

Matti-Pekka Nuorva

ELECTRICITY DISTRIBUTION CYBER SECURITY IN GERMAN AND NORTH AMERICAN MARKET AREA

Master's Thesis
Faculty of Information Technology and Communication Sciences
December 2022

ABSTRACT

Matti-Pekka Nuorva: Electricity distribution cybersecurity in German and North American Market Area

Master's Thesis

Tampere University

Master's Degree programme in Electrical Engineering

December 2022

The purpose of this work was to investigate the feasibility of developing a Cyber Security solution for a Bulk Electric System, or its components, that is equally compliant with standardizations of German and North American market area. The purpose for this investigation was to assess this possibility both as a means of enhancing security, and as a valid operational strategy to multinational operators.

For this purpose, two significant sources of market demands from the two market areas, NERC-CIP for USA and BDEW Whitepaper for Germany, were assessed and compared to form a larger set of combined demands and two Case Studies were made to illustrate said demands. The purpose of assessing and comparing the standards was to find which demands were either exclusive to one standard, mutually compatible, or mutually incompatible. The mutually compatible standards were included in the formulated combined demands. No mutually incompatible demands were found. These combined demands were demonstrated in the Case Studies, which were about designing a HMI-PC and arranging Remote Access to said HMI-PC. The combined demands and their significance for the Case Studies were also discussed near the end of the work.

The results of the work were conclusive in showing that the two standards can be combined in a beneficial way. The standard demands were largely compatible with each other. They approached the same topics with similar measures, albeit with different emphases, and did not make significant exclusive demands. As a result, they may be feasibly combined, as shown in the Case Studies.

Keywords: Operational Technology, Electricity Distribution, Cyber security, NERC, CIP, BDEW

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

TIIVISTELMÄ

Matti-Pekka Nuorva: Electricity distribution cybersecurity in German and North American Market Area

Diplomityö

Tampereen yliopisto

Sähkötekniikan DI-tutkinto-ohjelma

Joulukuussa 2022

Tämän työn tarkoituksena oli tutkia mahdollisuutta kehittää kyberturvallisuusratkaisuja sähkövoimajärjestelmälle, tai sen osille, jotka olisivat yhtä kompliantteja sekä pohjoisamerikkalaisten että saksalaisten markkinavaatimusten kanssa. Tarkoituksena oli selvittää olisiko tämä mahdollinen tapa sekä turvallisuuden parantamiseksi että ratkaisuna useilla markkina-alueilla toimiville toimijoille.

Tätä varten kaksi merkittävää markkinavaatimusten lähdetä, pohjoisamerikkalainen NERC-CIP ja saksalainen BDEW Whitepaper, läpikäytiin ja yhdistettiin vaatimuksiltaan, ja kaksi Vase Studya tehtiin näiden vaatimusten havainnollistamiseksi. Tarkoituksena oli löytää vaatimukset jotka olivat joko vain toisessa dokumentissa, keskenään yhteensopivia, tai keskenään poissulkevia. Yhteensopivat vaatimukset sisällytettiin yhdistettyihin vaatimuksiin. Toisensa poissulkevia vaatimuksia ei löytynyt. Yhdistettyjä vaatimuksia havainnollistettiin HMI-tietokonetta ja siihen muodostettavaa etäyhteyttä käsittelevissä Case Studyissä. Yhdistettyjä vaatimuksia ja niiden merkitystä Case Studyille käsiteltiin myös työn loppupuolella.

Työn tulokset osoittivat selvästi, että markkinavaatimusten yhdistäminen on mahdollista ja hyödyllistä. Vaatimukset olivat pääosin yhteensopivat. Vaatimukset käsitelivät pääosin samoja aiheita, mutta eri painotuksin, eivätkä tehneet toisensa poissulkevia vaatimuksia. Tämän seurauksena ne on mahdollista yhdistää kuten näytetty Case Studyissä.

Avainsanat: Operational Technology, Electricity Distribution, Cyber security, NERC, CIP, BDEW

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

TABLE OF CONTENTS

1. INTRODUCTION	1
2. MARKET DEMANDS	3
2.1 North American Market Demands	3
2.2 German Market Demands	4
2.3 Development & Procurement	4
2.4 Secure system design principles	5
2.5 Information Management	6
2.5.1 Transient assets and removable media	7
2.5.2 Data Transfer and Storage	7
2.5.3 Disposal and reuse of Cyber Assets	8
2.6 Network Architecture	8
2.6.1 Cloud Services	9
2.6.2 Virtualized components	9
2.7 System Requirements	10
2.7.1 Hardening	10
2.7.2 Malicious code	11
2.7.3 Encryption	12
2.8 Access Management	13
2.8.1 Electronic Security Perimeter	13
2.8.2 Physical Access management	13
2.8.3 Authentication management	14
2.8.4 Remote Access management	16
2.9 Vulnerability Management & Maintenance	17
2.9.1 Risk Management	18
2.9.2 Vendor products	18
2.9.3 Vulnerability assessment	19
2.9.4 Cyber Security Incidents	19
2.9.5 Patch Management	21
2.9.6 Backup	22
3. HMI CASE STUDY	24
3.1 Standard demands for HMI-PC	24
3.1.1 HMI as part of BES	24
3.1.2 Development & Setup	24
3.1.3 Information management	25
3.1.4 Hardening	26
3.1.5 Malicious code	26
3.1.6 Access Management	27
3.1.7 Electronic Security Perimeter	27
3.1.8 Physical Access management	27
3.1.9 Authentication management	27
3.1.10 Risk Management	28
3.1.11 Maintenance	29
3.2 System Setup	29
3.2.1 Settings	29
3.2.2 Hardening	30

3.2.3	Application whitelisting	30
3.3	Access management.....	31
3.4	System Configuration.....	31
3.4.1	Vulnerability assessment	Error! Bookmark not defined.
3.5	Maintenance	32
3.5.1	Risk management.....	32
3.6	Patch management.....	32
4.	REMOTE ACCESS CASE STUDY	33
4.1	Market demands for Remote Access	33
4.2	Standard demands for the Remote Access system	34
4.2.1	Development & Configuration	34
4.2.2	Access management	35
4.2.3	Hardening	36
4.2.4	Malicious code	36
4.3	Practical considerations	37
4.3.1	Secure architecture and design considerations.....	37
4.3.2	Access Management	38
4.4	System Requirements.....	38
4.4.1	Network Structure	38
5.	DISCUSSIONS	40
5.1	Remote Access.....	42
5.2	Hardening	43
5.3	Malicious code & Malware.....	43
5.4	Authentication Management.....	43
5.5	Baseline Configuration	43
5.6	Information Protection	44
5.7	Patch Management.....	44
6.	CONCLUSIONS.....	45
	REFERENCES.....	46

LYHENTEET JA MERKINNÄT

BDEW	Bundesverband der Energie- und Wasserwirtschaft, German Association of Energy and Water Industries
BES	Bulk Electricity System
CIP	Critical Infrastructure Protection
DMZ	Demilitarized Zone
DoS	Denial of Service
E-ISAC	Electricity Information Sharing and Analysis Center
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
HMI	Human-Machine Interface
IP	Internet Protocol
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NIST-NVD	National Institute for Standards and Technology's National Vulnerability Database
NERC	North American Electric Reliability Corporation
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
USB	Universal Serial Bus
VPN	Virtual Private Network

1. INTRODUCTION

Modern Distribution Automation is a mature technology that is built on information networks. Because of this cybersecurity is an inherent issue of the system, that only becomes more emphasized as automation becomes more extensive and human supervision decreases.

The role of cybersecurity is not only to prevent malicious actions, but also human error. The cybersecurity arrangements must allow both the proper function of the system and various human actions from maintenance and updates to managerial and business decision of the system. This necessitates the use of authorization and authentication methods, which can be compromised for inappropriate use of the system. Cybersecurity is therefore not just a matter of technical solutions, but also of policy and information management.

Like any technical field, the established best-practices of cybersecurity have increasingly changed into demands enforced by standards and legislation. Both policy and technical solutions have received many forms of standardization, which presents challenges to international operators that seek to provide solutions to operators on different market areas. One solution is to tailor every project to the specific demands of both the customer and their market area, but this is time consuming and requires the supplier start from scratch every time.

An easy solution to having to cater to multiple market areas is baseline solution that covers the demands of the supplier's most common market areas as thoroughly as possible, which may then be tailored to the specific demands of the customer and customer's market area. As market demands of different market areas may spring from different sources, they may have little common ground. As shown in Figure 1 they may cover entirely different topics, and when they do cover the same topics, they may do so in a contrary or complementary manner. For that, an international operator wants to find to what degree the standard demands are compatible, and how to cover the mutually incompatible demands depending on the customer's market area. This approach may also have the side benefit of providing better cybersecurity solutions by complying to a larger set of demands.

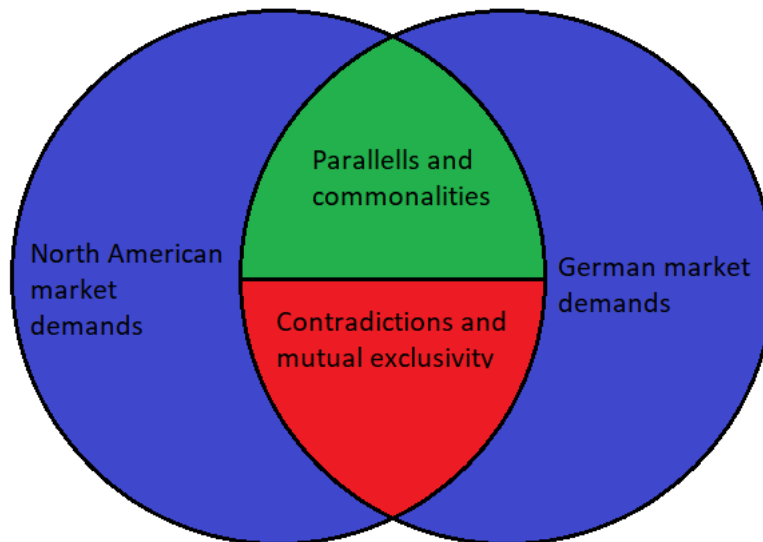


Figure 1: The matter of this thesis

The purpose of this work is to assess the possibility of building a solution that covers cybersecurity market demands for the market areas of United States of America and Federal Republic of Germany. This market area is chosen for its technology-leading status and prominence in the use of Distribution Automation, and therefore it's need for cybersecurity. The idea is to seek out the market demands and compare them as shown in figure 1. The demands that are made in only one of the standards, or which are mutually compatible are discussed for practical solution, and the demands which are mutually exclusive are discussed for the best solution for each respective market area.

For accomplishing the objective of this work both standards are divided to various topics based around the various practical considerations. The market demands of each topic are summarized and compared, and the results of these comparisons gathered for an overview. The overview seeks to find mutually inclusive market demands, and to what degree market demands are mutually exclusive. On the practical side of things, the practical solutions to combined standard demands are discussed. The practical solutions to the found combined standard demands are also discussed, including region-specific solutions to found mutual exclusivities. To demonstrate the feasibility of combined market demands two case studies are made, one for setting up a Human-Machine Interface (HMI) and another one for setting up Remote Access for said HMI, both compliant with the combined standard demands.

2. MARKET DEMANDS

2.1 North American Market Demands

North American Electric Reliability Corporation (NERC) is a non-profit regulatory authority that seeks to reduce the risks to the reliability of the electric grid. NERC enforces and develops standards, trains personnel, regularly assesses reliability, and monitors the bulk power system. NERC is the electric reliability organization of North America, and subject to oversight from Federal Energy Regulatory Commission (FERC) and Canadian Provincial authorities (NERC).

