VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Atte Vainionpää

A STUDY OF IEC 62443

Tietotekniikka
2016

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Atte Vainionpää
Opinnäytetyön nimi	A Study of IEC 62443
Vuosi	2016
Kieli	englanti
Sivumäärä	27 + 1 liite
Ohjaaja	Antti Virtanen

Opinnäytetyön toimeksiantajana toimi VEO OY ja siinä tutkittiin IEC 62443 -standardin osia 2-3 ja 2-4, sekä ”whitelisting”-menetelmää. Opinnäytetyössä oli tarkoitus tutustua kyseisiin standardin osiin ja käydä läpi alueet, joista VEO:lle saattaisi olla tulevaisuudessa hyötyä automaatiojärjestelmien kyberturvallisuuden parantamisessa, sekä olla mukana projektissa, jossa otetaan käyttöön ”whitelisting” yhteen automaatiojärjestelmään.

Kyberturvallisuuden käsittely vaatii pohjatietoa, jonka vuoksi käytiin läpi keskeisiä kyberturvallisuuden käsitteitä teollisuuden näkökulmasta. Näitä olivat yleisimmät uhat, toimenpiteet niitä varten, sekä verkkorakenne ja ”whitelisting”.

Työssä onnistuttiin kuvaamaan valittujen standardien keskeiset osat kattavasti, ja materiaalista on todennäköisesti hyötyä tulevaisuuden projekteissa.

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Atte Vainionpää
Title	A Study of IEC 62443
Year	2016
Language	English
Pages	27 + 1 Appendix
Name of Supervisor	Antti Virtanen

The client of this thesis was VEO OY. The objective was to study IEC 62443 standard parts 2-3 and 2-4, and whitelisting as a cyber security measure. The aim was to study these parts and focus on material useful to VEO in improving cyber security for future projects, and to be involved in a project where a whitelisting environment is applied to one system.

Studying cyber security needs a strong background, therefore some of the basis of cyber security was covered from industrial point of view. These were the most common threats, countermeasures, networking and whitelisting.

The objective of the thesis was reached and the most important areas of the chosen standard are covered. This material should prove itself useful in future projects.

CONTENTS

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS

BR	Base Requirement
COTS	Commercial Off-The-Shelf
CMMI-SVC	Capability Maturity Model Integration for Services
I/O	Input and Output
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
OS	Operating System
PDF	Portable Document Format
PLC	Programmable Logic Controller
RE	Requirement Enhancement
SCSP	Symantec Critical System Protection
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPC	Vendor Patch Compatibility
XML	Extensible Markup Language
XSD	XML Schema Definition

1 INTRODUCTION

The increasing use of COTS (Commercial Off-The-Shelf) products in the industrial world has vastly increased the possibility of cyber-attacks on industrial systems. The importance of cyber security continues to grow and product manufacturers and system integrators have to ensure that their products fill the security needs of both the customer and the industrial community in question. Industrial communities have created several cyber security standards to be used by product manufacturers and their customers. This thesis focuses on the IEC 62443 cyber security standard parts 2-3 and 2-4.

This thesis is done for VEO Oy. VEO Oy, founded in 1989 under the name Vaasa Engineering Oy, produces industrial automation, control and distribution systems for heavy industry customers, such as power plants.

The goal of the thesis is to study the chosen parts of the standard and cover the parts that matter in designing IACS (Industrial Automation and Control System) and to observe how application whitelisting is used at VEO. IACS, Industrial Automation and Control Systems, are systems used in big industrial sites, e.g. power plants.

2 OVERVIEW OF THE THESIS

This thesis focuses on IEC 62443 Standards 2-3 and 2-4, patch management in IACS and security program requirements for IACS service providers respectfully. This thesis will examine the basics of cyber security but focus on patch management and security program requirements as presented in the standard. The aim of this thesis is to study the two parts of the standard and whitelisting as an alternative to anti-virus software in industrial systems.

IACS is an abbreviation of Industrial Automation and Control Systems, sometimes called ICS, Industrial Control Systems. This abbreviation leaves away automation which at VEO is present in every system. These are large systems that consist of a wide variety of commercial devices, networking, servers and PLCs (Programmable Logic Controller); therefore every system is different but built for the same purpose.

Part 2-3 of the standard is about patch management. It can be used to improve existing patch management systems to match the standard or to establish a new one. The standard goes through the risks involved in patching devices, how to setup a patch management system and gives a standard way for companies to transfer information about their patches. It is aimed at asset owners, service providers and product suppliers.

Part 2-4 of the standard is about security program requirements for an IACS. It provides a comprehensive guide about different security capabilities for a system and using the maturity level system that is also introduced in this section, companies can make lists of requirements for a system they want, and suppliers can make a list to answer how well their systems fill those requirements.

VEO is applying cyber security measures into its control systems and one of the countermeasures currently applied is whitelisting. It is used as an alternative to anti-virus software in industrial environments.

