RECOMMENDED PRACTICE

DNV-RP-0575 Edition August 2021

Cyber security for power grid protection devices

DNV AS

FOREWORD

DNV recommended practices contain sound engineering practice and guidance.

Any comments may be sent by e-mail to *rules@dnv.com*

This service document has been prepared based on available knowledge, technology and/or information at the time of issuance of this document. The use of this document by other parties than DNV is at the user's sole risk. DNV does not accept any liability or responsibility for loss or damages resulting from any use of this document.

CHANGES - CURRENT

This is a new document.

Topic	*Reference*	*Description*
Rebranding to DNV, cross-references	All	Some of the documents referred to may not yet have been rebranded. If so, please see the relevant DNV GL document.

Acknowledgements

This recommended practice has been developed based on the results of a joint research and development project. The following companies, listed in alphabetical order, are acknowledged for their contributions to the project:

— Fingrid
— Statnett SF
— Svenska Kraftnät.

CONTENTS

Changes - current....................3
Acknowledgements....................4

Section 1 General....................7
1.1 Introduction....................7
1.2 Objective....................7
1.3 Scope....................7
1.4 Application....................7
1.5 References....................7
1.6 Definitions and abbreviations....................8

Section 2 Context....................12
2.1 Introduction....................12
2.2 Protection devices....................12
2.3 Substations....................13
2.4 The threat picture....................16
2.5 Rules and regulations....................18
2.6 Standards and guidelines....................19

Section 3 Attack surfaces....................21
3.1 Protection devices attack surfaces....................21

Section 4 Best practice to protect existing installations....................23
4.1 Cyber security management system....................23
4.2 Substation lifecycle....................25
4.3 Zones, conduits and barrier devices....................26
4.4 Secure remote access....................29
4.5 Malware control....................31
4.6 Hardening....................32
4.7 Patching....................33
4.8 Production data export....................33
4.9 Inventory management....................34
4.10 Incident response and recovery....................35
4.11 Intrusion detection system....................37
4.12 User authentication and authorization....................37
4.13 Logging and alarming....................38
4.14 Implementation of protective measures....................38

Section 5 Security for future substations......42
5.1 Digital substations 4.0......42

Section 6 Bibliography...... 43
6.1 Bibliography......43

Appendix A Alternative model......46
A.1 An alternative Purdue model......46

Appendix B Table based on section 4...... 47
B.1 Attack surface, threats and mitigation...... 47

Changes – historic......50

SECTION 1 GENERAL

1.1 Introduction

With power grids gradually becoming software intensive and digitally connected, their exposure to cyber threats has increased, putting key assets and the operations of an organization at risk. At the same time, the sophistication of cyber attacks is rising. This is adding to the threats sthat ecurity teams for information technology (IT) and operational technology (OT) must deal with, often without experience or any suitable cyber security solutions readily available. The power grid is vulnerable to cyber security incidents that may, in the worst case, be used to trip circuit breakers, as seen during two incidents in the Ukraine /4/, or to prevent protective systems from working in the case of an actual fault.

The purpose of power system protection is to isolate a faulty section of the electrical power system from the rest of the live system. Once this is isolated, the remaining portion of the power system can function to an acceptable extent without any severe damage due to the current fault /1/. As such, securing the protection devices is essential for the stability of the power grid.

1.2 Objective

The objective of this recommended practice (RP) is to propose practical guidelines describing attack surfaces, potential threats and possible countermeasures that a company should take into consideration when planning to improve the security of its protection devices and the digital technology within its substations. The RP aims to improve security for second and third generation substation protection devices. It offers a set of industry-reviewed activities to include when planning and assessing the implementation of security measures and controls in the power system.

1.3 Scope

This recommended practice is applicable to companies involved in operating, managing and securing existing (second and third generation) substations, and describes 45 risk reducing measures, covering people, processes and technology, to minimize attack surfaces and counter threats to power systems. These measures are based on a comprehensive review of current European Union (EU) and United States (US) legislation, and currently applicable standards and guidelines on cyber security in operational technology (OT).

Future substation infrastructure (digital substation 4.0) is briefly discussed.

1.4 Application

This recommended practice applies to power grid protection devices and operators (transmission and distribution service operators (TSO and DSO)) of power grids. It is also applicable for manufacturers and regulatory authorities in the power system. The intended audience is management level security personnel and operating personnel.

1.5 References

Table 1-1 lists the standards used in this document.

Table 1-1 Standards

Document code	*Title*
IEC 60870-5 series	Telecontrol equipment and systems. Part 5: Transmission protocols (101/104)

Document code	*Title*
IEC 60870-6 series	Telecontrol equipment and systems. Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations (ICCP/TASE.2)
IEC 61850 series	Communication networks and systems for power utility automation
IEC 61869-9	Instrument transformers - Part 9: Digital interfaces for instrument transformers
IEC 61968 series	Application integration at electric utilities - System interfaces for distribution management (CIM)
IEC 61970 series	Energy management system application program interface (EMS-API) (CIM)
IEC 62351 Series	Power systems management and associated information exchange - Data and communications security
IEC 62439-3	Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)
IEC 62443-2-1	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
IEC/TR 62443-2-3	Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment
IEC 62443-3-2	Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design
IEC 62443-3-3	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
IEEE 1815	IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)
ISA-TR84.00.09	Cybersecurity related to the functional safety lifecycle
ISO/IEC 27001	Information technology - Security techniques - Information security management systems - Requirements
ISO/IEC 27033 series	Information technology - Security techniques - Network security
ISO/IEC 27035 series	Information technology - Security techniques - Information security incident management
NERC CIP-XXX series	Critical Infrastructure protection
NIST SP 800-series	The series comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities
NIST TN 2051	Cybersecurity Framework Smart Grid Profile

1.6 Definitions and abbreviations

1.6.1 Definition of verbal forms

The verbal forms defined in Table 1-2 are used in this document.

Table 1-2 Definition of verbal forms

Term	*Description*
shall	verbal form used to indicate requirements strictly to be followed in order to conform to the document
should	verbal form used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others
may	verbal form used to indicate a course of action permissible within the limits of the document

1.6.2 Definition of terms

The terms defined in Table 1-3 are used in this document.

Table 1-3 Definition of terms

Term	*Definition*
digital substation 4.0	fourth (next) generation substation, with the goals of reducing copper wiring, the environmental impact, installation costs and engineering times, and improving personnel safety
protection devices	devices to sense an abnormal condition and trip a circuit breaker when a fault is detected
substation	high-voltage electric system facility

1.6.3 Abbreviations

The abbreviations described in Table 1-4 are used in this document.

Table 1-4 Abbreviations

Abbreviation	*Description*
AD	active directory
AO	asset owner
BGH	big game hunting
CEN	European Committee for Standardization
CERT	computer emergency response team
CIP	critical infrastructure protection
CSF	cyber security framework
CSIRT	computer security incident response team
CSMS	cyber security management system
CSRS	cyber security requirement specification
DMZ	demilitarized zone
DOS	denial of service

Abbreviation	*Description*
DSO	distribution service operator
ENISA	European Union Agency for Network and Information Security
EWS	engineering workstation
FW	firewall
GOOSE	generic object oriented substation event
HSR	high availability seamless redundancy
HMI	human machine interface displays
IACS	industrial automation and control systems
ICS	industrial control system
IDS	intrusion detection system
IED	intelligent electronic device
IGGN	INEOS Group Operations Guidance Note
IMS	information management system
IIOT	industrial internet of things
IOT	internet of things
IPS	intrusion prevention system
ISA	International Society of Automation
IT	information technology
MAC	media access control
ML	maturity level
MPLS	multiprotocol label switching
MU	merging unit
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	operational technology
PRP	parallel redundancy protocol
PS	product supplier
RAS	remote access server
RBAC	role-based access control
RP	recommended practice
RSTP	rapid spanning tree protocol
RTU	remote terminal unit
SANS	sysadmin, audit, network and security

Abbreviation	*Description*
SCADA	supervisory control and data acquisition
SAMU	stand-alone merging unit
SAT	system acceptance test
SI	integration system provider
SIEM	security information and event management
SL	security level
SL-T	security level target
SM	maintenance service provider
SSH	secure shell
SuC	system under consideration
TSO	transmission service operator
UCAIug	Utility Communication Architecture Internal User Group
UPS	uninterruptible power supply
USB	universal serial bus
VLAN	virtual local area network
VPN	virtual private network
WLAN	wireless local area network
WSUS	Windows software update service

SECTION 2 CONTEXT

2.1 Introduction

This section describes the context of this RP, including what protection devices are, what substations are, the threat picture, and the rules, regulations and standards that are applicable. It also outlines the attack surface for protection devices.