NERC's Critical Infrastructure Protection (CIP, or NERC-CIP) set of standards is applicable to most Bulk Electric power systems in United States of America. The set currently has 13 standards subject to enforcement. The set makes primarily demands for the Responsible Entity, which refers to the owners and operators of all parts of a Bulk Electric System [1]. However, since the Responsible Entity is primarily in charge of compliance with the demands, the Responsible Entities frequently demand that vendor products and Bulk Electricity System (BES) components they procure are as well.

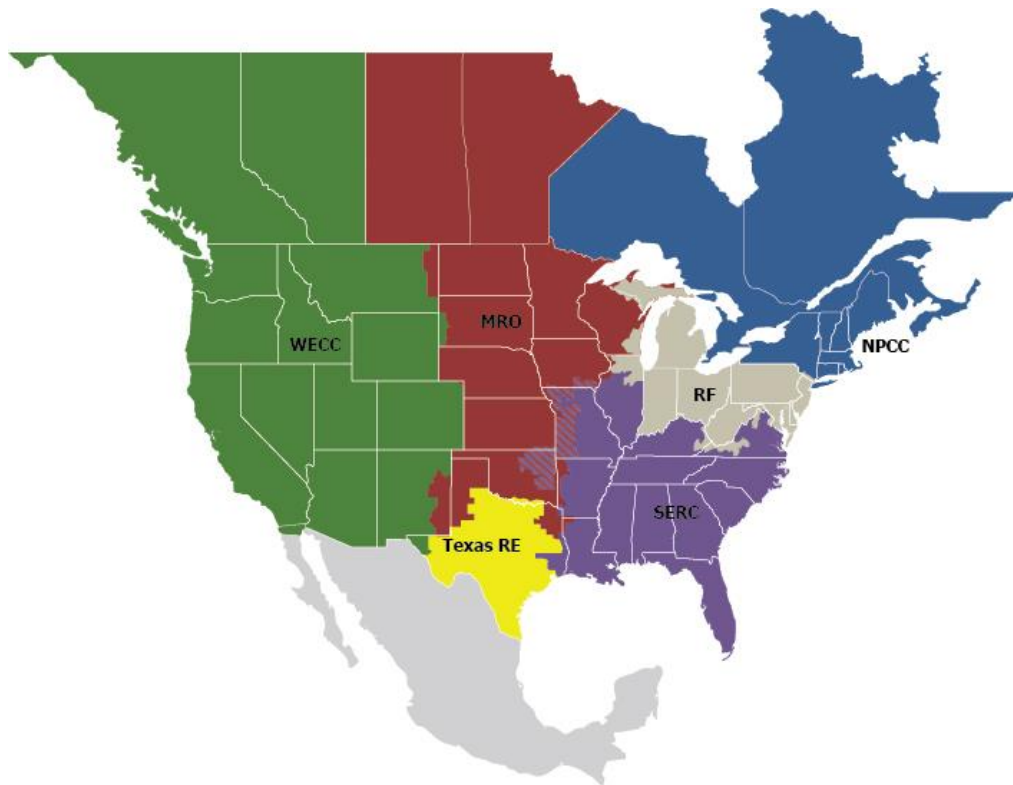


Figure 2: Market area of NERC [11]

Figure 1 shows the market area of NERC divided to its regional organizations. As can be seen on the map, NERC covers the entire area of USA except the State of Alaska, southern areas of Canada, and some areas in northern Mexico.

NERC's importance is widely acknowledged: "NERC's prototype has a significant impact and high reliability for bulk power systems governing and applicable in critical infrastructure" [23]. NERC CIP is also identified being one of the most referred-to pieces of regulation in three articles by Rafal Leszczyna [20][21][22]. These three articles are literature surveys that sought for the most influential cyber security regulation for Smart Grids, an application of electricity distribution operational technology.

2.2 German Market Demands

Bundesverband der Energie- und Wasserwirtschaft, German Association of Energy and Water Industries, is Europe's largest energy industry association, and includes nearly 2000 privately and publicly owned companies from municipal utilities to inter-region operators and covers around 90% of Energy production and electricity networks in Germany [13]. Its whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Requirements for Secure Control and Telecommunication Systems), referred to in this document as BDEW Whitepaper, is a whitepaper of security requirements of Control and telecommunication systems, derived from the ISO/IEC 27001 [18] and ISO/IEC 27019 [19] standards, and revised with Oesterreichs Energie, the representation association of the Austrian Energy Industry [14]. The Whitepaper covers the procurement, development, and implementation of control- and telecommunication systems to Operative Technology. While the whitepaper itself is academically not very referred-to, its basis the ISO 27000 standard family were identified as very referred to in Rafal Leszczyna's three literature surveys [20][21][22].

2.3 Development & Procurement

The supplier shall have the system developed by professionally trained employees that are deemed reliable by the supplier. The system is to be developed according to recognized development standards and quality management processes. Special attention is to be given to defining security requirements, threat modelling, risk analysis, requirements for system design and implementation, secure programming, requirements testing and security checks before commissioning. The supplier is to have a secure development process covering physical, organizational and personal security, verifiable by external audit. A secure programming guide covering security-related requirements and mandating the use of security enhancing compiler options and libraries. Testing plans,

procedures, expectations and results are to be documented as comprehensively as possible. Testing must be done by different people from the developers, and results documented and made available to the client. Approval of the system regarding updates and security patches must follow a specified process. The use of subcontractors requires a written permission from the client, and subcontractors are to be held to same standards as the supplier [12].

2.4 Secure system design principles

BDEW Whitepaper demands the following principles for BES and their components.

- Security by design: System is designed with a focus on security. Attacks and unauthorized actions are considered, consequences of security events are minimized by the system's design.
- Minimal need-to-know: Applications and personnel is only granted the rights required for their purpose.
- Defense-in-depth principle: Security issues are not mitigated by a single protection measure, but by stacked, multi-level and overlapping security measures.
- Redundancy principle: System is designed for failure of individual components not compromising overall security. System is designed to lower the impact of unlimited requests for resources, such as RAM or network bandwidth.

These principles essentially cover all the components and require that all components are designed and procured with security in mind. The need-to-know principle includes only assigning to devices or personnel the rights required for their tasks. Defense-in-depth requires stacked multi-level measures to ensure that a vulnerability in one layer does not endanger the system. Figure 3 gives a simplified example of the staggered and layered defenses: The process and office networks form their own security zones with their own defenses and are separated by a firewall. Both areas rely on multiple active and passive defense measures such as system hardening, malicious code software, and access management. However, the office network is considered contaminated but necessary for the operation of the process network, and therefore kept on the other side of firewalls. Similarly, the redundancy principle demands that a single component being breached should not endanger the entire system, but that components are segregated from one another. This is accomplished by the design on system's network and are therefore covered in chapter 2.6 Network Architecture.

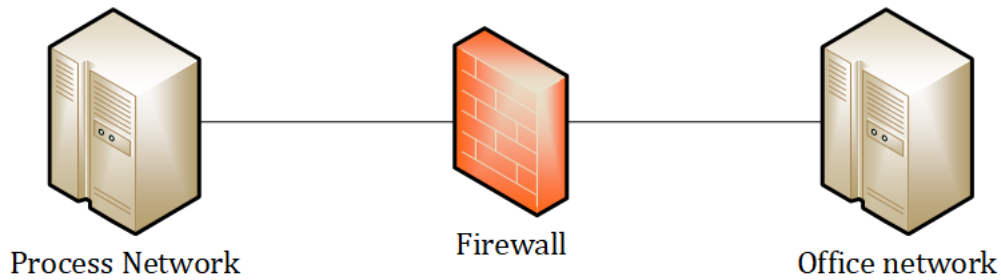


Figure 3 Simplified segmented company network

The client must receive the system's pertinent documentation upon delivery at the latest. All safety features, parameters and measures, and their default options must be included. The documentation must include the entire system architecture, the various components and their possible interaction in general, and sensitive components and their mutual dependencies and interactions. For client-specific customizations all project-specific customizations must be documented for the client in full. [12]

Network structure and configuration documentation shall cover all network connections and employed protocols, Internet Protocol (IP) addresses and ports and all network perimeters part of the system or interacting with it. Any changes must be included as part of overall change management. Expected normal and maximum data transmission rates must also be covered to allow limiting transmission rates for traffic prioritization and prevention of Denial of Service (DoS) issues [12].

2.5 Information Management

Information management means acquirement, custodianship, correct distribution, and disposal of information. It includes topics such as system documentation, use of removable media, storage, transfer and use of information and data, and use of encryption to safeguard information and data. This is commonly modelled as the CIA-triad (Confidentiality, Integrity, Availability). Confidentiality means the information is only received by the designated people, Integrity that the information is not unduly altered, and Availability that the necessary information is available to the people who require it.

Availability tends to be paramount for operational technology, Integrity in the second place, and confidentiality the least important. Information management is important for maintaining the cybersecurity of the system by preventing leaking of vital information such as user credentials, or information that can be used for planning and carrying out cyberattacks, such as system design documents. However, for Operational Technology the proper functioning of the system is paramount, and therefore the availability of infor-

mation must not be hampered by the system's security measures. For this reason various security measures must be designed in such a way that maintaining the integrity and confidentiality of the information do not endanger availability.

2.5.1 Transient assets and removable media

Transient assets are cyber assets that are directly connected to BES, but not designed to be part of any single BES. Because of this transient Cyber Assets can be a temporary part of BES or switched from one BES to another. Removable media similarly refers to any storage device that is designed to be installed and removed from the system while it's running, and transferring executable code between the system and the media. Examples of this are all external drives, from USB-stick drives to external hard-drives, and other memory devices such as different kinds of storage discs from floppy-disks to CD-ROM:s. Cloud Services such as Dropbox technically count as removable media, but their use is not recommended as they require an active internet connection, thus bypassing the network segmentation between the internet and process network.

A plan must be included that covers transient cyber assets and removable media. Transient cyber assets must be managed in a manner that always ensures compliance or ensures it before being connected to the BES Cyber System. Users, locations and uses must be authorized individually or by asset group. Risk of vulnerabilities must be mitigated by security patching, running live Operating System (OS) and software executables only from read-only media, system hardening or whatever "other methods" the Responsible Entity deems necessary. Risk of malicious code is to be mitigated with antivirus software including updates of signatures or patterns, application whitelisting or "other methods". Unauthorized use is to be mitigated by restricting physical access, media encryption, multi-factor authentication or other methods. If the transient Cyber Asset is managed by a third party, vulnerabilities are to be mitigated by review of software and malware mitigation, and determination if any additional actions are necessary before engaging the transient cyber asset. For removable media users and locations must be authorized, and before connecting the removable media to protected cyber assets the threat of malicious code must be mitigated by using methods of detecting malicious code on cyber assets other than the protected cyber assets and mitigating the effects of detected malicious code [8].

2.5.2 Data Transfer and Storage

Confidential data must be encrypted when transmitted via unsecure connection or stored on mobile storage system. Storing data must be limited to contractual amounts and durations [12].

2.5.3 Disposal and reuse of Cyber Assets

For information protection methods of identifying germane information, protecting, and securely handling, storing, transiting and using it must be defined. Prior to release, reuse or disposal of a Cyber Asset containing Cyber Asset Information, measures must be taken to prevent unwanted retrieval of Cyber Asset Information must be prevented [9].

2.6 Network Architecture

Network architecture refers to the designing and building of the information network that forms the process network of the BES. As per development principles introduced in Chapter 2.4 the network must be built with security in mind, with staggered and overlapping defenses, and to prevent the failure of a single component from impairing the security related functions in the network.