3 CYBER SECURITY

Cyber security is the protection of computer systems, the software, the hardware, and the information stored on them, as well as processes controlled by them /9/. For a long time the industrial world was disconnected from the internet, operating with specialized hardware and software, however this is no longer the case. Increasing use of commercial products and the introduction of the internet to industrial systems has made them vulnerable to every threat faced by commercial users. /1/

3.1 Objectives

The main objective of cyber security is to secure assets. The CIA triad, standing for confidentiality, Integrity and Availability, is an information security model for organizations, and it is widely used /11/, /13/. These can also be applied to cyber security. While cyber security covers the protection to everything connected to information systems, information security is normally meant to cover only information on systems /12/.

Confidentiality is ensuring that data is only accessed by authorized personnel inside the organization. This data is also usually categorized based on how valuable the data is. Confidentiality can be enabled in various ways, using e.g. encryption, passwords, disconnected storage. While most still use a user ID with single password, two-factor authentication is becoming more common. /11/, /13/

"*Integrity* involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle./13/" This means that the data has to be secured when transmitted. This can be accomplished with file permissions, UAC (User Access Control) and file versions. All data should be backed up in case of major system failures. /11/, /13/

Availability means that the data should be easily accessible by authorized personnel. This is best accomplished by constant system maintenance and sufficient commu-

nication bandwidth. Network security equipment can guard against denial-of-service attacks that are meant to slow the communication capabilities of the targeted organization. /11/, /13/

3.2 Threats

It is argued that two of the most common types of threats on a system are non-validated changes to system and accidental actions. Non-validated changes can occur from changes or updates to operating systems, software, hardware and different configurations. Accidents usually happen when a person not familiar with correct procedures operates the system and unwillingly causes a risk. /1/

Threat agents, sometimes called attackers, come in different forms. Examples of threat agents are *insider*, *outsider* and *natural*. Insider is a person who is trusted in the environment, usually working for one of the participating companies. *Insiders* can be malicious or they can pose a threat by bypassing protocols without the intention to do harm. *Outsider* is a person or a group from outside the targeted organization. *Natural* threat agent is a natural event e.g. earthquake or a flood. /1/

Threats are either *passive* or *active*. *Passive* threats consist of different kinds of information gathering. Information gathering can be done simply by engaging in a casual conversation an employee, though this is much easier if the threat agent is also an employee. Outsiders are able to gather information by observing routines. Passive information gathering can also be done digitally, usually by sniffing. Sniffing is a term for monitoring data from a communication stream. Sniffing can be done on many kinds of networks and the equipment for sniffing is widely available. /1/

Active threats require the attacker to do something other than just observing. These types of threats range from disabling communications with denial-of-service attacks to physical attacks on industrial equipment. The most dangerous active threat is malicious code, Stuxnet being the most known amongst the industry. Stuxnet was targeted mainly at the Iranian nuclear enrichment program and is estimated to have destroyed 10% of Iran's centrifuges. Stuxnet was initially spread using a USB flash

drive, and it used several zero-day exploits. “A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software./10/” It was also the first known cyber threat to target PLC’s /6/. These kinds of threats, though extremely dangerous, are also possibly the rarest threat. Complex code is usually developed by an organization and they need reasons to deploy their code to attack. Although these can be developed by small hacker groups, it is much more common for those groups to rely on denial-of-service attacks as they are cheap and easy to execute. The most common threats are the same that everyone faces almost daily. Phishing and spoofed email headers are very common, but they are usually filtered by the email service provider. /1/

3.3 Countermeasures

Preparing against cyber threats can be a hard task. In home systems it is possible to set up a software or hardware firewall and antivirus software. Knowing what sites to visit and what links to click is vital in avoiding malware and viruses. Antivirus software only protects from known viruses and, therefore, protection against zero-day exploits is virtually impossible. If a device has caught a malicious piece of code, several programs can be used to clean your system. Some viruses are persistent and in some extreme cases the whole system has to be reinstalled to get rid of the virus. In the industrial world many more countermeasures can be taken. The countermeasures that should be used depend on the types of threats each asset owner and product supplier faces. Countermeasures come in many different forms. A specific countermeasure is usually needed for a specific threat, e.g. to prevent an outsider sticking an infected USB flash drive into one of the systems computers, the facility needs physical security and access control. Some passive threats like sniffing are very difficult to detect, because they only listen the passing communications. This type of information leakage can be prevented by encrypting the important data and communication. /1/

3.4 Networks

All the devices in an IACS are connected to each other with a network. The network is part of the IACS and designing it properly can increase the security capabilities

of the IACS. For a long time the control system network was disconnected from the internet and used only its own network inside the facility. When control systems were first connected to the internet, they had no security measures. When the need for security was noticed, the control networks were separated from the enterprise network with a single firewall (figure 1.).