2.2 Protection devices

Protection devices are devices to detect short-circuits and system faults (abnormal and dangerous power grid conditions) and will trip a circuit-breaker. Originally, protection relays were electro-mechanical relays with moving parts. Then came slid state relays. Most of these devices have, by now, been replaced by modern technology relays. Such devices are still used in old installations, but the industry is moving to numerical relays. Fully numerical relays were commercially introduced in 1984. These devices are software-controlled systems where the software performs functions such as signal processing and running protection algorithms. Microprocessor relays with having communication possibilities were introduced at the end of the 1980s. This was the beginning of using serial communication of process signals within a substation and the first step in reducing signal cabling and process wiring within substations. A generic block-diagram is shown in Figure 2-1 /8/.

Protection devices are used for generators, transformers, busbars, transmission lines, distribution lines and cables.

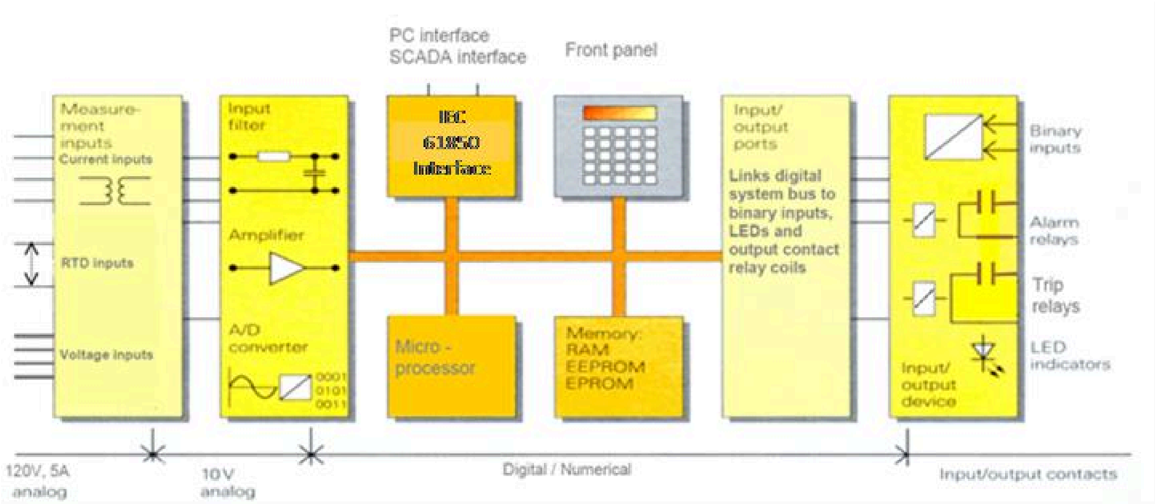

Figure 2-1 Components of a typical microprocessor-based relay. Source: Power System Relaying Committee, 2009. Understanding microprocessor-based technology applied to relaying. Adapted and reprinted with permission from IEEE. Copyright IEEE 2009. All rights reserved. /8/

The protection system is normally a redundant system. The simple principle behind the design is that faults shall be cleared even if one component of the fault clearance system is out of service (faulted). The principle is known as N-1.

The requirements for the fault clearance system can be described with the following factors:

- Reliability of fault clearance:
  - Dependability of protection: the probability that a protection device will not have a failure to operate under given conditions for a given time interval.
  - Security of protection: the probability that a protection device will not have an unwanted operation under given conditions for a given time interval.
- Redundancy: in an item, the existence of more than one means for performing a required function. In fault clearance, a fault in the power system shall be cleared even if one part of the fault clearance system is out of order, often referred to as N-1.
- Selectivity of protection: the ability of a protection device to identify the faulty section and/or phase(s) of a power system. The aim is to only trip the section where the fault has occurred and not disconnect electricity customers in unaffected sections, and at the same time to limit damage to equipment and the danger to people and the environment.
- Fault clearance time: the time interval between the fault inception and fault clearance. This time shall be as short as possible without violation of selectivity.

2.3 Substations

Power grid protection devices are installed in the substations. The design of substation automation systems, including their external communication connections, is of critical importance to reduce and mitigate the inherent vulnerabilities of these systems.

There are four generations of substations to distinguish between:

1) First generation are the very conventional substations that, at the end of the 1970s, started to be equipped with a remote terminal unit (RTU) to send a small amount of substation signals with very slow communication means to the supervisory control and data acquisition (SCADA) systems that were being introduced. At that time still with mimic-boards in the control system. All substation signals are hardwired to the RTU.
2) Second generation are conventional substations built or refurbished at the end of the 1980s and beginning of the 1990s. Substation control system were introduced in these substations. Protection relays became microprocessor based and in the mid-1990s, started to use serial communication to the control systems and/or RTUs started to be used. This was the first step in reducing signal cabling in the substations. Human machine interface displays (HMI) were also introduced, on both the SCADA level and as well as on the substation level, as part of the substation control systems.
3) Third generation are the substations equipped with substation automation systems based on IEC 61850, which was introduced in the early 2000s. These have protection and control devices on bay level and station level communicating, sharing data and sending generic object oriented substation event (GOOSE) messages on a station bus, with a station level HMI and gateway to perform the RTU function for remote monitoring and control with SCADA level. Figure 2-2 shows the simplified network design of the substation automation system, including the connection to SCADA. The figure is aligned with the different layers as defined in the Purdue model.
4) Fourth generation is what is referred to as a fully digital substation with a process bus directly digitally connecting the protection and control devices to the process, thus reducing all copper hardwiring to a minimum. This is the generation that today is starting to be built in some TSOs although most substations being built worldwide will still be of third generation, since this model is commonly used to illustrate security zones.

Figure 2-2 shows a simplified network design of the substation including related systems. The figure is aligned with the separate layers as defined in the Purdue model /3/, since this model is commonly used to illustrate security zones.

The Purdue model used in this RP is a reference model illustrating a generic IT/OT system architecture for substations. In this context, the chosen model is applied by and agreed to by the Nordic TSOs. The architecture includes vertical segmentation, a demilitarized zone (DMZ) and a centralized overall SCADA system. This model is used throughout the RP to illustrate statements and best practices. It shall be noted that there are many applications of the Purdue model for substation and grid operation systems, and an alternative view can be found in App.A. ENISA has created another commonly used version /27/.