Secure standards and protocols, including integrity protection authentication and encryption should be used where applicable, a non-negotiable for any remote parametrization and administration protocols, including custom ones. The entire system must be possible to integrate to the company overall network concept and central administration of relevant network parameters must be possible. Integrity protection, authentication and encryption must be ensured by protocols for administration and monitoring. [12]

Where technology allows, the general demand is to use only secure standards and protocols including integrity protection, authentication, and encryption where applicable. This requirement is non-negotiable for any remote parametrization and administration protocols and must also be taken to account where custom protocols are used. The entire system must be possible to integrate to company's overall network concept, and central administration of relevant network configuration parameters must be possible. Integrity protection, authentication and encryption must be ensured by protocols used for administration and monitoring. Network components must be hardened, and unnecessary services and protocols deactivated, management interfaces must be protected with access control lists. Network components provided by the supplier must be possible to integrate to central inventory and patch management. Wide Area Network connections must use IP protocol and unencrypted application protocols must be secured by encryption at the lowest network layer. Hardware and parametrization requirements are determined by the highest protection requirements among shared network infrastructure components. The shared use of components with different security requirements must in no way decrease protection level or availability [12].

The system's network structure must be segmented into zones of different functions and protection requirements, and be separated with firewalls, filtering routers or gateways

where technologically feasible. Communications with other networks must be compliant with the system's determined security requirements, and only using communication protocols approved by the client. The system's underlying network shall also be divided into segments separated by firewalls, filtering routers or gateways. [12]

2.6.1 Cloud Services

Cloud services are services run on a device outside the process network, usually from a distant geographical location through the internet. Their advantage is the centering of computational power to cater to needs of multiple customers.

When the system uses cloud services, agreements must be made on security related processes. Controls which can disrupt the energy supply must not be realized using cloud services. Downtime of cloud services must not restrict system's basic functions. [12]

2.6.2 Virtualized components

Virtualized components refer to the use of Virtual Machines as Cyber Assets. Virtual Machines use software emulating the hardware functions of a computer, which itself is run from the hardware of the host machine. Virtual Machines are, essentially, emulated computers within the host machine. This makes virtual machines convenient as disposable and replaceable assets for testing and other security related functions. They are also simpler to scale, so running multiple Cyber Assets as Virtual Machines on the same virtualization server is possible, and more secure than giving those same functions to a singular device, as the virtual machines may be segmented from each other, and their connections protected with firewall as if they were separate devices.

Hardware virtualization emulates computers on various levels of abstraction from complete hardware platforms to functionality required for specific software. Virtualization is performed by the host, a physical computer, running a virtual machine software for the guest software.

Software Virtualization refers to the virtualization emulating the entire computer. This makes software virtualization a useful tool for testing and running several virtual environments on the same guest machine.

Hypervisor is the platform that creates and runs virtual machines, presenting the virtual machine with the virtual operating platform. The Hypervisor is used to manage the guest machines on the host machine.

Container Virtualization is a virtualization technology in which the application is packaged into a software container that contains virtualized versions of all software components

up to and including the Operating System. Containers do not, however contain a virtualized version of the hardware, but instead run on the host hardware. This makes containers very cheap and movable, and particularly convenient for small services, such as running individual software incompatible with the host Operating System.

Virtualized components of different security or trust zones must be operated on different virtualization servers. Network segmentation and security zone segregation cannot be bypassed via virtualization servers. Management and administration service networks and virtualization infrastructure data storage must be firewalled from other networks and have only the minimum required network services required. Access must be restricted to administrators only. The virtualization layer, management and administration interfaces and associated infrastructure must be hardened identically as per manufacturer recommendations and included in patch management and backup concept. The virtualization servers must have necessary resources to run all virtualized components within. Outages must not have negative impact availability requirements and must be covered in emergency and restoration plans [12].

2.7 System Requirements

This chapter is a look into the system requirements according to the standards. Its purpose is to explore and explain the technical demands and requirements, and their supplementary policy requirements, placed on the technical execution of the designed system architecture. The chapter investigates topics like hardening, malware protection and the use of encryption, and how they are required for the system.

2.7.1 Hardening

All components of the system must be hardened according to the recognized best practices, and the system brought up to date. All unnecessary components must be removed or deactivated and protected from accidental reactivation. [12] Where technically feasible, only ports in the hardware necessary for their intended use must be enabled. Unnecessary but enabled ports are to be protected against use [5]. The system's basic configuration must be reviewed and documented. The development system and access systems and network infrastructure for Remote Access should likewise be hardened per industry best practices [12].

As we can see, both standards require all unnecessary ports and components in the system be deactivated. The purpose of this is to lessen the potential surface area for attacks. Industry best-practices for hardening vary, but generally include deactivation of

all unnecessary connections and removal or deactivation of all unnecessary software, user accounts, protocols etc. The requirements of Hardening are collected to figure 4.

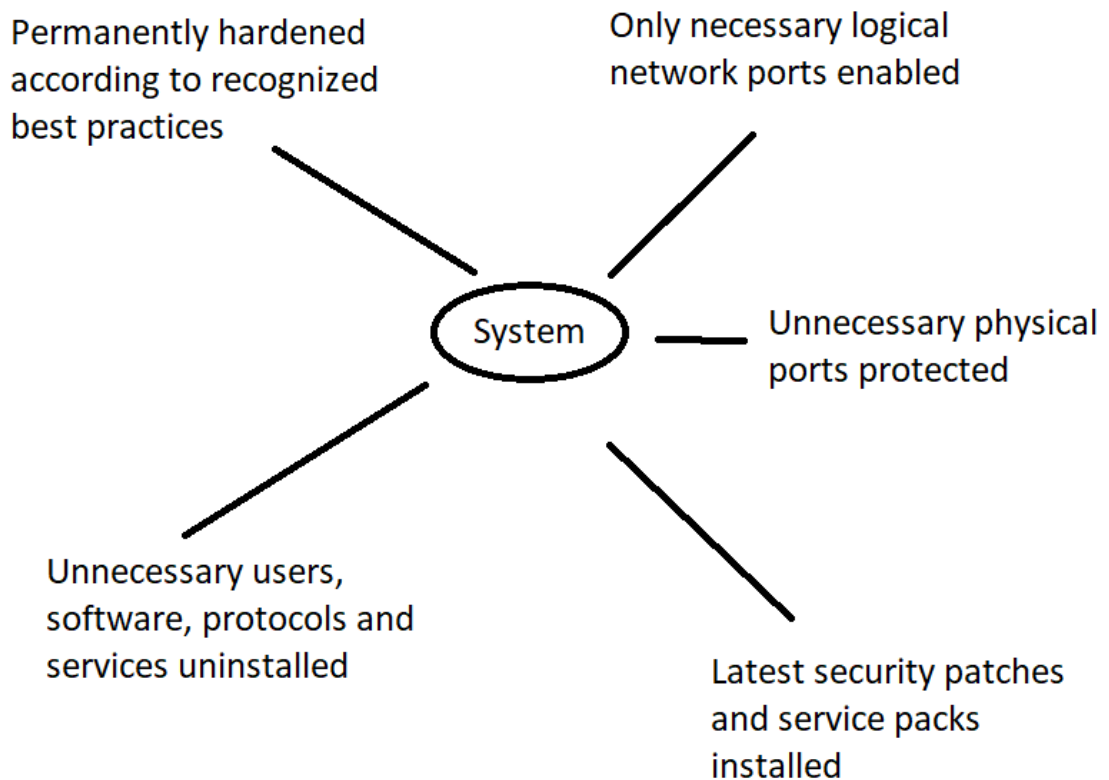


Figure 4: Requirements of hardening

2.7.2 Malicious code

Malicious code comprises of both the infamous malware, software such as computer viruses, and malicious code, scripts designed to create and exploit system vulnerabilities and to automate cyberattacks.

The Responsible Entity is to employ methods to deter, detect and prevent malicious code, and mitigate the threat of detected malicious code. If the methods use signatures and/or patterns, a process is required for updating said signatures and patterns and address testing and installing the updates. Detected malicious code should also generate security alerts and be logged for later risk management. [5]

Malware protection or a comprehensive malware protection concept shall be applied to all networked systems at appropriate locations. If the solution is pattern-based, the pattern files must be possible to update in a timely and automated manner. The update servers must not be directly connected to for updates from external networks, and the

time of updates must be configurable for terminal systems. Malware protection is also required for development platform. [12]

Both standards demand presence of malicious code protection solutions. These solutions are often based on patterns of malware or malicious code, and as such receive updates as new forms of malicious code are identified. This makes vendor malware suites attractive, as the companies running them have significant resources and know-how for maintaining knowledge about different malware-patterns.

Malicious code is not always something added to the software. Typically, software vulnerabilities, including malicious code, are searched for during the procurement and testing of the system. However, updates to the malware protection concept, such as to the patterns of a pattern-based solution, can enable the malicious code protection concept to detect previously undetected security risks, such as backdoors. Once a backdoor goes active, it is much easier to detect due to the data streaming through it. One purpose of the network architecture demands in chapter 2.6. is to mitigate the damage caused by a cyberattack through a previously inert, undetected back door, and to enable back tracing it to its source.

2.7.3 Encryption

Encryption refers to ensuring the confidentiality and integrity of data by application of a cypher that only the recipient is supposed to be able to decipher. However, various encryption techniques can also be used to verify the sender.

All confidential data must be encrypted for storage and transmission. All development data and vital Cyber Asset data must be transmitted or stored encrypted. However, in the case of remote access, the encryption of Remote Access connection must cease at the intermediate system. [12]

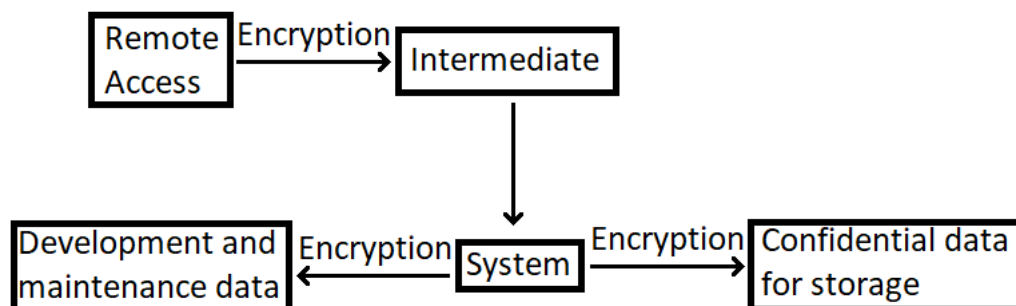


Figure 5: Application of encryption in BES Cyber system data transfer

The customer shall use approved cryptographic methods deemed secure for the foreseeable future by state-of-the-art technological knowledge within the limits and demands of national legislation [12].

Typical encryption methods might be symmetric and asymmetric encryption. Symmetric encryption refers to encryption in which the message is both encrypted and decrypted with the same encryption key. The key is shared between the correspondents, which also forms the method's big weakness, the possibility of a malicious actor intercepting the key.

One such method is the Asymmetric- or public key encryption. Asymmetric encryption is based on two keys, public and private, which can be used to decrypt a message encrypted by the other one. This means anyone can send a message only the key-holder can decrypt by encrypting the message with the public key which is, as the name implies, publicly available. Similarly, the private key can be used as a digital signature to authenticate the message's origin by hashing the message and encrypting the hash with their private key. Though slower than symmetric encryption, the strength of asymmetric encryption is that one does not need to share the encryption keys, eliminating the possibility of the key being intercepted.

2.8 Access Management

Access management is management of different forms of access to the system, such as physical or electronic access. The purpose of access management is to prevent undesirable surveillance and manipulation of the system and communications used to manage it.