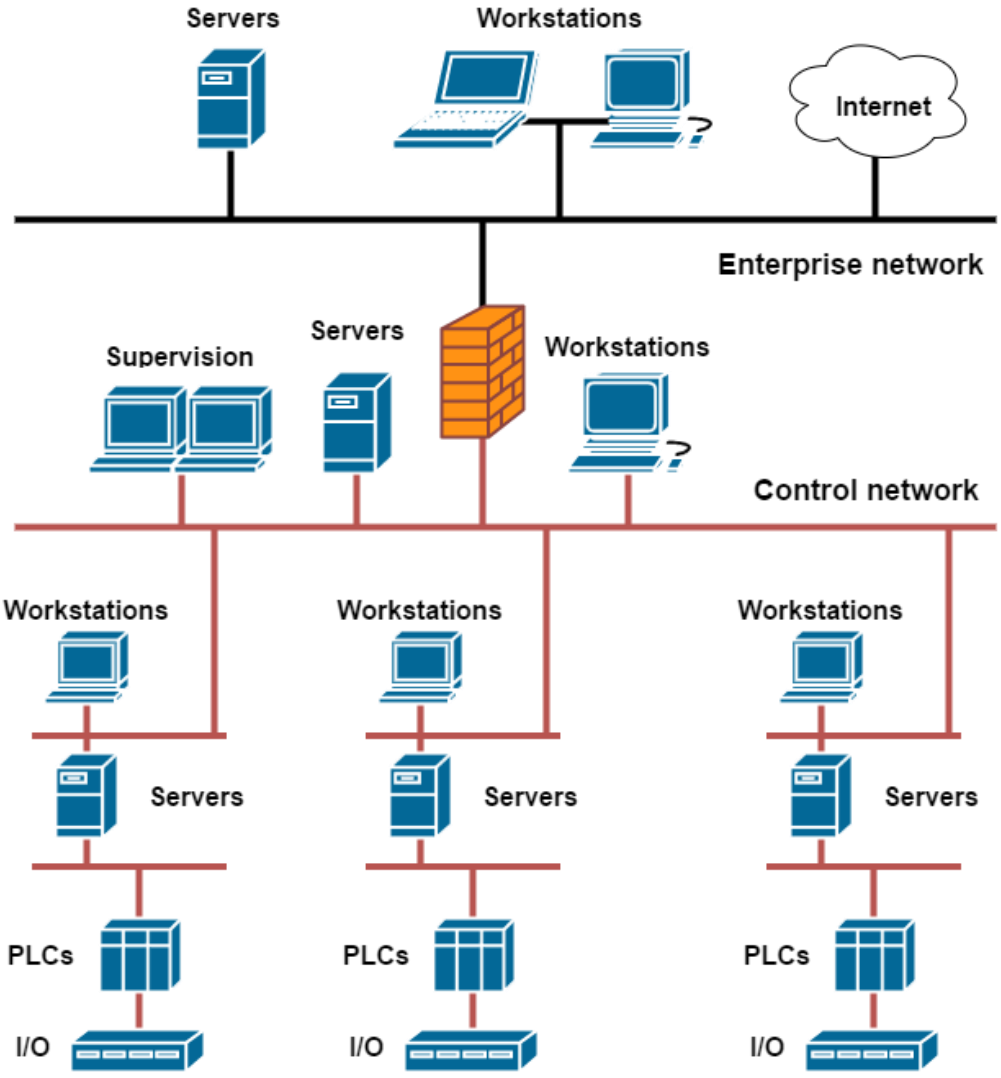

Figure 1: Plant network with one firewall /1/

Breaching this single firewall would compromise the whole system. Modern system networks are built using zones and conduits (figure 2.).