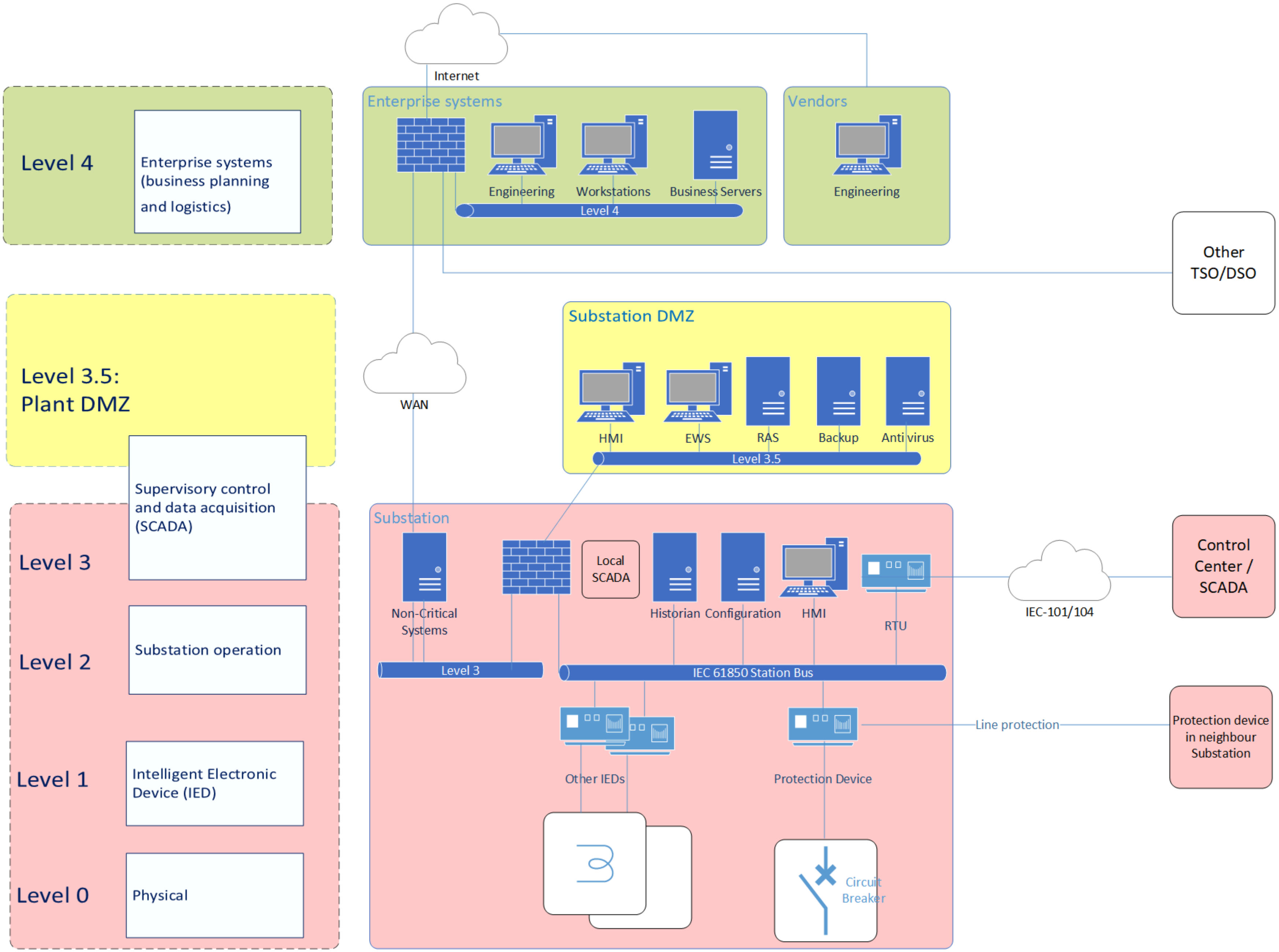

Figure 2-2 Third generation substation

In this sample a local substation demilitarized zone (DMZ) is shown. An alternative is to have a central DMZ as shown in Figure 4-6.

2.4 The threat picture

Since most protection devices are software-controlled systems with external interfaces, they are vulnerable to cyber security incidents. Two incidents in Ukraine demonstrate how vulnerabilities in the protective systems were used to trip circuit breakers. In the first of these attacks, seven 110 kV and 23 35 kV substations were disconnected for three hours, causing approximately 225 000 customers to lose power. The steps involved in this attack are shown in Figure 2-3 based on a description from SANS /4/ and ISA /5/.

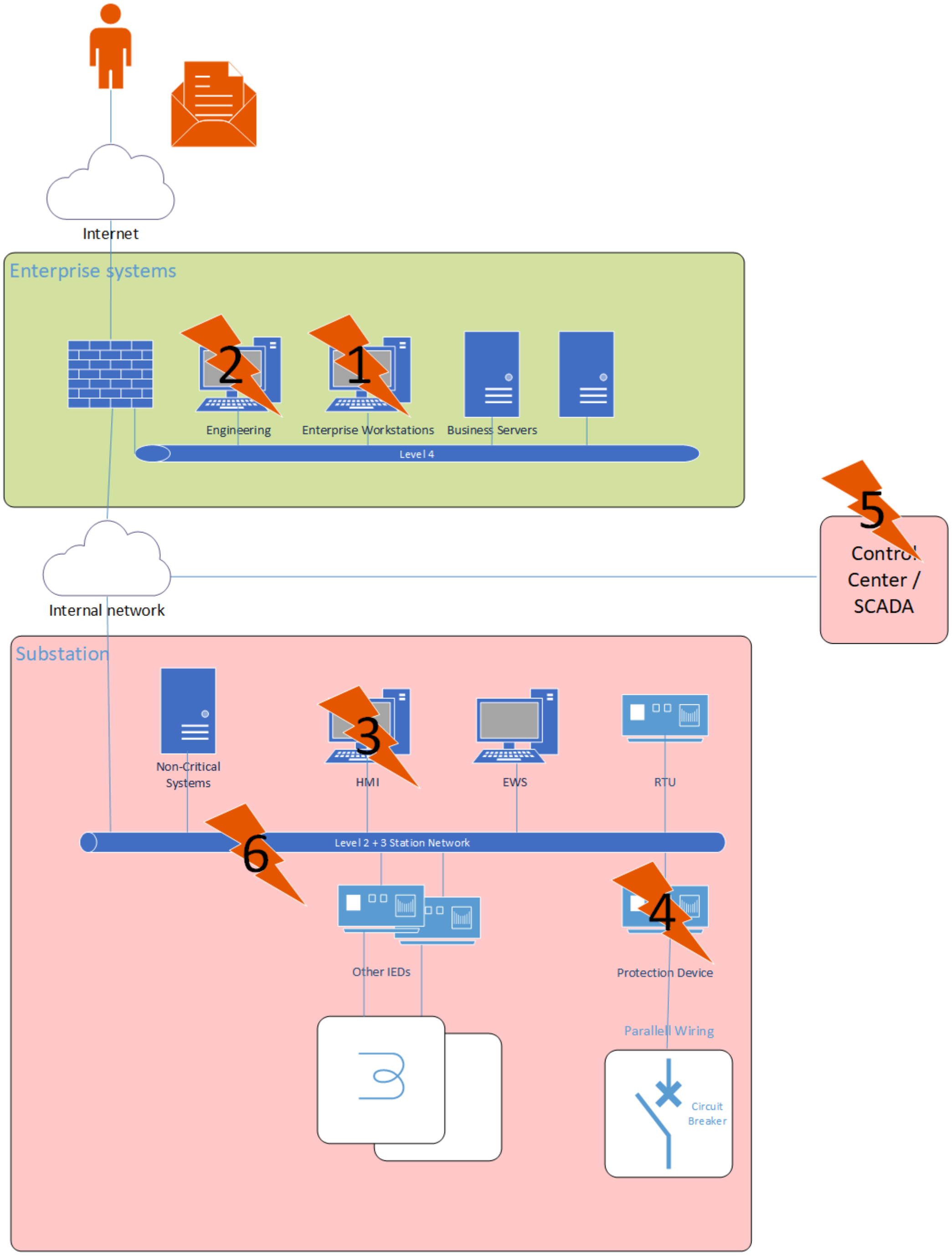

Figure 2-3 Cyber attack on Ukraine power grid

Attack preparation:

1) An employee opened an e-mail containing a variant of the 'Black energy' malware. The malware to other hosts scanned and propagated.

2) The malware detected a secure shell (SSH) tunnel to the OT domain. It recorded keyboard strokes and captured passwords and credentials. No multifactor authentication was required.
3) The malware used the SSH tunnel to connect to the OT system and installed malware on the OT system.

The attack:

4) The SSH tunnel was activated to control the HMI. Commands were sent to the protection device to trip the breakers.

To hide the attack:

5) The UPS on the control centre was shut down to disable the centre. In addition, the call centre was jammed by a denial of service (DOS) attack.

6) Passwords were changed in local systems to prevent the operator from taking control. Workstation and server disks were erased. Gateway firmware was overwritten.

In addition to targeted attacks as seen in Ukraine, the protective systems are vulnerable to more generic cyber incidents including malware and potential cryptoviruses. Recent incidents based on ransomware could, if replicated on protective systems, have severe effects. The EU's computer emergency response team CERT-EU) warns the energy industry about 'big game hunting' (BGH), which is highly targeted, low-volume, but high-return ransomware attacks against large organizations. It seems that, in 2020, at least 10 energy companies in Europe, Asia, Africa and North America have fallen victim to BGH.

2.5 Rules and regulations

2.5.1 General

The following rules and regulations have been identified as relevant to cyber security for power grid protection devices.

2.5.2 EU

The 2008 Directive on European Critical Infrastructures has been the basis of the EU approach to cyber security in power grids.

In February 2013, the European Commission published a cyber security strategy outlining the EU's vision for building cyber security capabilities.

The Network and Information Systems (NIS) Directive provides rules forming the basis for the current EU cyber security regime. The NIS Directive requires the designation of national competent authorities, the creation of computer-security incident response teams (CSIRT), and the adoption of national cyber security strategies /25/.

The Cybersecurity Act /23/ aims to strengthen the EU's response to cyber attacks and improve cyber resilience. The Act requires ENISA to improve coordination and cooperation in cyber security across EU member states and EU institutions, agencies and bodies.

In April 2019, the Commission issued *Recommendation on cybersecurity in the energy sector*, which contains guidelines that member states and key stakeholders (particularly energy grid operators) should take into account when making decisions about their infrastructure /24/. These measures include guidelines on cyber security risk analysis and preparedness, updating software and hardware, and establishing an automated monitoring capability for security events in legacy environments /6/.

2.5.3 North America

The *North American Electric Reliability Corporation Critical Infrastructure Protection* (NERC CIP) framework is a set of requirements designed to secure the assets operating North America's bulk electric system. It consists of nine standards and 45 requirements for security of electronic parameters, protection of critical cyber assets, personnel and training, security management and disaster recovery.