2.8.1 Electronic Security Perimeter

An Electronic Security Perimeter (ESP) is to be established and all Cyber Assets placed within it. The ESP should only be accessible for routable communication from Cyber assets outside the ESP through the identified Electronic Access Point. The Electronic Access Point is to require permissions and reasons for access, refuse access by default, and have means of detecting malicious communications in and out of the system. [3]

2.8.2 Physical Access management

Physical access covers access to the physical devices of the BES. This means both the individual's ability to access the physical Cyber Assets or their interfaces, but also the ability to make the physical connection between devices, such as plugging in an Ethernet cable or a Universal Serial Bus (USB) drive or forming wireless connection.

The Responsible Entity is obligated to implement at least one physical security plan defining operational and physical controls. The plan must be set to restrict unescorted physical access to a predefined group, to establish a visitors' program to others, and monitor access through physical access points. Physical access should be controlled by at least one method, two or more whenever technically feasible. Each person's identity and time of entrance and exit should be logged, and the logs retained for 90 calendar days. For visitors, their point of contact should be logged as well, and they should be escorted all times. Access management should utilize at least one method of control for unescorted access, two or more for high impact systems whenever technically feasible. [4]

The system should also monitor access to Physical Access Control System as well. In the event of unauthorized physical access through the access point or to Access Control System, the system should issue an alert to personnel identified in incident response plan within 15 minutes of detection. [4]

The plan must also restrict access to cabling and other non-programmable communication components located outside the physical security perimeter which connect cyber assets within the same electronic perimeter. All physical access systems must be tested and maintained at least every 24 calendar months. [4] On-site maintenance should happen through a predefined process by predefined people with personalized accounts. [12]

Physical security happens on all levels from individual devices to the overall site and must be addressed as such per the defense-in-depth principle. Because of the different requirements, the security measures can take many different forms from fences and checkpoints of the physical site to locked rooms or cubicles of large network components to physical plugs or other blockages of unused ports on physical Cyber Assets.

2.8.3 Authentication management

Authentication management means management of the user rights and privileges, and the means of verifying the identity and granting access to said user, be it physical or network access. The purpose of authentication management is to make sure the predetermined right people, and only those people, have the right information and access rights at the right time. Authentication management uses authentication factors such as passwords and physical tokens for verification.

Responsible Entity is required to implement an access management program to authorize access to BES Information storage, verify quarterly the authorization records of individuals with access, and every 15 calendar months verify all user accounts and various other access categories to be necessary and that their rights and privileges are required for their function. [2]

The responsible entity shall also implement an access revocation program. In case of termination access will be revoked within 24 hours of termination, access to BES Cyber System Information by the end of next calendar day, and non-shared user accounts within 30 calendar days from effective date. In case of reassignment or transfer unnecessary accounts and access will be removed by the end of next calendar day. [2]

Responsible Entity is also required to implement an authorization program for interactive access [12] with at least one method of enforcing authentication [5]. This includes personalized accounts for Remote Access with Multi-Factor Authentication (MFA) [3] User identification and authentication must not rely exclusively on data outside the process network. [12]

The system's user concept must contain at least the following roles:

- Administrator: Installs the system, and maintains and manages it, able to change security and system configurations.
- User: Operates the system within the planned normal use and can change operationally relevant settings.
- Read-only user: Is not permitted to make changes but is able to view system status and pre-determined operating data.

The typical user rights must abide by a secure system configuration and regular system use must be possible with only user or read-only user rights. Security system settings and configurations must only be possible to be viewed and edited by the Administrator. Individual user accounts must be possible to deactivate without removing them from the system. [12]

The individual user must be identified and authenticated by their personal user account, unless given permission for group accounts by the client for a narrowly defined exceptional cases. The system must support state-of-the-art password policy, and two-factor authentication wherever technologically feasible. [5]

All login attempts must be centrally logged, and alarm raised in case of unsuccessful login. Only a narrow range of actions must be allowed without authentication. The number of failed attempts should be limited by system logout or the system raising an alert. The logs should be retained for 90 days and sampled every 15 days for Cyber Security Incidents [5].

Central logging can be achieved by using central logging standard such as Syslog and operating a Syslog Server, possibly in the form of a vendor service.

Security related or critical actions as defined by client/System Operator require a prior authorization of the requesting user for the requesting system component. OWASP TOP 10 and OWASP Application Security Verification Standard and BSI Guideline is to be applied for Web applications and services, unless justified and pre-approved by the client. Before processing data as part of security-related activities, the integrity of the data shall be verified. [12]

2.8.4 Remote Access management

Remote Access refers to user-initiated connection from an external Cyber Asset by a routable protocol. This is usually done by a remote access protocol. System-to-system process communications are not included in remote access.

BDEW Whitepaper demands Remote Access should take place via centrally administered access servers placed and operated from within a Demilitarized Zone (DMZ) network and requires Multiple Factor Authentication. Administration, maintenance and configuration of all components must be possible by an out-of-band network [12]. A DMZ network refers to a subnet acting as a buffer between public, unsecured networks (usually the internet), and Organization's secure private network. Usually, a DMZ contains organization's forward facing services and allows access to untrusted networks for services that don't require access to the secure parts of private network.

NERC-CIP demands the use of an intermediate system to prevent direct access to the system [3]. Therefore, a DMZ network in which the access servers act as a proxy as shown in figure 6 covers both demands. The external device with remote access connection only makes requests to the intermediary system, which passes the requests on to the internal network if they are deemed safe. The internal network responds to the requests to the intermediary, which likewise passes the response to the external device. The structure of such a network is covered in figure 7.

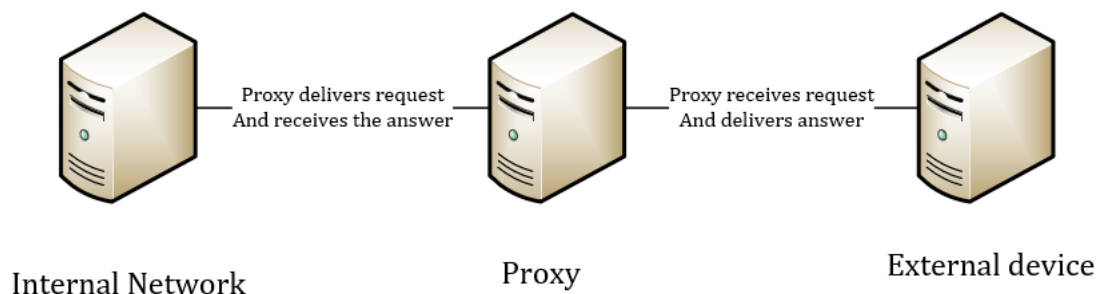


Figure 6: Operating principle of proxy server

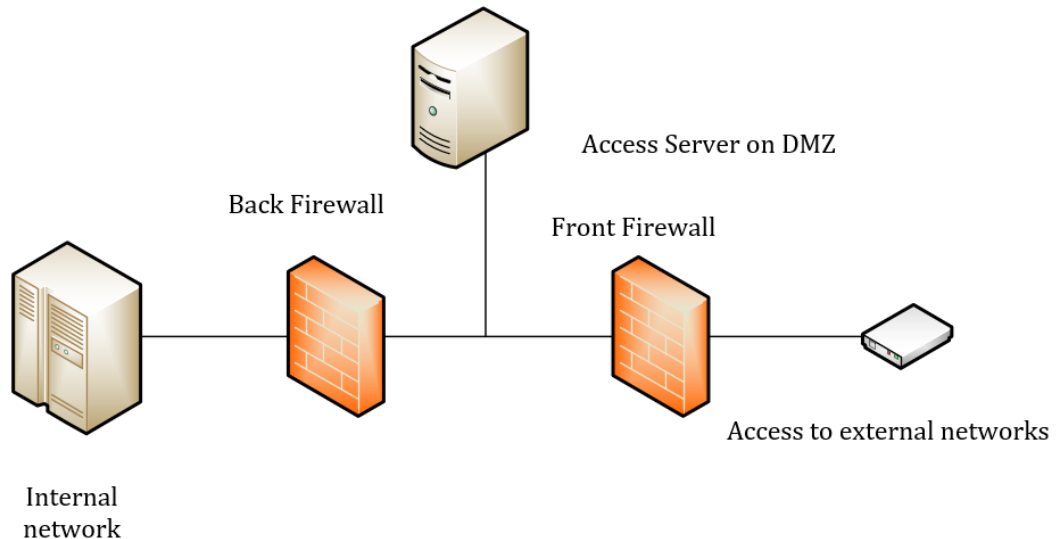


Figure 7: DMZ Access server scheme

For remote access, encryption should terminate at the intermediate system, and measures implemented to detect malicious communications in or out of the system [3]. Connection should only use technology and protocols deemed secure, and short-range wireless technologies (such as Bluetooth) in the connection between the Intermediate system and main system should only be implemented after risk assessment. Access should only be granted to predefined people with personalized accounts following a predefined maintenance process. Authentication attempts should be logged, and repeated failures to authenticate cause lockout or alarm. [12] Multi-factor authentication of personalized accounts should be used wherever technically feasible. The system should also have methods for determining and disabling active remote access sessions. [3]

As such, dial-in should not be possible to terminal devices. Encryption of the remote access should terminate at the DMZ. Remote Access should be under control of System operator with methods for determining and disabling active sessions. The recipient of the message in the remote access is not the internal network, but the access server.

2.9 Vulnerability Management & Maintenance

CIP-003 Requires the Responsible Entity to review and update their policies for following standards CIP-004 to CIP-011 with Medium and High Impact systems and policy for Low Impact Systems as identified in CIP-002, and to gain the approval for them from the appointed CIP Senior Manager. For High and Medium Impact Systems this includes the plans for each of the currently enforced versions for standards from CIP-004 to CIP-011. For Low Impact systems this includes Cyber Security Awareness, Physical Security Controls, Electronic access controls, Cyber Security Incident (as defined in CIP-8) response

and transient Cyber Asset and Removable Media malicious code risk mitigation and Declaring and responding to CIP Exceptional Circumstances as defined in CIP-003. Evidence of such plans include documentation from company document management system indicating renewal and approval of plans every 15 calendar months. [1]

CIP-004-6 requires documented process for quarterly reinforcement of cyber security practices (and possibly associated physical security practices) for the responsible Entity's personnel with authorized access to BES Cyber System electronically, or physically and unescorted. Standard also requires cyber security training programme for the various roles and responsibilities for each applicable requirement in the standard. The content includes: The Responsible Entity is to require the completion of the training prior to granting access to its Cyber Assets, except during CIP Exceptional Circumstances. The training must be completed every 15 calendar months. [2]

Each responsible entity is also required to implement personnel risk assessment program to manage electronic and unescorted physical access. The programme should include confirmation of identity, seven years criminal history records check in person's current site of residence and any previous site in which the person has resided for six consecutive months during the seven-year check period, or as complete a check as possible and documentation as to why complete check was not possible. Criterion to check that contractors and vendors have been checked in the same manner, and that personnel with access have had the personnel risk assessment in manner proscribed. [2]

BDEW Whitepaper only covers procurement of the system, and as such does not make demands of reviewing policies and continuous improvement.