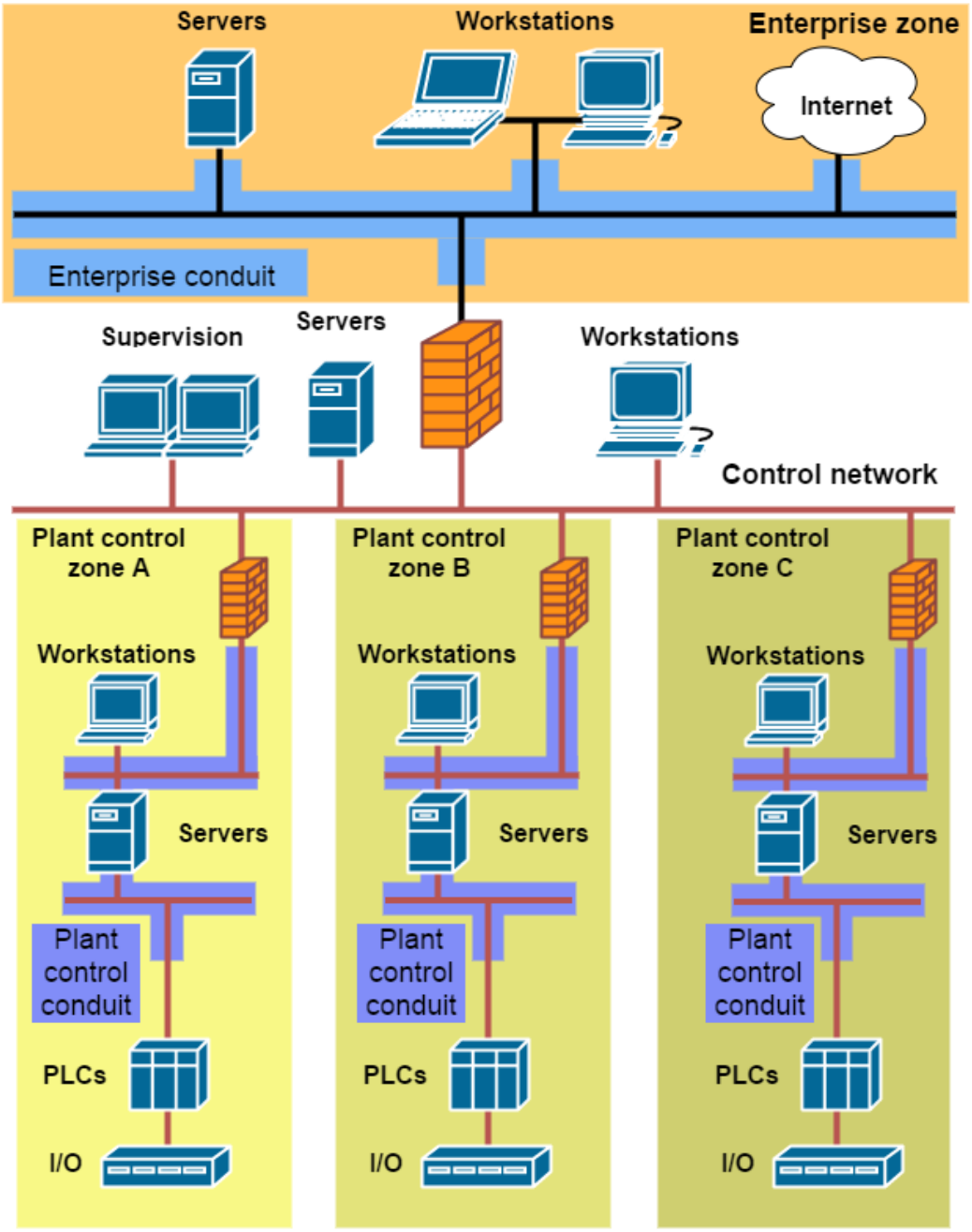

Figure 2: Zoned plant network /1/

The system designer makes a list of all devices in the IACS and divides them into different zones. Zones are defined by grouping assets with similar security requirements. This process is also called network segmentation. The conduits represent network connections between zones. Conduits and zones are protected with firewalls, but while installing a firewall in every place possible may be very secure it will also be expensive. This type of network setup greatly improves the network

security. If it doesn't fully stop invaders it will slow them considerably. Even if they can breach the first layer they still have a way to go to reach any crucial parts of the system. Similar network setup is also possible without physical changes, using virtualization, VLAN. VEO is currently using segmentation in their IACS networks (Figure 3). /8/