All organizations subject to NERC CIP shall identify critical assets and perform regular risk assessments for their identified assets. Policies shall be in place to access, monitor and modify the configuration of assets. NERC CIP further requires the use of firewalls to block vulnerable ports and implementation of tools that monitor for cyber attacks.

Failure to comply with NERC CIP can lead to fines, sanctions or other actions /21/.

2.5.4 Other regulations

The NIST framework is frequently used as the foundation for national regulation. This means that the laws are based on the five functions that make up NIST: identify, protect, detect, respond and recover. With this best practice approach to regulation, the measures suggested in the RP are applicable in that context.

2.6 Standards and guidelines

There are a large number of standards and guidelines which may be applicable to cyber security for power grid protection devices. Standards from e.g. NERC, NIST, BDEW, IEC, ISA, ISO, CEN, CENELEC and ETSI are relevant. In this RP the purpose is to focus on some applicable standards. Figure 2-4 /7/ gives a high-level positioning of the European standards.

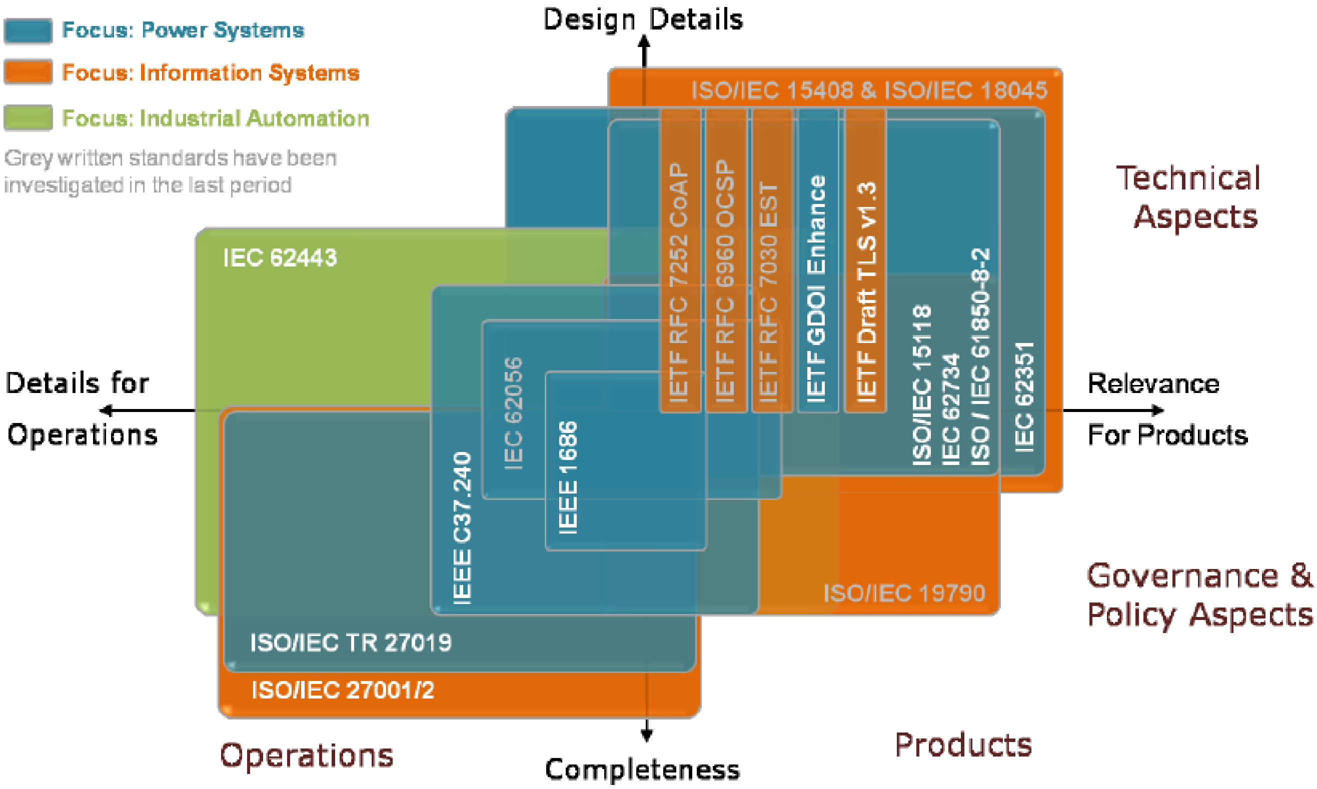

Figure 2-4 Relevant standards for cyber security and power systems. Source: © CEN, reproduced with permission. © CENELEC, reproduced with permission. © ETSI, reproduced with permission /7/

The National Institute of Standards and Technology (NIST) is an American organization run by the US Department of Commerce. It publishes standards applicable to many sectors, including cyber security and energy. The NIST framework for improving cyber security applies to this RP /10/, several of the standards in the SP 800-series /22/, and the Cybersecurity Framework Smart Grid Profile. The standards cover technology, processes and people, with activities ranging from policy writing and risk assessment to penetration testing and network monitoring.

SECTION 3 ATTACK SURFACES

3.1 Protection devices attack surfaces

Figure 3-1 shows potential cyber security attack surfaces for protection devices. Incidents exploiting these attack surfaces may in the worst case trip circuit breakers or prevent protective systems from working in the case of an actual fault.

These attack surfaces (identified by numbers in Figure 3-1), their related threats and the corresponding mitigation guidelines (topics are in section 4) are listed in Table B-1. Each number in Figure 3-1 corresponds to a number in Table B-1. The threats are a subset of ISF /9/ and MITRE /15/. For a more detailed related analysis, the complete MITRE ATT&CK for ICS list of threats may be used. CIGRE has defined an approach to attack modelling /16/.