2.9.1 Risk Management

According to CIP-13, the Responsible Entity is required to develop, implement, and review every 15 calendar months at least one cyber security risk management plan for medium to high-impact bulk electric systems (BES), and have the reviewed plan approved by CIP Senior Manager or delegate every 15 calendar months [8]

2.9.2 Vendor products

The plan should include one or more process for identifying and assessing cyber security risks in vendor products and services procured for and installed to the BES. Incidents identified in vendor products by the vendor and coordination of responses to said incidents, notification by vendors that onsite or remote access to vendor and its representatives should not be granted, known vulnerabilities disclosed by the vendor, software

integrity and authenticity verification, and coordination of controls for access to the vendor or vendor's system should be addressed. The changes to existing contracts, or specific clauses in the future ones are not required from implementation of the plan, nor include the vendor performance and adherence to contracts. The evidence for fulfilling the requirements is the documentation of the plan, its implementation, review, and approval. [10]

In the planned and contractually stipulated timeframe, the supplier shall make manufacturer support and security patches for system component developed by it and third parties available. Discontinuation of service shall be covered by a binding agreement detailing procedure and minimum terms.

2.9.3 Vulnerability assessment

Vulnerability assessment means reviewing the system for vulnerabilities. The purpose is to discover and document the vulnerabilities of the system to prioritize their remediation process.

A paper or a genuine vulnerability assessment is to be produced every 15 months. On high impact systems every 36 calendar months an assessment must be performed in a test or production environment that controls for adverse effects from external factors and emulates the basic configuration, and the results and differences of test environment are to be documented. Active vulnerability assessment is to be performed on all new Cyber assets that are to be added to the production environment, and the results documented [6]. The purpose and methods are left up to the operator. The methods can vary from reviewing of the system documentation to checking for publicly disclosed vulnerabilities of system components from publicly available sites such as National Institute of Standards and Technology (NIST) [15], Zero Day Initiative [16] or CVE Details [17] to penetration testing, a simulated cyberattack on the system, .

2.9.4 Cyber Security Incidents

Cyber Security Incidents refer to something infringing upon the security of the system, or the system tripping an alarm. Whenever the system trips an alarm, it must be investigated to discover if the incident was genuine, or if the alarm is false. This is not only important for the vulnerability assessment of the system and fixing of said vulnerabilities, but also remove false alarms which encumber the system and waste resources. Different possibilities of true and false positives and negatives are shown in Figure 8.

	Positive	Negative
True	Correct reaction to unwanted action. Investigate logs, assess damage and determine if future action is required	System operating normally and under no unwanted action. No actions required.
False	False alarm. Investigate logs to determine cause for false alarm and devise plan to prevent future incidents	Undiscovered incident. System logs sampled regularly to discover. If discovered after-the-fact follow true positive procedure

Figure 8: Cyber security incidents

As shown in figure 8, Cyber Security Incidents include:

- False alarms (false positive): Alarm trips, but upon investigation no unwanted actions are deemed to have taken place.
- Detected Cyber Security Incidents (true positive): Unwanted actions trip an alarm. These are investigated to discover the extent of damages and the vulnerabilities exploited.
- Undetected Cyber Security Incidents (false negative): Unwanted action have occurred but have not tripped an alarm. These are discovered after the fact by reviewing system logs.
- There is also the possibility of true negative, in which the system is under no unwanted action and trips no alarms. However, a post-hoc investigation may uncover other problems in the system, such as there being no logs for wanted actions know to have taken place, or routine actions being neglected.

For post-hoc investigations and identification of cyber security incidents, events at the BES Cyber System or the Cyber Asset must be logged, including malicious code detection, and all login attempts. Security events that are cause for alert must be determined and set up to cause alert. Such events must include detection of malicious code and failed login. [5]

Event logs are to be retained for 90 calendar days unless technically infeasible or under CIP Exceptional Circumstances. A sample of event logs or a summary of them is to be reviewed every 15 calendar days at most for identifying oreviously undetected security

events [5]. The purpose of the demand and sampling of event logs is to uncover previously undetected Cyber Security Incidents. This is done by searching the logs for events that have for some reason not tripped alarms, but upon inspection are deemed to be signs of a Cyber Security Incident.

One or more process is required for identification and classification of Cyber Security incidents. The process should include criteria to evaluate and define attempted compromise of the system and determine if the incident is a reportable cyber security incident or to compromise as determined by criteria and provide notification. The roles and responsibilities of response groups or individuals, and procedures for handling the incidents should also be included, as well as the time records of incidents responded will be retained. Response plans should be tested every 15 calendar months. Deviations of the plans when responding to incidents or exercises should be documented. [5]

Any lessons learned should be documented, the plans updated, and personnel included in the plans notified 90 days after incident or exercise. Updates to response plans and notifications to personnel involved are also required no later than 60 days after changes to roles, responsibilities, response groups, individuals or technology that impacts the ability to execute the plans. [5]

Responsible Entity is obligated to notify Electricity Information Sharing and Analysis Center (E-ISAC) and the United States National Cybersecurity and Communications Integration Center if under jurisdiction of U.S.A, or their legitimate successors of incidents and attempts to compromise, unless prohibited by law. Notification must include the functional impact and attack vector. Notification is required to be left one hour after a Cyber security incident, on in case of an attempt to compromise by the end of next calendar day, and any updates within seven calendar days of determining new or changed attribute or information. [5]

2.9.5 Patch Management

A patch management process should be set up to identify the source of security patches on updateable Cyber Systems, evaluate received patches every 35 calendar days, and within 35 calendar days of evaluation apply the patch, or create/revise mitigation plan for the vulnerability addressed by the patch. The mitigation plan is to be implemented in the timeframe included in the plan, or a CIP Senior Manager or delegate must approve a revision or extension for the plan [5]. This timeline is summed to figure 9.

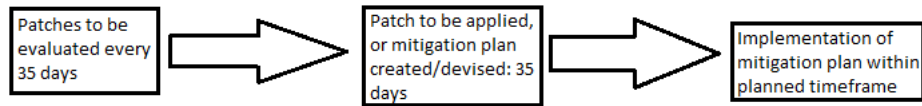


Figure 9: Timeline of patch management

All components must be patchable, and patch management for individual components and the entire system must be supported by supplier. The system must be designed to support control and management of patch installation, testing and documentation. The security patches must be possible to install by the operator independently. Required uninstallations must be authorized by the operator and documented in a tamper-proof, transparent way. Integrity of patches and updates must be verified cryptographically. [12]

Supplier shall ensure that security patches are available through the entire contractual timeframe. The contractor must obtain, test and, when necessary, deliver security patches for components used by the contractor that are manufactured by a third party. All testing and delivery must happen within the stipulations of the contract. [12]

2.9.6 Backup

Responsible entity is required to have a backup plan. The plan should include the conditions for activating the plan, roles and responsibilities, processes for back-ups and storage of necessary information to restore the BES Cyber System, their verification and preserving of the data of an incident mandating the recovery effort without impeding the recovery. The plan is to be tested at least every 15 calendar months in practice, paper drill or tabletop or operational exercise. A representative sample of the recovery data is to be tested every 15 months to ensure backup useability, and the full recovery plan in an operational exercise every 36 calendar months, conducted in representative environment. An actual recovery effort substitutes for either or both. Any lessons learned should be documented, the plans updated, and personnel included in the plans notified 90 days after recovery testing or exercise. Updates to plans and notifications to personnel involved are also required no later than 60 days after changes to roles, responsibilities, response groups, individuals or technology that impacts the ability to execute the plans. [7]

Procedures for back-up and recovery for the individual component in relation to the system and the configuration must be documented, tested and in place, including a central back-up for distributed component's configuration parameters. Procedures must be updated and retested after relevant system updates. The supplier is required to provide documented and tested procedures for relevant emergency and crisis scenarios as defined by the operator as the operator's business emergency management. This includes

estimated recovery times. Part of the approval process of the release changes for relevant system updates must be updating and retesting of these proceedings. [12]

The two standards demand very similar things, with NERC-CIP making broader demands for details, and the circumstances surrounding the actual backup procedure.

3. HMI CASE STUDY

To demonstrate the findings and discussions based on the findings, a case study will be made of setting up a Human-Machine Interface Personal Computer (HMI-PC or HMI). HMI refers to the hard- and software the operator uses to control the system. The HMI surfaces can range from control panels with visual indicators and simple control devices like buttons, dials, and switches to a full industrial PC. This Case study assumes the HMI will be a PC.

Because HMI is an interface designed for human to use the control apparatus of the BES, it's both a prime target for cyberattacks and prone for both accidental and purposeful misuse by the operator. Therefore, it needs to be secured against both kinds of threats. It also must be present in any kind of Cyber System that is not intended to be completely divorced from human control. Because of this, an HMI makes for a good example to demonstrate applying the combined market demands.

3.1 Standard demands for HMI-PC

The purpose of this chapter is to investigate how discovered market demands apply to a HMI-PC. As shown in the previous chapters there are no demands made to the HMI specifically, but the HMI is a part of the BES's cyber system, and therefore must be compliant with the overall demands while filling the demands of the individual component.

3.1.1 HMI as part of BES

The HMI will likely be part of the baseline configuration of the BES. If this is not the case, the system is to be approved separately and any impact on the demands of CIP-5 and -7 compliance is to be determined beforehand [8]. This process will likely be part of the system's risk assessment procedure [6].

After setup, the system is to be configured to a secure state and development and testing facets of the system demonstrably removed as per demands of CIP-10 [8].

3.1.2 Development & Setup

Setting up the HMI includes procuring the hardware, firmware, and software, and setting it up as a functional device. The standards make various demands on the process.

Individual components are to be designed and developed with focus on security, which naturally applies to the HMI as an interface. The HMI is to be developed within the established and certified secure development procedures, using secure standards and protocols, including integrity protection authentication and encryption where feasible. The system must be integrable to overall company network concept, and the HMI must not be able to bypass network segmentation. The HMI should only communicate with the rest of the BES Cyber Systems via pre-determined Network Adapter and be manageable via an out-of-band network. After setup and either first boot or re-boot, the system is to be configured to a secure state [12].

The development of the HMI should follow the secure system design principles of BDEW Whitepaper:

- Security by design: The system should be designed with focus on security, with attacks and unwanted actions considered.
- Minimal need-to-know: Each user and component is only granted the rights and privileges required for their function.
- Defence in depth: Security measures need to be staggered and complementary
- Redundancy principle: the failure of a single component must not endanger the system's security functions.

Of these, the second demand applies to the HMI as a display and control device. The device should have the ability to display data and deliver the commands given by human operator, but also restrict different operators from performing actions their position does not require. This demand is also required of the HMI user concept, covered in chapter 3.2. HMI Access Management. The defense in depth principle only applies for security measures being complementary, as the HMI as an individual component can only contain the security measures of the HMI. This applies to the various security measures demanded by the standards, such as hardening, malicious code protection and access management as well as any other security measures implemented by the developer. Finally, the redundancy principle similarly means that the failure of the HMI should not impair the security functions of other components.

3.1.3 Information management

As an Operational Technology component, availability of information is of paramount importance to the HMI, and as an interface its purpose. However, this means that availability is best ensured by ensuring the security of the HMI. This means making sure hard-

ening and software whitelisting is in place, and the machine is resistant to Denial of Service- attacks. Similarly, integrity and confidentiality require making sure the HMI is safeguarded without interrupting its proper functions.

All confidential data must be encrypted when stored or transmitted. All development data and vital Cyber Asset data must be transmitted or stored encrypted. However, in the case of remote access, the encryption of Remote Access connection must cease at the intermediate system [12]. These demands are primarily for integrity and confidentiality of information that is delivered to on transferred from the HMI.

3.1.4 Hardening

Hardening the system includes disabling of unnecessary logical ports and protocols, removal of all unnecessary software, and whitelisting of pre-approved applications. Unnecessary physical access ports are to be blocked from access. [5] Unnecessary components must be removed or deactivated, and the system hardened according to whatever recognized best practices are recognized in the industry at present. [12] Essentially the system must be hardened as discussed in chapter 2.7.1 In the specific case of an HMI the device likely contains a vendor Operating System with a Graphic User Interface. Such operating systems tend to come with additional applications that are unnecessary to the system's function and need to be removed or deactivated. This process can and has been automated to a degree, with some programs for it being available free on the internet, and certain companies having developed similar tools for their private use. However, the only way to truly make sure is for the developer to manually check and manually remove the undesirable software.