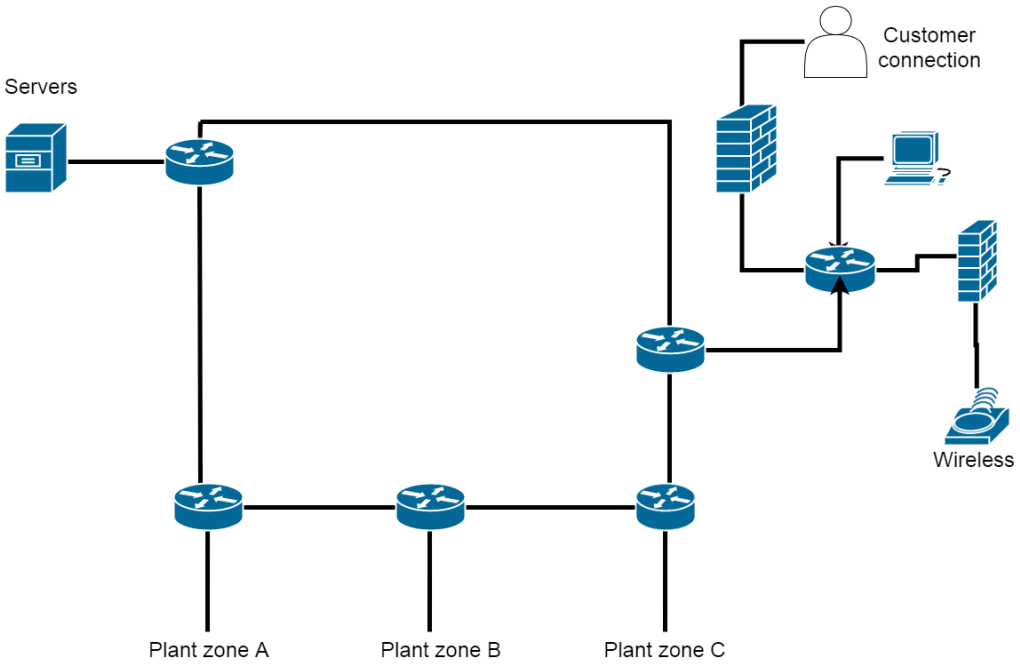

Figure 3: VEO segmentation example

3.5 Whitelisting

Whitelisting exists in different contexts; all references in this text refer to application whitelisting. Whitelisting is considered an alternative to anti-virus software. Anti-virus software has a list of known threats and it compares files in the system to those on the list. When it spots a threat it usually blocks it and notifies the user. This is known as blacklisting. For industrial systems this is not enough, as it doesn't protect against unknown threats. In whitelisting this goes the other way. The system administrator creates a list of files the system is allowed to run, everything else is blocked by default. This provides more security than anti-virus, but not without flaws. Whitelists usually use hashes to identify files, while it's nearly impossible to create two different files with the same hash, some whitelisted applications may

have flaws that allow it to be exploited /5/. Whitelisting can also use other methods besides hash to determine the allowed software. These include files signed by certificates from trusted authorities, and Windows Software Restriction Policies /7/.

Whitelisting is not without its own risks. Some software create additional files when executed and these files are not present when the whitelist is created, therefore they cannot be placed on the list. This may require whitelisting entire folders, which is an enormous hole in the system. One of the most common ways to exploit a whitelisting solution was inserting a worm in e.g. a PDF-file (Portable Document Format) and then opening the PDF-file with a whitelisted program. Some systems were even unable to prevent execution of files when attached to command prompt data stream. /7/

Patching software may also cause big problems in whitelisting as the file database also needs to be updated, for this reason some claim that unpatched systems using whitelisting are more secure than those under scheduled patching. However this was not confirmed in tests. In addition, whitelisting doesn't protect from web-based threats or non-executable files, which are usually spotted by anti-virus software. This leads to the conclusion that whitelisting may not be sufficient in replacing anti-virus systems on its own, but should be used alongside them. /7/

4 IEC 62443 STANDARDS

4.1 General

The standard was originally developed by the International Society of Automation under the name of ISA99 standard and currently utilized in the ongoing development of the IEC 62443 series. The standard currently consists of 13 parts of which two are still in development. In this project we focus on parts 62443-2-3 and 62443-2-4 (figure 4). /1/

