Technical testing.	**Met.**	It is possible to erase all information from the device (such as programs, password and configuration data) and reconstitute the device to its original state.

		from all parts of the component.				
123.	SD 7.4 Display options	Component shall be able to easily display or communicate the version of the currently installed firmware to the user of the component.	Verfiy by technical testing that it is possible to check the version of the installed on the device firmware in the device settings.	Technical testing.	**Met.**	It is possible to display the current installed version of the device firmware through settings in CCW.
124.	SD 7.5.1 Deployment process	The software deployment process shall follow: a) The new software and firmware components shall be created with an approved software integrity mechanism to generate a factory code or signature for the binary. b) Deployment of the software/firmware to the component shall begin with the download of the software/firmware components which can be via a remote connection or directly connected component on a trusted path (for example a crossover cable or a storage unit added to the component). c) Download of the software/firmware components to the component shall not interrupt the continued operation of the component as intended and not create a safety hazard unless an indicator is visible that the component is in an upgrade process. d) The component may allow the erase of the audit log via	Verify in the documentation of the device that the process of firmware creation and installation is in compliance with the process described in the requirement.	Reviewing the documentation.	a) Not met. b) Met. c) Not met. d) Not met.	a) There are no codes or signatures fort he binary of the firmware. b) The firmware can be downloaded from a website of the vendor and saved on a trusted path (any path of your choosing). c) While updating the firmware of the device, the device is not capable to function as programmed, there is no any physical indication on the device that it is in update state. d) There is no logging capability present.

		operator intervention to allow for download of the software only if at a minimum, the component should start the new log with a record of the log erasure including the timestamp, and authenticated means and account.				
125.	SD 7.5.2	After download of the software, the software shall verify the integrity test of the component. a) If the integrity test fails, the component shall stop the download process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The component shall continue to operate as intended. b) The component shall carry out the integrity check only when the component has received the complete software binary. c) The integrity mechanism shall be included in the software binary and shall not be downloaded separately.	Verify in the documentation that the device checks the integrity of the component after installation of the new firmware by reviewing the documentation.	Reviewing the documentation.	Not met.	The device does not perform integrity tests for the component after installation of new firmware.
126.	SD 7.6 Uninstalling process	During the process of erasing/uninstalling of the old software, and install of the new software the component shall have an indicator of its current status of firmware installation. This indicator shall be both visual and audible if the component has	Attempt to uninstall the current firmware installed on the device to verify that the device has visual and/or audio indication that uninstall process is in place.	Technical testing.	Not met.	There is no visual or audio signal that the device has uninstall process in place.

		the capability to have a visual signal.				
127.	SD 7.7.1 Usage of well-established design and pre-configuration requirements	Functionalities that are not needed shall not be installed.	Check in the documentation what functionality is in needed for normal functioning of the device. Verify in the setting of the device that no additional functionality that is not specified within documentation is in place.	Reviewing the documentation. Technical testing.	**Met.**	No unspecified in the documentation functionality was discovered during technical testing.
128.	SD 7.7.2	Functionalities that are installed shall have no undocumented capabilities, especially not those that run against the security and privacy interests of the operator (free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorized data forwarding).	For the installed functionalities check in the documentation that what capabilities shall be in place. Verify in the settings for each function that there are no undocumented capabilities preset (e.g. unauthorized data forwarding).	Reviewing the documentation. Technical testing.	**Met.**	No undocumented capabilities for each functions of the device were discovered during technical testing.
129.	SD 7.7.3	The component shall not utilize technologies, protocols and functionalities that are outdated or already recognized as insecure (e.g. SSL 3.0, MD5, or RC4, among others)	Check in the documentation what type of technologies, protocols and functionalities are in place. Verify on the Internet that they are not outdated or considered insecure.	Reviewing the documentation.	**Met.**	The device does not utilize technologies, functions or protocols that are considered insecure.
130.	SD 7.7.4	The complete component, including extensions and enhancements, must be ready for mitigating known vulnerabilities.	Check in the documentation if they state how to mitigate the known vulnerabilities within the device. Check if they describe the process of mitigating newly discovered vulnerabilities.	Reviewing the documentation.	Not met.	Ni information about mitigating of vulnerabilities was found in the documentation.

131.	SD 7.8 Implementation security	The critical assets used to provide security shall be protected using hardware security. Exception: the requirement may be waived if the component's risk and threat analysis shows that these methods are not required or add no additional protection.	If tested within the system after the process of risk analysis, verify that critical identified assets are protected with hardware mechanisms (if stated in risk assessment).	Reviewing the documentation.	Not relevant.	Not tested within the system, no analysis of risk assessment is performed.