3.1.5 Malicious code

Per CIP-7, the HMI requires methods for deterring, detecting and preventing malicious code and to mitigate threat thereof. [5] The malicious code protection concept should be applied to networked systems at appropriate locations. [12] If the methods are based on signatures or patterns a process of updating said signatures is also required, including testing and installing the updates [5] and the patterns should be possible to update in a timely and automated manner without direct connection to update servers on external networks. [12]. Detected malicious code should generate security alerts for later risk management [5]. This demand likely means installing a vendor malware suite or developer's own malicious code protection concept at the HMI, as the HMI both requires one as a control device, and because as an interface it enables managing the security alerts by the human operator.

3.1.6 Access Management

As part of the BES the HMI is subject to its programmes and procedures of Access Management as demanded by standards. While for the most part this means that the HMI is simply included in normal procedures of the larger system, some measures need to be taken to the HMI specifically as a component of the BES, or due to the requirements of the HMI's qualities and function. These requirements are covered in their respective sub-chapters.

3.1.7 Electronic Security Perimeter

As a Cyber Asset of the system the HMI is to be placed within the BES's Electronic Security Perimeter. Whatever traffic the HMI's function may require with Cyber Assets outside the ESP should go through the Electronic Access Point as usual, and incoming traffic to the HMI be subject to the usual scrutiny. [3]

3.1.8 Physical Access management

As per the Defense-in-depth principle [12] the HMI should have physical access to it restricted even from within the BES's physical security perimeter. This should include at least one method of controlling unescorted physical access to the system to restrict it to predefined group of people. Access to the HMI should also be included in the protocols for unescorted access and visitors' program. Physical Access to the HMI should be monitored by the BES:S security measures. [4]

As the HMI is connected to the other parts of the BES within the same Electronic Access Perimeter, access to its cabling must be restricted if the HMI is placed outside the Physical Access Perimeter. Physical access systems must be tested and maintained at least every 24 calendar months as with the larger system. [4] On-site maintenance should happen through a predefined process by predefined people with personalized accounts. [12]

3.1.9 Authentication management

The HMI as part of the BES is subject to the access management and revocation programmes demanded by CIP-7. Responsible entity is required to verify quarterly the authorization records of individuals with access, and every 15 calendar months verify all HMI's user accounts and HMI-software's user accounts and various other access categories to be necessary as per the larger demands for access management programme. Personal user accounts must be removed within 30 calendar days from effective termination date. In case of reassignment or transfer personal accounts will be removed by the end of next calendar day. [5]

For interactive access with the HMI an authorization programme is required [12] with at least one method of enforcing authentication [5]. User identification and authentication must not rely exclusively on data outside the process network [12].

The system's user concept must cover the following roles:

- Administrator: Installs the system, and maintains and manages it, able to change security and system configurations.
- User: Operates the system within the planned normal use and can change operationally relevant settings.
- Read-only user: Is not permitted to make changes but is able to view system status and pre-determined operating data.

The normal function and uses of the HMI must be possible with only User or Read-Only User credentials. Accessing and changing security system settings and configurations must require Administrator-level credentials. Individual user accounts must be possible to deactivate without removing them from the system. [12]

The individual user must be identified and authenticated by their personal user account, unless given permission for group accounts by the client for a narrowly defined exceptional case that includes the HMI. The system's password-policy should be as state of the art as possible and require two-factor authentication where feasible. [5]

All login attempts to the HMI must be centrally logged, and alarm raised in case of unsuccessful login. Only a narrow range of actions must be allowed without authentication to either the OS or to the HMI-software. The number of failed attempts should be limited by system logout or the system raising an alert. The logs should be retained for 90 days and sampled every 15 days as per required Cyber Security Incident policy [5].

Security related or critical actions for the HMI require a prior authorization of the requesting user for the requesting system component. Before processing data as part of security-related activities, the integrity of the data shall be verified. [12]

Remote Access is not in the scope of this Case Study, and as such will not be discussed here.

3.1.10 Risk Management

HMI-PC is to be made compatible with Standard demands for Vulnerability Assessment and Cyber security Risk Management. This includes abiding by the BES's established risk management procedure. [6]

Active vulnerability assessment, with documented results, is to be performed on the HMI before it is added to the process environment [6].

3.1.11 Maintenance

The system must be patchable as per demands of BDEW Whitepaper. As per demands of CIP-7, the patch is to be tested and shown to not impede the function of the HMI before it is applied [5].

As mentioned previously, on-site maintenance should happen through a predefined process by predefined people with personalized accounts. [12]

3.2 System Setup

Setting up the HMI includes procuring the hardware, firmware, and software, and setting it up as a functional device. This includes phases such as

- Installing and updating firmware.
- Setting up user profiles and profile groups.
- Hardening the system.
- Inputting system settings.
- Installing and updating the software.
- Configuring the system firewall
- Setting up security measures, such as integrating the system to BES's anti-malicious code concept, and software whitelisting.

3.2.1 Settings

System settings are adjusted to support the device's function as an HMI. This process is dependent on the requirements of the specific HMI software but may include concepts like NIC Teaming or allowing certain user profiles necessary rights.

To mitigate threat of malicious code, the system has multiple layers of defense as per the defense-in-depth- principle [12]. The system must be restricted in running unsigned scripts, have policy restricting software execution (such as Whitelisting discussed in a later chapter), and be part of the BES's anti-malicious code concept. This may be something as simple as a vendor anti-virus suite, or something more complicated such as a custom pattern-based solution on a device not connected to the internet which's patterns

are manually updated as part of system maintenance [5]. Confidential data (such as authentication data, cyber security incident data and operating data) is only to be stored on the device encrypted [12].

3.2.2 Hardening

Hardening also includes removing all software that is not necessary for the HMI's function or security measures, such as the Operating System or the malware suite. One way to achieve this is to simply delete all software unnecessary to the system's function and installing the HMI-software afterwards. In addition, the hardening process includes a more system specific parts like disabling unnecessary network adapters.

3.2.3 Application whitelisting

To prevent use of malicious code, an extensive Software Restriction Policy is set up. All software is blocked from use by default, and a whitelist of exceptions is created. This security policy includes:

- A whitelist of folder paths of necessary executable files for the proper function of the system, including the OS and the HMI software.
- An extensive blacklist of most executable file types (such as .exe, .bat and .url) blocked from functioning outside the designated whitelisted folders. Certain file types, such as shortcuts, are maintained viable to smooth the operation of the HMI without significant increase of risks.
- Denying permission to write on the whitelisted folder paths where it does not impede the proper function of the system.
- Enforcement of above rules on all User Profiles on the OS.

By default, Local Security Policy is turned off, and the Registry Keys for it are present, but only contain a value disabling Authenticode-signatures. This can easily be remedied by importing proper Registry Keys from an external source. For that .reg-files containing the keys, and a batch-script for executing the files, is prepared as a .exe-file.

In initial testing, it was noticed that since the initial version only adds keys, certain paths were left both unrestricted and restricted. For that purpose, a batch file was created that removes all exception Registry Keys before implementing desired ones.

The whitelist is set in such a manner, that Command Prompt, Registry Editor and Local Security Policy Editor are all whitelisted. As such they can be used for maintenance and customization should the need arise.

3.3 Access management

As part of a Bulk Electric System, the HMI is to be installed within the Physical and Electric security Perimeters of the BES, which are outside of the scope of this Case Study. However, since all components should be designed with security in mind according to the BDEW Whitepaper, the HMI should include its own physical access management such as a locked room or cubicle opened with a personalized token, such as a key card, and Electric Access Point Such as HMI Firewall. If the HMI is housed within the same cubicle as other Cyber Assets it connects to, this naturally also restricts access to the HMI's cabling. The HMI itself demands logging into a User Profile of the Operating System (OS), and to a personal profile to gain access to the applications the HMI runs.

The OS User concept consists of two user groups: User and Admin, which correspond to BDEW Whitepaper's demanded User and Administrator roles respectively [12]. There is no Read-only user, as the data is not recorded in plain text to be viewed without running a relevant application and logging in i.e. without at least User-level credentials. By default, User groups consists of personal accounts, but may be replaced with group accounts if given permission by the Responsible Entity [12].

The operative applications depend on the demands of the system, but they should overall require login to a personal account, with a User Concept featuring the roles demanded by BDEW Whitepaper. As per the Need-to-know- principle, user accounts are only to be made to predetermined personnel authorized to use the HMI. The OS accounts use data only residing within system, fulfilling the demand of not exclusively using authentication data from outside the system. [12]

The established access management and revocation programmes [5] are to be followed as a part of larger policy. This includes removal of personal accounts to MHI applications of the terminated or reassigned personnel if the HMI user concept has them.

3.4 System Configuration

Active vulnerability assessment, with documented results, is to be performed on the HMI before it is added to the process environment [6]. To assess and address the vulnerabilities of the system, the components and software of the system are checked for vulnerabilities. In the case of bulk components and software this can be done on several publicly available sites, such as CVE Details (CVE) [17] Zero Day Initiative (ZDI) [16] or, particularly in case of the BES operating in USA, the National Institute for Standards and Technology's National Vulnerability Database (NIST-NVD, NIST) [17]. In case of an in-house hardware or software by the Responsible Entity or vendor, companies typically

maintain databases of known vulnerabilities of their products. Further procedures such as penetration testing may also be done.

3.5 Maintenance

3.5.1 Risk management

HMI-PC is to be made compatible with Standard demands for Vulnerability Assessment and Cyber security Risk Management. This most likely includes abiding by the BES's established risk management procedure and addressing vulnerabilities as they are discovered.

3.6 Patch management

The system must be patchable as per demands of BDEW Whitepaper. As per demands of CIP-7, the patch is to be tested and shown to not impede the function of the HMI before it is applied.

As mentioned previously, on-site maintenance should happen through a predefined process by predefined people with personalized accounts. [12]

4. REMOTE ACCESS CASE STUDY

The purpose of this chapter is to set up remote access scheme to the HMI set up in the previous case study. The purpose is to enable secure Remote Access to the HMI-device of the Bulk Electric System from a computer (referred to here as the Remote HMI) outside both the electrical network and the physical perimeter of the BES. Such a connection would likely be used for maintenance and servicing geographically remote BESs or their parts, either by the Operator of the system, or by a third party as a part of maintenance contract.

4.1 Market demands for Remote Access

According to NERC-CIP-5 an intermediate system is required to prevent direct access to the system and measures to detect malicious communication in and out of the system. Encryption should terminate at the intermediate system. Personalized accounts should be used for access with Multi-Factor Authentication for said accounts. Methods should be in place to determine and terminate active sessions [3].

Central access servers to be placed in and operated from a DMZ to isolate the process network, and all components be manageable via an Out-of-Band- network. Connections only with technology and protocols deemed secure, and wireless communications are to be implemented after risk assessment. Access to predefined people following predefined maintenance protocol only. Access through Central Access Servers to require MFA. [12]

BDEW Whitepaper demands Remote Access should take place via centrally administered access servers placed and operated from within a DMZ network and requires Multiple Factor Authentication. All components be manageable via an Out-of-Band- network including administration, maintenance and configuration [12]. NERC-CIP demands the use of an intermediate system to prevent direct access to the system [3]. The DMZ network covers both these demands.