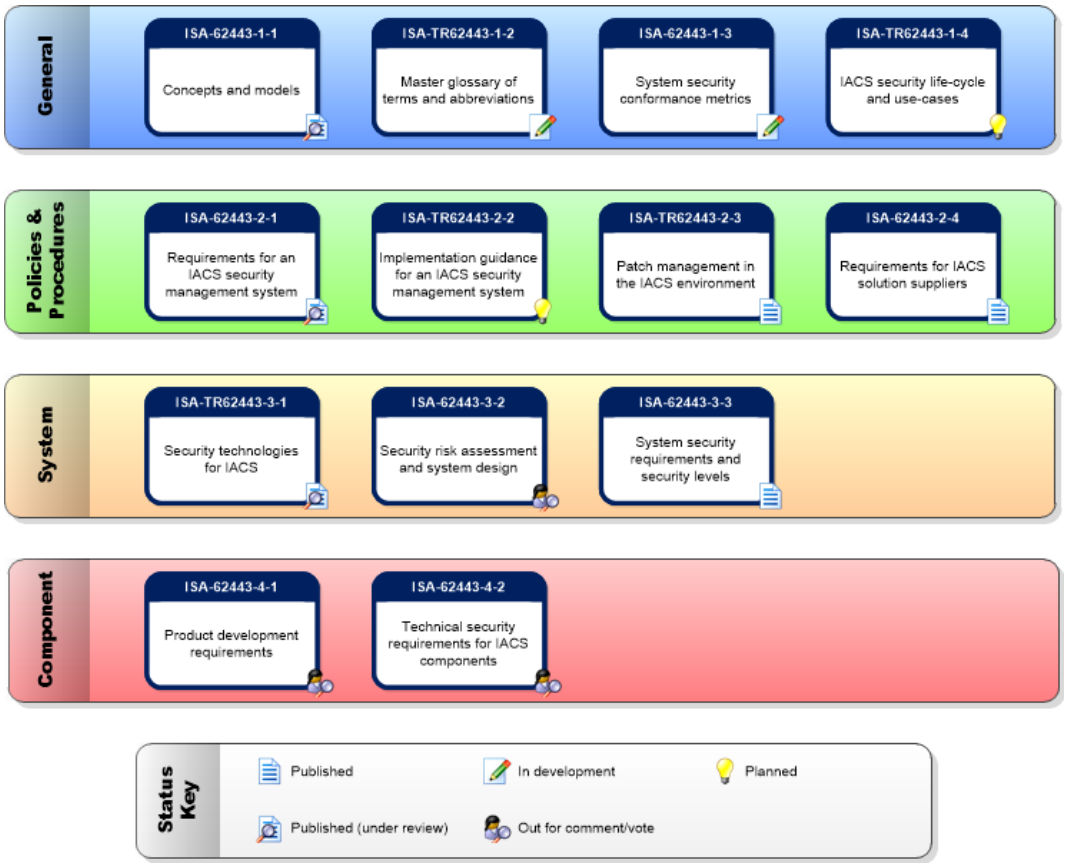

Figure 4. Status of IEC 62443 series of standards /2/

4.2 Patch management in an IACS

Part 62443-2-3 is a technical report on IACS patch management. It can be used by both asset owners and product suppliers to better implement and operate patch management systems and procedures in both existing and future facilities. Patch management takes a lot of time and resources from the parties involved. Each product that is going to be patched has to be tested on a test system to verify that the patch doesn't cause any additional security issues. Backups need to be taken before and after patching from the systems that are about to be patched. After installation, the patches have to be tested on the actual systems before resuming normal operations. Due to the extensive amount of work needed for patching an IACS, the patching is usually done during regular maintenance outages. However, some systems may be so critical that outages are out of the question and therefore they can't be patched at all. The same can be true for obsolete control systems. Asset owners with systems that cannot be patched have to rely on other means of threat mitigation. This can be done e.g. with more strict security policies or additional network security capabilities.

Patch management can lead to several problems in the system. These problems can be incompatibility issues, system performance decrease or even false positives in security software. When vulnerabilities are found in the system, the patch needs to be created and applied. Given the amount of similar systems or devices some product suppliers have, the patching is done case-by-case at the asset locations. Because of this fact, the attackers have the upper hand when vulnerabilities are discovered. Although patching an IACS takes a tremendous amount of work and sometimes means system outages, patching should always be considered. The loss of an IACS system can, in worst cases, result in loss of life. So, as stated in the standard: "Applying patches is a risk management decision."

The standard provides recommended requirements for asset owners and IACS product suppliers regarding patching their IACS associated devices.

One key to good patch management is patch information. As stated previously, patches have to be tested before installation. One major issue is compatibility within

systems; IACS are based on many different systems, OSs, databases and other commercial and non-commercial IT-products. All of these have to be tested before applying new patches to the IACS. In addition, many facilities use products from multiple product suppliers. This adds a staggering amount of complexity when testing patches within the system. This part of the IEC 62443 standard introduces asset owners and product suppliers a standard way to share information about their patches. Vendor patch compatibility (VPC) file is introduced in the standard. VPC files are based on XML and are defined using an XSD file. (Figure 4) VPC files should be named as follows:

Company_patch_compatibility_2016-05-05_01.xml

The first part of this convention is the vendor name, always followed by "patch compatibility". After this, the date the file was released, formatted using ISO 8601. The last number after the date is a possible file number if the company releases multiple files on a single date. /3/