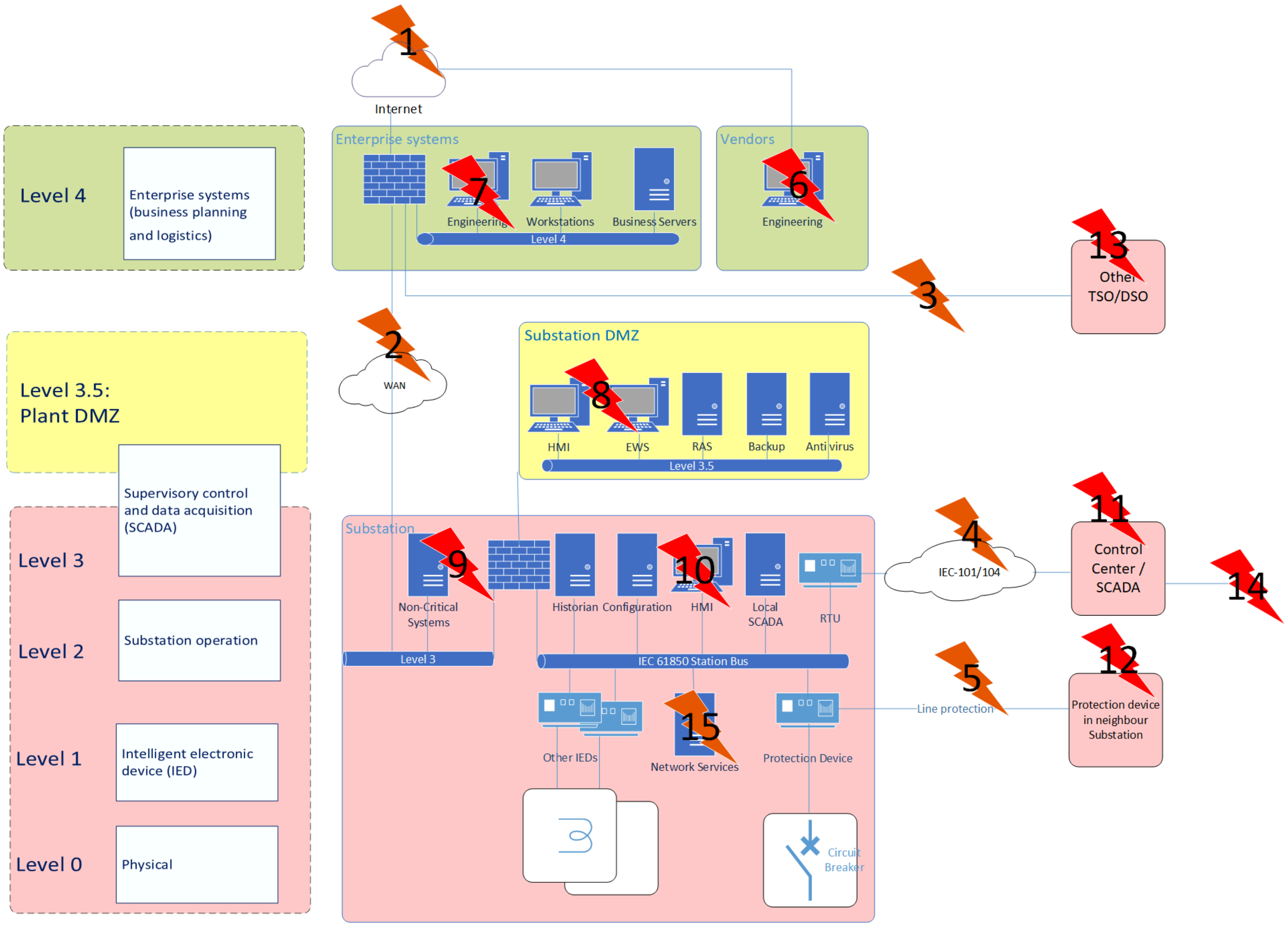

Figure 3-1 Protection device attack surfaces

SECTION 4 BEST PRACTICE TO PROTECT EXISTING INSTALLATIONS

4.1 Cyber security management system

The organization responsible for securing the substations should implement a cyber security management system (CSMS). Such a system should include security measures related to the people, process and technology, see Figure 4-1.

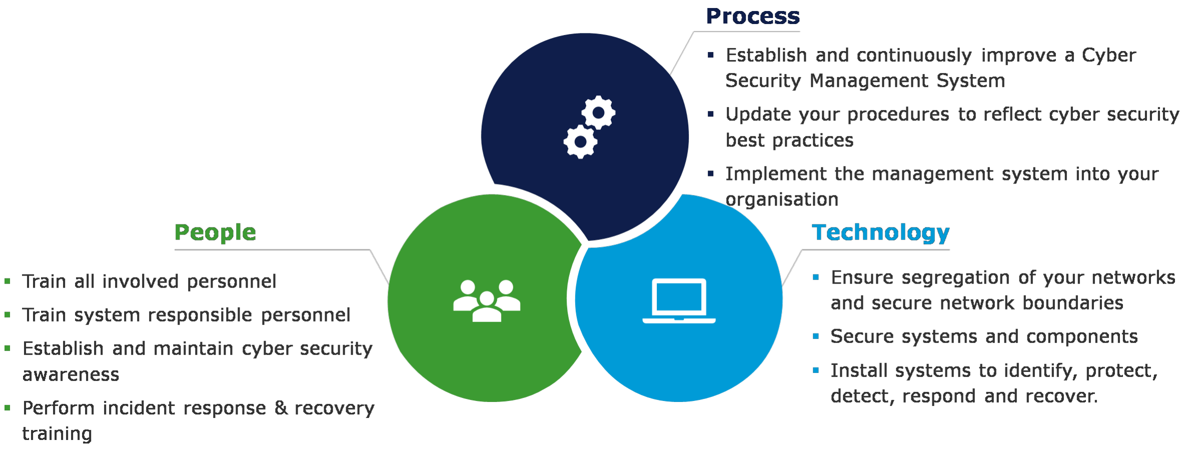
Process
Establish and continuously improve a Cyber Security Management System
Update your procedures to reflect cyber security best practices
Implement the management system into your organisation
People
Train all involved personnel
Train system responsible personnel
Establish and maintain cyber security awareness
Perform incident response & recovery training
Technology
Ensure segregation of your networks and secure network boundaries
Secure systems and components
Install systems to identify, protect, detect, respond and recover.

Figure 4-1 People – process - technology

Understanding the importance of people - process - technology and their interaction is essential given that the electrical grid environment consists of numerous substations and that the substation lifecycle can last for decades before it is updated or reaches the 'end of life'. Given the capital expenditure required, the equipment specifications and the need to maintain very high system availability, upgrade and replacement cycles are longer than could be expected for IT components which have a lifecycle of three to five years. Historically, OT was not connected to external networks and cyber security was not a design requirement, but the integration of these systems is now commonplace. This exposes the OT network and equipment to new threats and exposes vulnerabilities which were not previously exploitable. These facts make this electrical grid environment 'vulnerable by default', a point that should be understood throughout the organization. Intelligently utilizing all of an organization's assets, people - process - technology, may mitigate the inherent risks.

A minimum security baseline shall be present in all parts of both the control and enterprise networks. The enterprise networks are the ideal place for an attacker to gain a foothold in order to establish persistence, laterally move to other zones of the network, compromise accounts, escalate privilege on systems and protectively marked documents, exfiltrate information, and reconnoitre and map the network. Armed with this knowledge, an attacker can design and implement a solid plan to execute the attacks most likely to work in the compromised environment.

The best principles related to people competence and awareness are described in ISO/IEC 27001 chapters 7.1 and 7.2. The ISA/IEC 62443-2-1 standard details these principles for the OT environment and includes the requirements for training in handling crisis situations.

It is important to include all employees in the awareness programme - not merely OT staff. Typically sustainable and measurable improvements of employee cyber security awareness are achieved when combining testing with repeated training two to three times per year.

The best practice for processes is to implement a cyber security management system (CSMS) based on ISO/IEC 27001 or the NIST cyber security framework /10/ /17/. The ISA/IEC 62443-2-1 standard tailors the ISO/

IEC 27001 management system to the OT environment while the NIST CSF cybersecurity framework smart grid profile tailors the NIST CSF to the power grid environment /2/.

Figure 4-2 shows the components of the ISA/IEC 62443-2-1 based on the cyber security management system. It is also important to understand that these standards only provide a guide to the processes which should be adjusted to find the 'easy wins' by identifying methods and procedures that strengthen the organization.

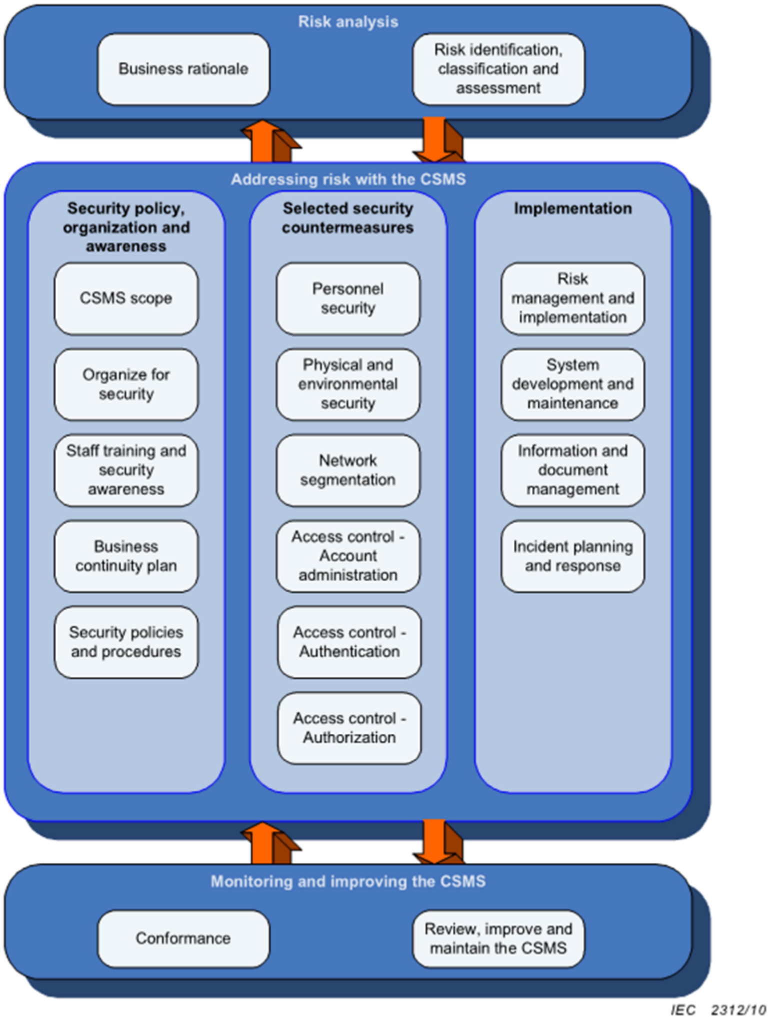
Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control - Account administration
Access control - Authentication
Access control - Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS
IEC 2312/10

Figure 4-2 Cyber security management system. Source: IEC 62443-2-1 ed.1.0 Copyright © 2010 IEC Geneva, Switzerland. www.iec.ch (published with permission from IEC)

The maturity of the organization may be assessed according to the capability maturity model (CMM) developed by the Software Engineering Institute at Carnegie-Mellon University /13/. Both NIST and ISA/IEC 62443 have adopted this concept. ISA/IEC 62443-2-1 defines four maturity levels (ML), as described in Table 4-1.