For remote access, an intermediate system that does not access the Cyber asset directly is required, encryption should terminate at the intermediate system, and measures implemented to detect malicious communications in or out of the system. [3] Connection should only use technology and protocols deemed secure, and wireless technologies should only be implemented after risk assessment. Access should only be granted to predefined people with personalized accounts following a predefined maintenance process. Authentication attempts should be logged, and repeated failures to authenticate

cause lockout or alarm. [12] Multi-factor authentication of personalized accounts should be used wherever technically feasible. The system should also have methods for determining and disabling active remote access sessions. [3]

Remote access should only take place via centrally administered access servers in a DMZ. Remote Access should be under control of System operator with methods for determining and disabling active sessions. Encryption of the remote access should terminate at the DMZ, and remote access should require Multi-Factor Authentication. Remote access should be logged centrally, and repeated failed attempts reported.

4.2 Standard demands for the Remote Access system

This chapter covers the standard demands for the Cyber systems and assets used in the execution of the Remote Access scheme. As a part of the BES these systems and assets are still subject to the development principles and standard demands made for individual components.

4.2.1 Development & Configuration

The development of the Remote Access system is subject to same demands as the system at large. As such the system is to be developed with emphasis on defining security requirements, threat modelling and risk analysis, secure programming, requirements testing and security checks before commissioning. The overall approval process for updates and security patches is to be followed as normal. [12]

Where technology allows, the general demand is to use only secure standards and protocols including integrity protection, authentication, and encryption, as this requirement is non-negotiable for any remote parametrization and administration protocols. Administration and monitoring must ensure Integrity protection, authentication, and encryption [12].

Network components must be hardened. Services and protocols deemed unnecessary must be deactivated, and access control lists implemented for management interface protection [12]. This demand applies for Remote Access to HMI, as HMI is a management interface relying on information network access outside the system. The used Network components must be possible to integrate to central inventory and patch management. Hardware and parametrization requirements are determined by the highest protection requirements among shared network infrastructure components. The shared use of components with different security requirements must in no way decrease protection level or availability. [12]

The HMI is required to communicate with Cyber Assets outside the BES's Electronic Security Perimeter and therefore communications with other networks must be compliant with the system's determined security requirements, and only happen using communication protocols approved by the client. Administration, maintenance, and configuration of all network components must be possible via an out-of-band network [12]. Remote Access is naturally part of this, but it also applies to whatever network components are built for facilitating the Remote Access.

BDEW Whitepaper demands the following principles for BES and their components.

- Security by design: System is designed with a focus on security. Attacks and unauthorized actions are considered, consequences of security events are minimized by the system's design.
- Minimal need-to-know: Applications and personnel is only given the rights required for their purpose.
- Defense-in-depth principle: Security issues are not mitigated by single protection measure, but by stacked, multi-level and overlapping security measures.
- Redundancy principle: System is designed for failure of individual components not compromising overall security. System is designed to lower the impact of unlimited requests for resources, such as RAM or network bandwidth.

For Remote Access the security by design primarily applies to the Access Servers, as the device to which the remote access is formed is also subject to these demands and presumably designed around them, as shown for the purposes of the HMI from the previous chapter. This is also how the Defense-in-Depth and Redundancy principles are in effect. Minimal need-to-know principle means curtailing the access rights and user privileges to the personnel that are expected to make use of the Remote Access connection, and only to the rights said personnel need in their functions. It also means the Access Servers themselves should have next to no rights, as their function is to act as a middleman for requests by the Remote User.

4.2.2 Access management

As Remote Access is made to the HMI, a component of the BES, the Remote Access is subject to normal standard demands of the HMI. Any credentials specific for the Remote Access and separate from the HMI's own access management are subject to access management and revocation programmes. Their necessity is to be reviewed every 15 calendar months, and personal user accounts removed within 30 calendar days of effective date in case of termination and the following calendar day in case of transfer [5].

An authorization programme is to be implemented [12] and to include at least one method of enforcing authentication [5] with Multiple Factor Authentication [3]. Personal accounts are to be used, unless permission for group accounts for a narrowly-defined special case that includes the Remote Access is given from the client [5]. Identifying and authenticating user must not rely solely on information from outside the network [12].

Remote Access accounts are to fall within the BES's user concept. However, as the requirements of Remote Access may not fall within the parameters of regular system use, the Remote Access may require a custom role. As usual, individual user accounts must be possible to deactivate without removing them from the system. [12]

All login attempts for Remote access must be logged centrally, and unsuccessful login resulting in an alert. The system should either lock out or raise further alarm after a pre-determined number of unsuccessful logins has happened. The logs should be retained for 90 days and sampled every 15 days for Cyber Security Incidents. [5]

4.2.3 Hardening

Network Infrastructure for the Remote Access should be hardened [12]. Hardening should happen according to the recognized best practices, and the infrastructure brought up to date. All unnecessary components must be removed or deactivated and protected from accidental reactivation. [12] Only necessary ports should be enabled where feasible and protected against unintended use where not [5]. The Remote Access infrastructure should be reviewed and documented as part of the larger reviewing and documentation of the system after hardening [12].

4.2.4 Malicious code

The Responsible Entity is to employ methods to deter, detect and prevent malicious code, and mitigate the threat of detected malicious code according. If the methods use signatures and/or patterns, a process is required for updating said signatures and patterns and address testing and installing the updates. Detected malicious code should also generate security alerts and be logged for later risk management. [5]

Malware protection or a comprehensive malware protection concept shall be applied to all networked systems at appropriate locations. If the solution is pattern-based, the pattern files must be possible to update in a timely and automated manner. The update servers must not be directly connected to for updates from external networks, and the time of updates must be configurable for terminal systems. Malware protection is also required for development platform. [12]

4.3 Practical considerations

Remote Access works by forming a network access between the Remote-HMI and the HMI. This is done by forming a Virtual Private Network (VPN) tunnel through the Internet from the Remote-HMI to an intermediate system. A VPN Tunnel is a network structure where the Cyber Asset connects to a separate server which forms encrypted connection to destination. The destination only sees the IP of the VPN service provider and receives all messaging from them encrypted. Encryption must cease at the receiving Cyber Asset, which per the standards is the intermediate system in a DMZ. This also fulfils the demand of encryption ceasing at the Intermediate system.

4.3.1 Secure architecture and design considerations

As the BDEW Whitepaper's requirement for secure standards and protocols is non-negotiable for remote administration, such as Remote Access, Remote Access will likely be achieved with a vendor Remote Desktop software. At its simplest this can be something like Microsoft Remote Desktop, a feature in Windows 10 professional and newer Windows operating systems. However, if a more complicated connection is required, such as remote controlling a Linux machine with a Windows machine, other third-party suites can fulfill that purpose.

The system is designed to fill BDEW whitepaper's secure system design principles as follows.

- Security by design: The System is primarily designed around the access management systems and ensuring that network connection may only be made through them.
- Minimal need-to-know: Is a policy requirement, and therefore not part of technical consideration. However, Remote Access credentials should only be granted to vetted users, and the credentials subjected to the standard Access Management policy or regular checking and purging of unnecessary accounts [5].
- Defense in depth: Remote Access is naturally subject to the pre-existing security measures of the HMI. MFA authentication is to be used. Manual determination of session is also a possible solution. The access systems are to be hardened to ensure access only through Electronic Access Point, which is to require authentication.
- Redundancy principle: As the case study covers an individual system, following this principle is not possible in the scope of the case study. However, the system likely has a secondary HMI without Remote Access capabilities in case the main

one is taken offline and can be used to cover some of the damages of a Cyber Security Incident through Remote Access.

The HMI is set up as in the previous chapter, and therefore not directly connected to the internet, but via a Router or an Ethernet Switch. Furthermore, a DMZ-network with Firewall is placed between the Local Area Network and the Internet and handles authentication for the Remote Access.

As the Remote Access will be formed to an HMI set up as in the previous case study, we can assume the HMI to be compliant with the standard demands for hardening. However, the Remote Access itself should require authentication. The natural place for authentication control is the Intermediate system at the DMZ.

Administration, maintenance, and configuration of all network components must be possible via an out-of-band network [12]. Therefore this also applies to the Access Control DMZ.

4.3.2 Access Management

Since the system is set up as in previous chapter, most of the authentication management is the same. Operating System's User Concept is otherwise the same, but an additional user profile, RemoteUser, is added with desired rights, likely corresponding to User or Read-Only User. The DMZ Access Servers are to require a separate login to a personalized account with Multiple Factor Authentication [3]. The Authentication factors must be such that they can be used from wherever the Remote Access happens, such as Username & Password and a mobile authentication app. If Remote Access is to happen from a predetermined secured workstation, physical token complete with token reader installed to the Remote-HMI may also be possible. An electronic access port may also be used to read a physical drive, such as a USB-key. All authentication attempts at the Intermediate system are to be logged and repeated failed attempts should cause an alarm [5].

4.4 System Requirements

4.4.1 Network Structure

Wireless connections are very useful over vast geographical distances, or to places where terrain lends itself poorly to installing communication lines underground. This means that at least part of the internet connection between the HMI and Remote HMI will likely be wireless. However, the security issues with the necessary internet connection can be resolved with a VPN tunnel.

The actual connection between the DMZ and the BES should be a physical one, achieved with cabling. Access to cabling should be restricted as the DMZ and HMI are part of the different zones of network. A wireless connection is possible as well, after the risk assessment demanded by BDEW whitepaper.

5. DISCUSSIONS

As no contradictions between standards could be shown in Chapter 2, it can be asserted that the standards are not mutually exclusive in any way. However, they do have significant overlap with each other, and the demands they make complement each other. Underneath is a table of comparisons between the standards, divided to topics covered by both standards. The last column covers the commonalities discovered in Chapter 2 by which a system can be compliant with both standards regarding each issue.

Table 1: Comparisons between standards

Issue	NERC-CIP	BDEW Whitepaper	Commonalities
Remote access	<ul style="list-style-type: none"> When technically possible, perform authentication for Dial-up access. Remote access: Only through intermediate system. Utilize encryption terminating at intermediate system. MFA for Remote Access sessions. One or more methods for determining and disabling vendor RA sessions. 	<ul style="list-style-type: none"> No Dial-in access to terminal devices. Centrally administered access servers for Remote Access. Access servers to be hardened and in a DMZ, with malware protection and latest security patches installed. Central logging of all Remote Access. Remote and on-site access only by predefined and properly trained people. Personalized accounts only with Two-Factor Authentication. Sessions are to be allowed explicitly and individually. Sessions are to be disconnected individually by users or on timeout. Access systems are to be isolated as a subnet, and preferably physically. 	<ul style="list-style-type: none"> Dial-in access to access systems only. Remote Access only by approved people with personalized accounts through at least two factors of authentication. Dial-up access to be authenticated when possible. Only sessions individually and explicitly approved by System Operator. Disconnection by System Operator, timeout, or user. Access systems to be isolated both physically and as a subnet. Access systems are to be hardened.
Hardening	<ul style="list-style-type: none"> Where technically feasible, only enable necessary ports. If disabling logical ports is not possible, open ports considered necessary. Protection required 	<ul style="list-style-type: none"> Hardening as per recognized best practices. Unnecessary users, protocols and software to be uninstalled, if possible, permanently deactivated if 	<ul style="list-style-type: none"> All unnecessary access points to be disabled or deactivated and protected from activation. System to be Hardened as