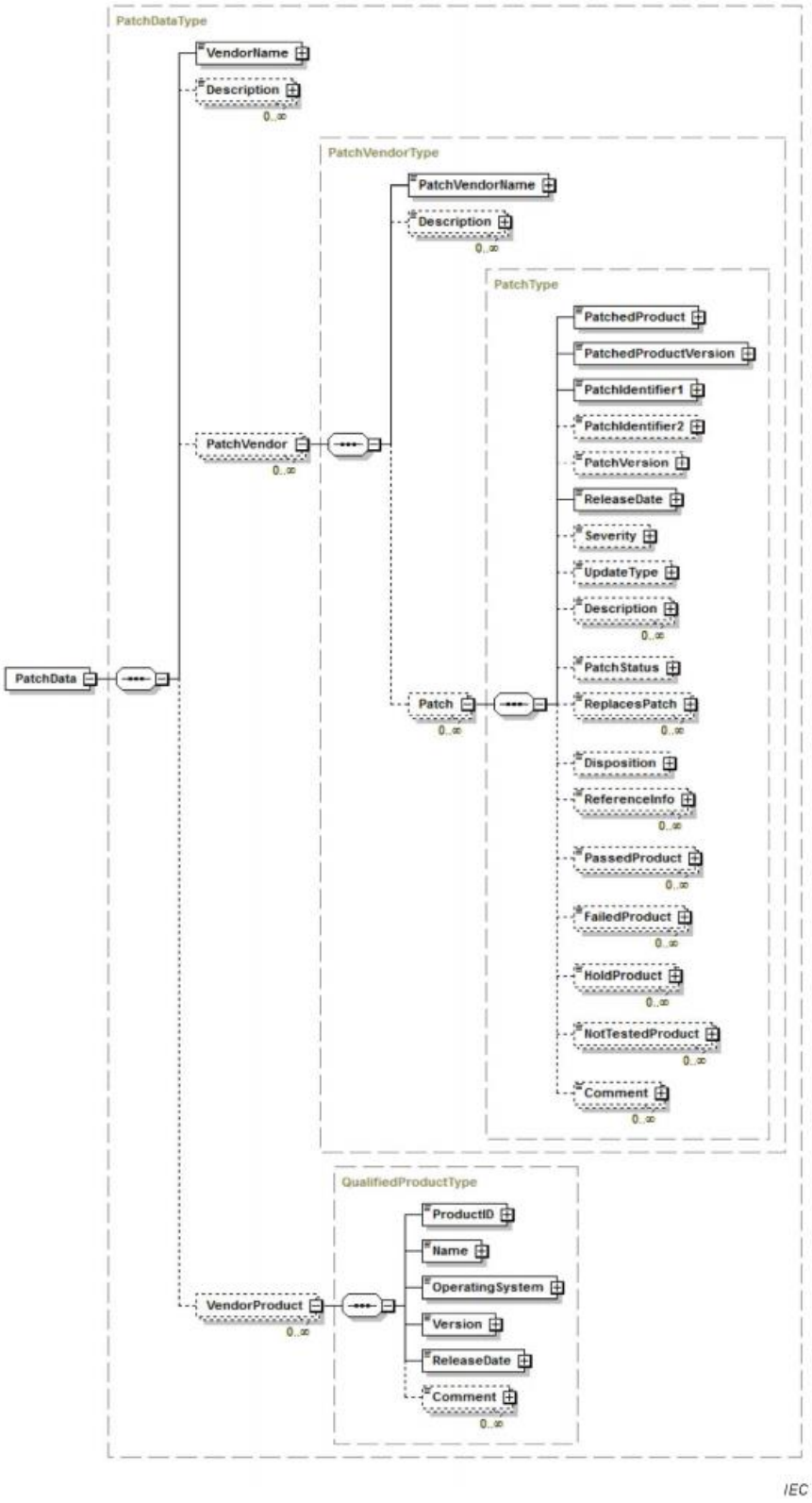

Figure 5: VPC file schema /3/

4.3 Establishing a patch management system

The standard provides guidance on how to establish and maintain a patch management system. This information is crucial to asset owners and as such doesn't concern VEO, which is an IACS service provider. The first step into a patch management system is gathering information about the existing environment. Every piece of software and hardware in the system has to be checked to list versions in use. This information should be kept secure, because it may open new vulnerabilities in the system. The information needed from the system may be gathered manually or with an automated scanning tool. If done properly, this information can be used in determining what parts of the system are vulnerable when a new vulnerability is discovered. The standard introduces multiple ways to gather the data along with a list of data that should be gathered. This list of devices is called an asset list and it should also contain device specific information (Figure 5).

CWA901		
	Make	HP
	Model	HP EliteDesk 800 G1 Tower
	Serial Number	
	Bios Version	L01 v02.65
	OS	Windows 7 SP 1
	OS license	
	HMI license	
	MAC address	EC-B1-D7-35-BB-24

Figure 6: VEO asset list sample

The second phase is project planning and implementation activities, here the asset owner makes a business case, defines roles and establishes a patch deployment and installation infrastructure along with restoration and backup infrastructure. The next phase is procedures and policies for patch management, it includes monitoring, evaluating, testing and installing patches. The last phase, operating a patch management system, is a "run and maintain" process. /3/

4.4 Security program requirements for IACS service providers

Part 2-4 of the IEC 62443 standard defines requirements for security capabilities. These are used to show what capabilities the service provider can provide for their system. Because systems can be very diverse and new products may be introduced,

the requirements in this standard are loose, allowing different kinds of implementations. A predefined set of requirements is called a profile. Asset owners can use these profiles to request a specific set of capabilities from their service provider.

Two kinds of service providers are introduced, integration and maintenance service providers. Integration service providers analyze the environment the IACS is to control, develops the IACS and how it connects to internal and external networks, installs, configures and tests the system. It is also stated in the standard that this definition is loose and it may exclude or include some activities.

The standard introduces maturity levels based on the CMMI-SVC model. These levels are used as benchmarks to state how well the asset owner's requirements are covered by the service provider. There are four maturity levels in the standard: Initial, Managed, Defined (Practiced) and Improving. These are used to define Base Requirements (BRs) and Requirement Enhancements (REs).

These requirements are presented in tables. The tables have eight columns, six of which are indicators and representations, the two last ones describe the requirement. These are explained and shown with an example in Appendix 1.