Table 4-1 Maturity levels

Number	*Maturity level*	*Description*
ML1	Initial	Processes are performed in an ad-hoc and often undocumented manner.
ML2	Managed	Processes are documented.
ML3	Defined	Processes are documented and practised.
ML4	Improving	Effectiveness or improvements of the processes, or both, can be demonstrated.

Organizations responsible for cyber security in power grids should regularly assess their maturity level with an aspiration to achieve the highest.

For more information, see ISO/IEC 27001, ISA/IEC 62443-2-1, NIST CSF /10/ /17/ and NIST TN 2051.

4.2 Substation lifecycle

Figure 4-3 shows the ideal high-level cyber-security activities that shall be performed during the substation lifecycle. The figure indicates where these activities are described in the ISA/IEC 62443 standard.

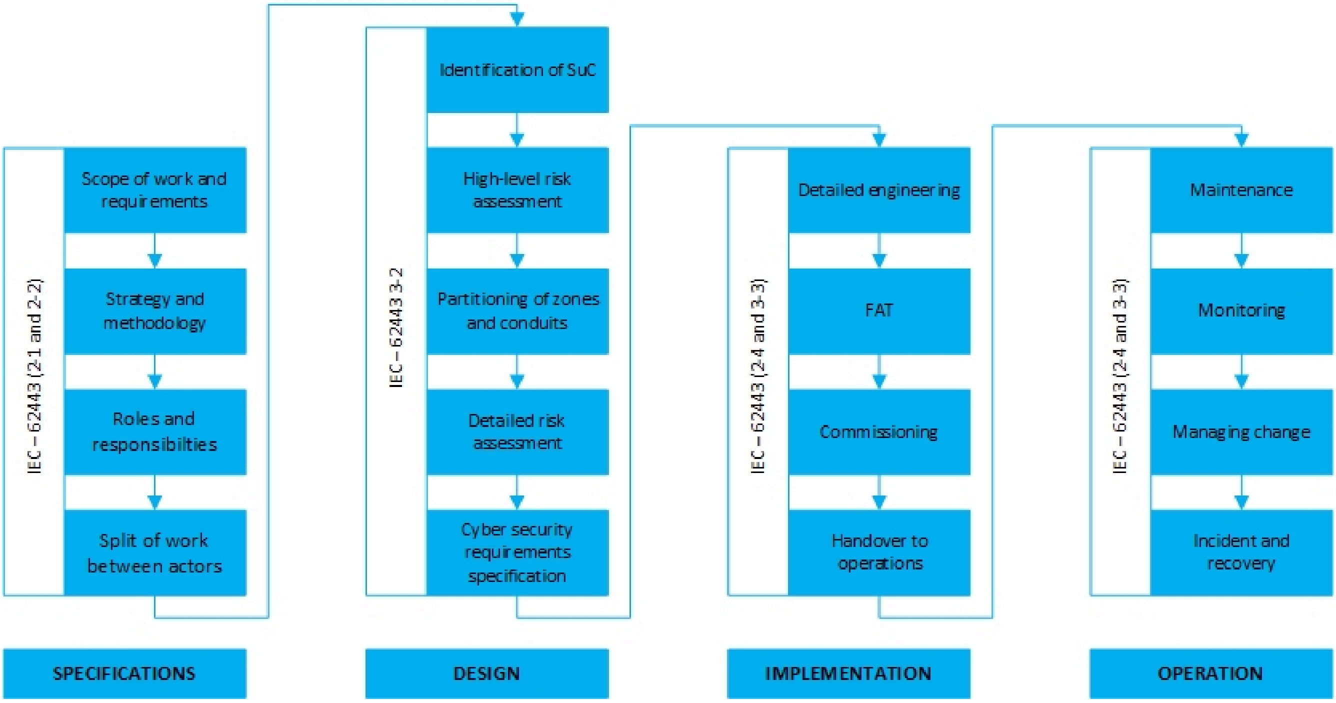
IEC – 62443 (2-1 and 2-2)
Scope of work and requirements
Strategy and methodology
Roles and responsibilties
Split of work between actors
IEC – 62443 3-2
Identification of SuC
High-level risk assessment
Partitioning of zones and conduits
Detailed risk assessment
Cyber security requirements specification
IEC – 62443 (2-4 and 3-3)
Detailed engineering
FAT
Commissioning
Handover to operations
IEC – 62443 (2-4 and 3-3)
Maintenance
Monitoring
Managing change
Incident and recovery
SPECIFICATIONS
DESIGN
IMPLEMENTATION
OPERATION

Figure 4-3 Cyber security during the substation lifecycle

In addition to these high-level activities particular attention should be paid to the supply chain relating to critical components. Software integrity shall be assured from when the products are shipped from the vendor until the product is put into operation. Shipping, storage and the commissioning phase are potential weak points in cases where a high number of actors have access to the site. Software is often downloaded over the public internet and in all cases shall be subject to integrity checking. Common methods of validation include the use of digital signatures and checksums.

A clear definition of roles and responsibilities during these activities is required. According to ISA/IEC 62443-2-2, there are four roles:

— asset owner (AO) (=TSO or DSO)
— maintenance service provider (SM)
— integration service provider (SI)
— product supplier (PS).

Note that the SM, SI and PS may be the same organization.

Table 4-2 contains examples of the responsibilities of these roles in a substation lifecycle.

Table 4-2 Responsibilities example

Activity	*Phase*	*Main responsible*	*Performed by*	*Input provided by*
Scope of work and requirements	Specification	AO	AO	
Strategy and methodology	Specification	AO	AO	
Roles and responsibilities	Specification	AO	AO	SI, SM, PS
Split of work between actors	Specification	AO	AO	SI
Identification of the system under consideration	Design	AO	AO/SI	AO, SI, PS
High-level risk assessment	Design	AO	AO/SI	AO, SI, PS
Partition the SuC into zones and conduits	Design	AO	AO/SI	AO, SI, PS
Detailed cyber security risk assessment	Design	AO	AO/SI	AO, SI, PS
Establish the cyber security requirements specification	Design	AO	AO/SI	AO, SI, PS
Detailed engineering	Implementation	AO	AO, SI, PS	AO, SI, PS
FAT	Implementation	SI	PS	
Commissioning	Implementation	SI	PS	
Handover to operation	Implementation	SI	SI	AO, PS
Maintenance	Operation	AO	SM	PS
Monitoring	Operation	AO	SM	PS
Management of change	Operation	AO	SM	PS
Incident response and recovery	Operation	AO	SM	AO, PS, CERTs, SOC, etc.

For more information, see ISA/IEC 62443-2-2 and DNV-RP-G108 /9/.

4.3 Zones, conduits and barrier devices

Reducing cyber risk on industrial control systems is achieved by segregating the network into different zones and implementing barrier devices between these zones. One approach is to use the ISA/IEC 62443-3-2 draft standard, which describes how zones and conduits shall be defined, and how a security level target (SL-T) shall be assigned to the zones and conduits. This SL-T will then dictate which requirements to apply for the systems involved. Figure 4-4 shows a simplified example zone and conduits model for substations. This model shows that the current practice is to have separate zones for critical and non-critical systems.

Changing the zone model for an operating substation will most probably mean downtime. The recommended approach is to establish the new zone model in parallel and implement new systems in the new model. Firewalls may be run in 'learning mode' before network traffic is blocked. However, the most secure way is to define the required traffic communications together with the service provider and OT staff in advance. Then, create the zone modelling and identified firewall configuration and inspect the traffic together with the OT staff to adjust the firewall rules as required.