	<p>against unnecessary physical input-output ports for network connectivity, console commands or removable media.</p>	<p>not. Basic configuration to be reviewed and documented.</p>	<p>per industry best practices.</p>
Malware	<ul style="list-style-type: none"> Malware protection is to be present to detect, deter and prevent and mitigate malicious code. A Process is to be set up to test and install updates for signature or pattern-based solutions. 	<ul style="list-style-type: none"> Malware protection or an equivalent malicious code mitigation concept is to be present at appropriate locations. Updates to pattern-based malware protection are to be installed in timely and automated manner. 	<ul style="list-style-type: none"> Malware protection is to be set up at appropriate locations, with updates to signature- and pattern-based solutions to be tested before installation. Installation is to be automated.
Authentication management	<ul style="list-style-type: none"> Authentication is to be enforced on all users, all account types and individuals with access to shared accounts to be identified Rules for password management and logging failed authentication attempts. 	<ul style="list-style-type: none"> Authentication is to not rely only on information from external sources. Personal accounts with rights according to user roles, group accounts only with permission. State-of-the-art password policy and MFA. Central login of all authentication attempts. 	<ul style="list-style-type: none"> All users are to have an account and authentication to be enforced on all users. Central logging of all authentication attempts. System to require MFA and state-of-the art password.
Baseline configuration	<ul style="list-style-type: none"> Baseline configuration is to be developed and documented. Changes to the baseline to be authorized, documented and tested, and baseline updated if necessary. System is to be regularly monitored for unauthorized changes. 	<ul style="list-style-type: none"> System is to be configured to a secure state after boot or re-boot. Basic configuration to be reviewed and documented after hardening. 	<ul style="list-style-type: none"> BDEW offers the procedure for creating the secure state, and NERC-CIP how it is to be managed.
Information protection	<ul style="list-style-type: none"> Methods for defining Cyber Security Information are to be determined, and procedures for handling, storage, transit and use set up. Disposal and reuse of Cyber Assets to include purging of all unnecessary 	<ul style="list-style-type: none"> Storage and transit of Cyber Security Information only encrypted. Confidential client data during development encrypted during transmission process or transit on removable media. 	<ul style="list-style-type: none"> NERC-CIP offers the general outline of Cyber Security Information use, and BDEW Whitepaper more specific outline for handling, storage, transit and use.

	Cyber Security Information.		
Patch management	<ul style="list-style-type: none"> • Patch management process required. • Both patches and their sources are to be evaluated regularly, and process to mitigate detected weaknesses or vulnerabilities is to be set up. 	<ul style="list-style-type: none"> • System updates must be available for entire contractual timeframe. Manufacturer support and security updates must be available for third party components for the contractual timeframe. 	<ul style="list-style-type: none"> • Responsible Entity is to set up a patch management process, and regularly evaluate and process patches published by vendors. • Vendors are to make the system updates they publish available to all their clients during the contractually stipulated timeframe.

5.1 Remote Access

For Remote Access the standards emphasize different aspects of Remote Access. BDEW makes tighter demands of the Remote Access systems and Remote Access scheme as such, but certain CIP’s demands that pertain to electronic access in general tighten the demands made by BDEW.

NERC-CIP’s most important demand is the demand for an intermediate system that prevents direct access to Cyber Assets. BDEW specifies several other demands, effectively turning the access servers to a bastion. Remote Access and be accessible only for predefined people following a predefined maintenance process. This is to be enforced with personal accounts with MFA. Sessions are to be allowed explicitly and individually by system operator and disconnected by System Operator or Timeout.

BDEW Whitepaper demands that no dial-in access to be made to terminal devices. Naturally NERC-CIP’s normal demands regarding communications and Electronic Security Perimeter are still in effect. Therefore, communications from the intermediate system must come through the Electronic access point as normal. This means no Dial-in access should be made directly to Cyber Assets inside the ESP.

5.2 Hardening

For Hardening the standard demands are very uniform, merely stressing slightly different aspect of Hardening. NERC-CIP emphasizes industry best-practices and disabling or removal of unnecessary component of the system, while BDEW Whitepaper emphasizes protection against physical input. Both demands are fully executable, and the software side of hardening is even automatable to a degree. They are relatively sufficient in and of themselves but may be complemented with for example software whitelisting preventing additions and running of additional software. For the Case Studies the different standard demands on hardening have negligible difference, as they are essentially demanding the same things with slightly different emphases.

5.3 Malicious code & Malware

The standards require a malicious code protection concept to be set up at appropriate locations. For the Case studies these locations are the access servers and the HMI-PC. If the Remote Access scheme has a dedicated Remote Access PC that should have Malware protection as well. On a pattern-based concept the patterns should be updateable in a timely and automated manner, and the updates themselves should be tested before application. The most likely solutions to these demands are a vendor malware suite with regular updates, and vendor code signing to ensure that every software component comes from a known vendor and therefore can be traced to said vendor in case of the software containing malicious code.

5.4 Authentication Management

Authentication management demands are mostly uniform, with NERC-CIP offering a more concrete set of demands for the password policy. BDEW Whitepaper would allow a limited range of actions without authentication, whereas NERC-CIP does not. Both standards also allow group accounts, but BDEW's demands for them are stricter. BDEW also offers a framework for the user concept. For the Case Studies both sets of demands are viable wither combined or alone. Remote Access may require the BDEW Whitepaper user concept framework being complemented with a separate Remote User role.

5.5 Baseline Configuration

According to both standards the system requires a documented baseline configuration, however, BDEW Whitepaper goes into more detail on how it is to be created, and NERC-CIP as to how said configuration is managed. CIP places much more of an emphasis on

updating the baseline configuration, and regular screenings for unauthorized changes, such as malicious code. The BDEW whitepaper demands are technically sufficient for ensuring the system operator knows what the system they operate contains, The CIP demands however are more thorough and therefore more useful for maintaining the security of the system.

5.6 Information Protection

Information protection from standard demand point-of-view mostly consists of demand NERC-CIP makes policy demands of defining Cyber Security Information, and the procedures for handling it, but leaves determining them up to the Responsible Entity. BDEW Whitepaper is more concerned with handling of information both during the design and use of the system.

5.7 Patch Management

Both standards demand that the security patches to system components must be available. This demand is naturally made with the caveat that the vendor that supplies the components makes and releases patches. BDEW Whitepaper makes more demands on patch management as a contractual maintenance service, while CIP is more focused on maintaining the security of the security patches.

6. CONCLUSIONS

Objective of this work was to investigate the possibility of combining standardization from multiple Market Areas for the purposes of creating a more universal, and possibly better cyber security infrastructure for an electricity distribution control system. The main method of this research was a literary review of the existing research on cyber security and the chosen standards, and of the standards themselves. The scope was limited to these two standards due to their prominence in the chosen market area, and the legislation of the market area placing less demands on technology and policy of control systems, and more to the results that are to be achieved with them. An additional, demonstrative research method was to investigate implementing two parts of a hypothetical Bulk Electric System, one typical, one optional: An HMI-PC and a Remote Access connection to the HMI. The purpose of these case studies was to demonstrate the feasibility of combining the standard demands with a practical example. Finally, the various implications of the standard demands regarding each other and the case studies were discussed.

As a result, the two standards were found to be perfectly compatible with each other. In some cases, one standard made more stringent or detailed demands than the other, in which case the more narrowly defined set of demands were used. It also was shown that setting up an HMI-PC and a Remote Access connection to it was entirely possible within the combined standard demands.

In its conclusion, this work has shown that it is entirely possible to build a cyber security template that is compliant with multiple standards. This is not surprising, as the threats and problems of cyber security are not specific to market areas, and as such different standards by and large address the same issues. Further, the work has shown this is not only possible, but also beneficial for the cyber security of the system being developed. In fact, something like this is likely to develop naturally as an existing system, or vendor components of a BES, being marketed to multiple different market areas is expanded and developed to accommodate needs of new customers and the standardization they operate under.

REFERENCES

- [1] NERC: CIP-003-8 - Cyber Security — Security Management Controls
https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-003-8&title=Cyber%20Security%20%E2%80%94%20Security%20Management%20Controls&Jurisdiction=United%20States
- [2] NERC: CIP-004-6 Cyber Security - Personnel & Training
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training&Jurisdiction=United%20States
- [3] NERC: CIP-005-6 Cyber Security — Electronic Security Perimeter(s)
[https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-005-6&title=Cyber%20Security%20%E2%80%94%20Electronic%20Security%20Perimeter\(s\)&Jurisdiction=United%20States](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-005-6&title=Cyber%20Security%20%E2%80%94%20Electronic%20Security%20Perimeter(s)&Jurisdiction=United%20States)
- [4] NERC: CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-006-6&title=Cyber%20Security%20-%20Physical%20Security%20of%20BES%20Cyber%20Systems&Jurisdiction=United%20States
- [5] NERC: CIP-007-6 Cyber Security - System Security Management
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber%20Security%20-%20System%20Security%20Management&Jurisdiction=United%20States
- [6] NERC: CIP-008-6 Cyber Security — Incident Reporting and Response Planning
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-6&title=Cyber%20Security%20%E2%80%94%20Incident%20Reporting%20and%20Response%20Planning&Jurisdiction=United%20States
- [7] NERC: CIP-009-6 Cyber Security - Recovery Plans for BES Cyber Systems
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-009-6&title=Cyber%20Security%20-%20Recovery%20Plans%20for%20BES%20Cyber%20Systems&Jurisdiction=United%20States
- [8] NERC: CIP-010-3 Cyber Security — Configuration Change Management and Vulnerability Assessments
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-3&title=Cyber%20Security%20%E2%80%94%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments&Jurisdiction=United%20States
- [9] NERC: CIP-011-2 Cyber Security - Information Protection
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-011-2&title=Cyber%20Security%20-%20Information%20Protection&Jurisdiction=United%20States
- [10] NERC: CIP-013-1 Cyber Security - Supply Chain Risk Management
https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-013-1

[1&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&Jurisdiction=United%20States](#)

- [11] NERC: ERO Enterprise | Regional Entities available: <https://nercstg.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>
- [12] BDEW Bundesverband der Energie- und Wasserwirtschaft: Whitepaper Requirements for Secure Control and Telecommunication Systems, 2018: https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf
- [13] EEF BDEW | European Energy Forum: <https://www.europeanenergyforum.eu/members/associate/bdew>
- [14] OE Oesterreichs Energie: Oesterreichs Energie, the representation of the interests of the Austrian e-economy, introduces itself: <https://oesterreichsenergie.at/wir/ueber-uns>
- [15] National Institute of Standards and Technology: <https://www.nist.gov/>
- [16] Zero Day Initiative: <https://www.zerodayinitiative.com/>
- [17] CVE Details: <https://www.cvedetails.com/>
- [18] ISO/IEC: ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, 2022
- [19] ISO/IEC: ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry, 2022
- [20] Rafał Leszczyna, Standards on cyber security assessment of smart grid, International Journal of Critical Infrastructure Protection, Volume 22, 2018, Pages 70-89, ISSN 1874-5482, available: <https://www.sciencedirect.com/science/article/pii/S1874548216301421>)
- [21] Rafał Leszczyna, Cybersecurity and privacy in standards for smart grids – A comprehensive survey, Computer Standards & Interfaces, Volume 56, 2018, Pages 62-73, ISSN 0920-5489, available: <https://www.sciencedirect.com/science/article/pii/S0920548917301277>
- [22] Rafał Leszczyna, A review of standards with cybersecurity requirements for smart grid, Computers & Security, Volume 77, 2018, Pages 262-276, ISSN 0167-4048, available: <https://www.sciencedirect.com/science/article/pii/S0167404818302803>
- [23] Mohammad Kamrul Hasan, AKM Ahasan Habib, Zarina Shukur, Fazil Ibrahim, Shayla Islam, Md Abdur Razzaque, Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations, Journal of Network and Computer Applications, Volume 209, 2023, 103540, ISSN 1084-8045, available: <https://www.sciencedirect.com/science/article/pii/S1084804522001813>