Using these requirements the asset owner can define exactly what is required from the system it is acquiring and product suppliers can define what their capabilities are. This information can be used as the asset owner to choose the best product supplier and as the product supplier to develop products with more capabilities. /4/

5 WHITELISTING AT VEO

The most recent addition to cyber security capabilities in VEO's systems is whitelisting. The whitelisting is applied on a monitoring system setup that is used with VEO's IACS in various power plants. It is used to monitor everything happening in the facility. The two software packages installed to handle the whitelisting were McAfee Application Control and Symantec Critical System Protection, abbreviated SCSP.

5.1 McAfee Application Control

McAfee Application Control handles whitelisting by creating tasks to apply on the system. Creating these tasks is easy for the user and doesn't require previous experience with the software. The software can be used without management server, but the use of management server allows the software to send reports to the host system in various forms, including system event viewer, system logs, emails and SQL databases. The agent is lightweight and allows patching host system files while operating. The software also allows memory protection. McAfee Application Control has known weaknesses: JavaScript and other scripts can be run, and the agent doesn't monitor network or non-executable files.

5.2 Symantec Critical System Protection

SCSP is a more robust whitelisting tool. It offers protection on everything, including executable and non-executable files, network and registry. However it requires expert level knowledge to be used to its full potential, and the whitelisting process is time consuming and complex. Policy rules cannot be applied without the management tool. All the tools in the software package are protected behind system user passwords. SCSP is not able to send event logs to the host system and patching the host system is not possible without fully disabling SCSP. Its complexity may also leave some vulnerabilities depending on the user knowledge level.

6 RESULTS AND CONCLUSION

The IEC 62443 standard is built to be comprehensive, it provides information to various types of organizations, including asset owners, product suppliers, integration service providers and maintenance service providers. Many of these do not apply to VEO and, therefore, are covered only on the surface. VEO is mainly an integration service provider, it chooses products from product suppliers, builds the IACS which is then handed over to the asset owner. While the standard provides some information directly to integration service providers, it is not nearly enough to fill the thesis from only that point of view. For this reason the information about the standards covered is mostly introductory. In hindsight, other sections of the standard may have proved to be more useful. However, this thesis covers the important areas of these standards from VEO's point of view and should save time when developing future systems if these areas of the standard have to be used.

The aim was also to observe the usage of whitelisting in one of VEO's systems, but the project was paused after the person responsible for the project fell ill. For this reason there is only a recap of the used whitelisting software covered in this thesis.

REFERENCES

/1/ IEC/TS 62443-1-1:2009 Industrial communication networks. Network and system security. Part 1-1: Terminology, concepts and models

/2/ ISA99 Committee Wiki. Accessed 13.4.2016 http://isa99.isa.org/ISA99%20Wiki/Home.aspx

/3/ IEC/TR 62443-2-3:2015 Security for Industrial automation and control systems – Part 2-3: Patch management in the IACS environment

/4/ IEC 62443-2-4:2015 Security for Industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

/5/ Wirt S., Antivirus vs. Whitelisting – Which Should You Use? Accessed 29.5.2016 http://www.ccs-inc.com/blog/article/antivirus-vs.-whitelisting-which-should-you-use

/6/ Kushner D., The Real Story of Stuxnet Accessed 29.5.2016 http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

/7/ Obermeier S., Schierholz R., Hristova A., Securing Industrial Automation and Control Systems Using Application Whitelisting Accessed 29.5.2016 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7005242

/8/ Hauet J., ISA99/IEC 62443: a solution to cyber security issues? Accessed 30.5.2016 http://www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf

/9/ Cybersecurity Basics, University of Maryland Accessed 1.6.2016 http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm

/10/ What is a Zero Day Exploit? Kaspersky lab Accessed 1.6.2016 http://www.kaspersky.com/internet-security-center/definitions/zero-day-exploit

/11/ Scarfone K., Jansen W., Tracy M., NIST Guide to General Server Security Accessed 1.6.2016 http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

/12/ Kissel R., Glossary of Key Information Security Terms Accessed 2.6.2016 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

/13/ confidentiality, integrity, and availability (CIA triad) http://whatis.tech-target.com/definition/Confidentiality-integrity-and-availability-CIA

Req ID	**BR/RE**	**Functional area**	**Topic**	**Subtopic**	**Doc?**	**Requirement description**	**Rationale**
SP.04.02	BR	Wireless	Network Design	Communications	No	The service provider shall have the capability to ensure that wireless protocols used in the Automation Solution are compliant with standards commonly used within the industrial security community and with applicable regulations.	"The capabilities specified by this BR and its REs are used to provide confidence that wireless networks use protocols that have been vetted for use in industrial applications. Having this capability means that the service provider (1) uses a commonly accepted standard wireless technology in the Automation Solution and (2) has an identifiable process that ensures that the wireless technology used is compliant with local regulations."
Requirement ID	Base Requirement/ Requirement Enhancement	Main functional area	Topic addressed by the requirement	Subtopic addressed by the requirement, may have multiple	Documentation required to be provided to asset owner?	Text of the requirement	Background, justification, and other aspects.

Requirement table sample