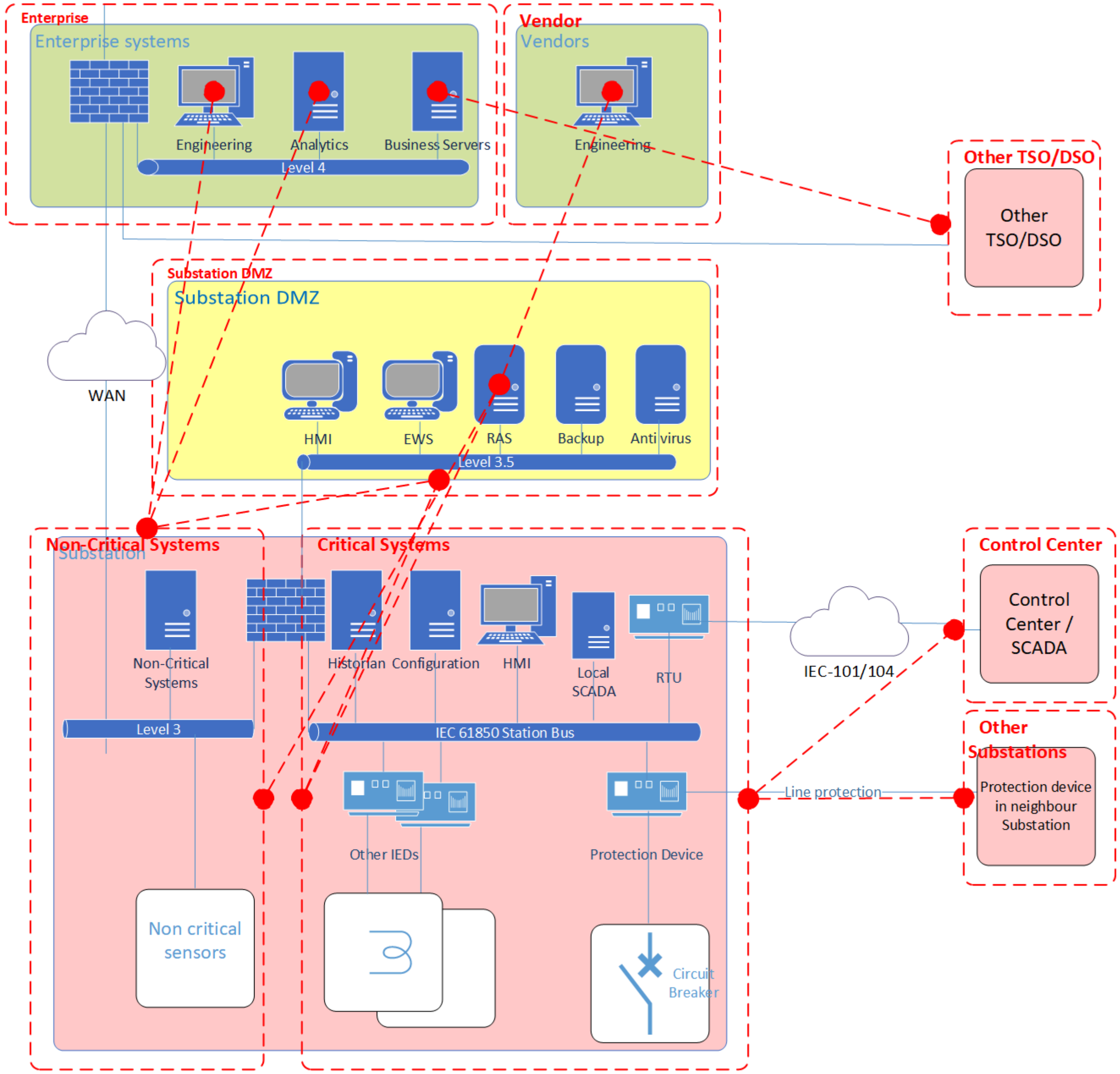

Figure 4-4 Zones and conduits model for third generation substations

Best practice dictates the use of firewalls between the zones. Ideally application layer firewalls (OSI layer 7) should be used, but their support for industrial protocols is limited. Filtering on ports and IP addresses (OSI layer 3-4) is the most used option. The installation of new layer 3-4 firewalls may require the redesign of the IP address scheme. For networks with requirements for low latency, and to reduce IP addressing complexity, level 2 firewalls may be considered in combination with other security measures.

NIST SP 800-41 or ISO 27033 may be used as a guideline for configuring, maintaining, monitoring and auditing the firewalls. It is good practice is to implement sufficient networking and system services (e.g.

time services and a user directory) in the zones to enable 'island mode'. The external firewalled connection may then be disconnected according to the incident response plan, see [4.10]. Such a concept will limit the number of openings in the firewall, which in turn will reduce vulnerabilities and simplify monitoring and audits.

Non-critical sensors for e.g. condition-based monitoring and wireless traffic (if allowed) shall always be kept in separate zones.

Internet of things (IOT) and industrial internet of things (IIOT) devices (or similar devices) shall be in separate zones. IOT devices are cheap, consumer-based devices with few security features built in and therefore represent a significant risk to the network. In addition, they may be connected to the internet with a 3G/4G/5G wireless connection.

All firewalls shall be regularly audited, and any changes in configuration should be handled in a management of change (MOC) system. Regular penetration testing should be performed.

External conduits for unsecured protocols like IEC-101/104 shall be upgraded with secure versions or secured in e.g. virtual private network (VPN) tunnels or in dedicated networks with monitoring of firewalls and network traffic.

For more information, see ISA/IEC 62443-3-2, NIST SP 800-41, ISO 27033 and NERC CIP-005.

4.4 Secure remote access

Allowing vendors and own employees to connect from the internet/intranet into the substation for maintenance and operation introduces a higher risk of cyber security incidents. As such, correct implementation is necessary.

Operating hundreds of geographically spread substations is nearly impossible without remote access. The best practice is to build a dedicated remote access system, buy a dedicated product or hire a dedicated service. These approaches all introduce solution-specific pros and cons. Regardless of the solution, a system for remote access to substations should always include the following security functions:

- Physical security requirement for the vendor site (if vendors are allowed to work from the vendor site).
- Client PC requirements, including hardening, patching and malware protection (preferably a behaviour-based endpoint protection system). The client PC security status should be verified with a 'host checker'.
- Multifactor authentication.
- Secure tunnel from client to jump-host/remote access server (RAS) (if vendors are allowed to connect from their location, two jump-hosts/RAS may be involved).
- Authorization on jump-host/RAS based on work orders, role (role-based access control (RBAC)) and location.
- Hardened jump-host/RAS implementation at DMZ, establishing a new remote session to target.
- Session recording. The session recordings shall be regularly audited and analysed.
- '4-eyes'. Critical actions shall be approved by two or more persons.
- Centralized logging and monitoring of all events.
- Threat control of network traffic (IPS) ideally on source network, DMZ and destination network.
- Malware check of transferred files (if file transfer is allowed). Sandboxing techniques are preferred, executing software in a safe controlled environment before moving to production.
- Closing of inactive or idle sessions.

Remote access should never be allowed from internet unsecured locations. In the case of remote access by vendors/suppliers, a physical authentication/verification process shall also be in place to ensure the right person is given access.

By building a centralized solution for power stations and substations, it will be easier to manage traffic flows, users and their access. It will also introduce a central location for managing and accessing the substation environment, making internet access at the substation unnecessary. The solution relies on multiprotocol label switching (MPLS) or similar dedicated connections from a centralized location to substations. Where dedicated data connections are not possible, an internet connection with a VPN may be considered if no direct connection to the internet is provided and the VPN is terminated on a separate firewall. This firewall shall only allow tunnel traffic from the centralized location with fine-grained access control.

Figure 4-5 shows a RAS solution giving access to the engineering workstation (EWS) and HMI in substation DMZ.

Another concept is to have a central DMZ with a virtual server running virtual implementations of EWS and HMI as shown in Figure 4-6. Such a concept may simplify software upgrades and control.

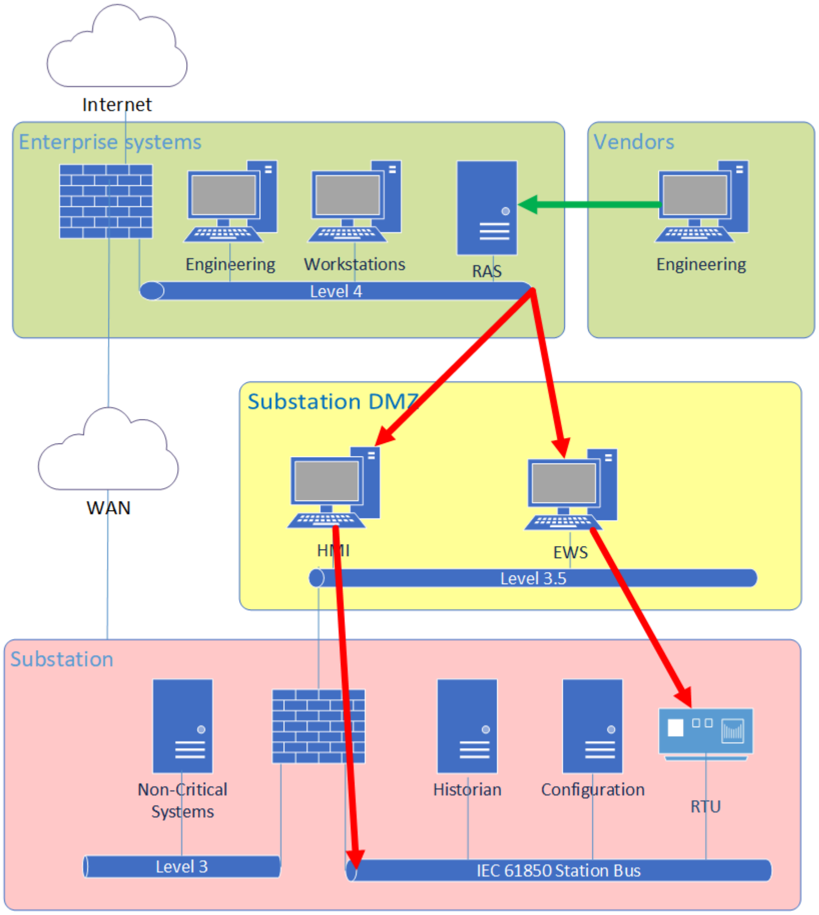

Figure 4-5 Traditional central RAS

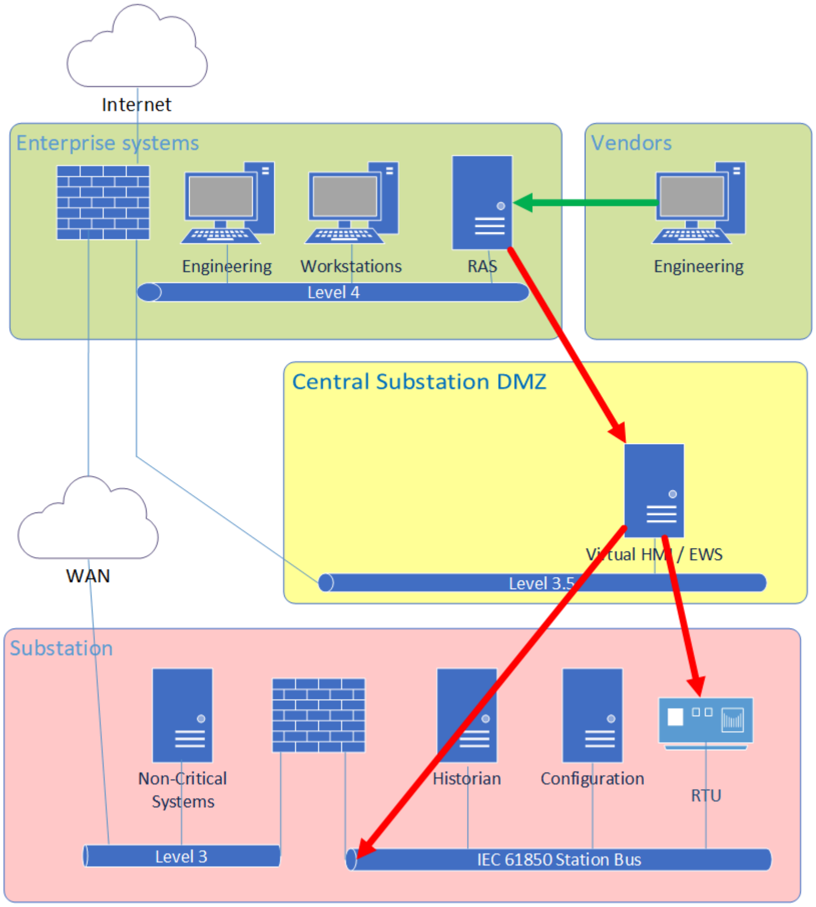

Figure 4-6 RAS with virtual HMI/EWS

Access rights for the remote access system should be regularly audited. User accounts shall have a defined limited lifetime (such as six months). This will disable unused accounts and the obsolete accounts of former employees. Existing active accounts may be authorized for another six months. It is also possible to limit access from the internet based on the geo-location (e.g. countries), which will roughly restrict/stop some connection attempts from unauthorized locations.

Penetration testing of the remote access security should be performed regularly.

System logs should be exported to an external log server (e.g. security information and event management (SIEM) system). Logging shall be configured on clients, the VPN gateway, firewalls, the jump-host/RAS, authorization system (e.g. active directory (AD)) and end-systems. The centralized logging or SIEM shall perform log correlation, analytics and alerting, and preferably have some behavioural based alerts and custom alerts.

For more information, see NIST SP 800-46, CPNI /11/ and NIST SP 800-114.

4.5 Malware control

All critical systems vulnerable to malware attacks should have antivirus software, whitelisting (allow only authorized software to execute) and signature verification (allow only signed software to execute). In addition, all transfers of files and data into the substations should be scanned for malware. Software upgrades should be signed from the vendors. Firewalls should block worms and IDS should detect abnormal data traffic.

The antivirus solution should detect malware based on signatures and on heuristic and behavioural analysis and utilize sandboxing and data mining techniques. Antivirus signature files shall be regularly updated, with signature-based solutions requiring the most frequent updates.

This ideal protection regime is challenging to implement and manage. Many outdated systems do not support anti-malware options, or the reliability and real-time response cannot always be guaranteed if running such solutions. Therefore, compensating measures shall be implemented elsewhere in the complete view of people, process and technology. Cyber security measures and requirements should be included in requests for proposals (RFP) and incorporated into binding contracts with vendors.

As a minimum, a file transfer solution with effective malware scanning should be implemented, and if removable storage devices and portable computers are allowed, a malware scanning solution ('sheep-dip-station') should be in place. Such solutions shall have updated signature files, and logging, labelling and alarming in place. Auditing and regular testing with e.g. the Eicar /12/ test malware should be performed. Only dedicated and properly labelled removable storage devices should be allowed in the substation domain.

Malware control should be implemented in all systems outside the substation environment which may provide a direct or indirect route to an identified attack surface (see Sec.3) and in non-critical systems inside the substation.

For more information, see NIST SP 800-83, SANS /14/ and NIST SP 800-167.

4.6 Hardening

Ideally all systems vulnerable to cyber security incidents should be hardened. Such hardening may for end-systems include:

- blocking unused ports and protocols
- removing unused applications and services
- disabling interfaces for portable media (depending on the removable media policy)
- disabling not required wireless interfaces (depending on the wireless policy)
- blocking/protection of physical and logical access to diagnostics and configuration ports
- disabling default accounts (including 'guest accounts')
- restricting or denying access to shared folders
- changing default passwords
- setting password restrictions, idle timeout, etc.
- disabling temporary vendor access established during commissioning.

While newer systems may have implemented 'secure by default', older systems require hardening. Some systems have documents or profiles to enable a hardened state.

The hardening of critical substation systems may not be possible due to conflicts with the applications and the risk of making changes to a running system. As a minimum, the systems involved in external communication (RAS, routers, firewalls, etc.) shall be hardened. The hardening of such network devices includes:

- physical security (e.g. locked cabinets)
- disabling/blocking unused ports
- disabling wireless interfaces that are not operationally necessary (Wi-Fi, 4G, etc.)
- changing default administrative passwords
- management only from a dedicated port or separate network
- disabling default configurations like default VLAN
- disabling temporary vendor access established during commissioning.

Implementing media access control (MAC) address security (MAC lock, limit MAC addresses per port, static MAC, etc.) may be considered. The administrative burden shall be aligned with the risk. MAC address spoofing limits the effect of such measures.

For more information, see NIST SP 800-123 and Windows Server Security Guide /17/.

4.7 Patching

Ideally all systems vulnerable to cyber security incidents should be regularly patched. Patching involves installing security fixes and updates from the software and operational system vendors as soon as possible after release.

The patching of industrial systems is considered complex and time consuming. Patching may imply unacceptable down-time. The patch shall be approved by the system vendor to make sure it does not affect functionality and availability. Approved patches may be downloaded from the vendors (subject to integrity verification), or the vendors may supply lists of approved patches. Industrial patching is often first performed on test systems and then stepwise on redundant systems.

For hundreds of substations with extreme availability requirements, the cost and operational risk involved in patching may be higher than the cyber risk. For un-patched systems, other compensating measures as described in this guideline shall be considered.

As a minimum, the systems involved in external communication (RAS, routers, firewalls, etc.) shall be regularly patched. Systems outside the substation with an identified attack surface (see Sec.3) shall be regularly patched. The current status on patching should be available in the inventory system (see [4.9]).

The system to bring patches into the substation domain shall be secured. Patches should first be replicated to a server in DMZ and then replicated to the substation network. Patches shall be verified for authenticity and integrity.

For more information, see ISA/IEC 62443-2-3 (draft) and NIST SP 800-40.

4.8 Production data export

In other industries, the need for production data to be exported to external systems for analytics, optimization, accounting and maintenance is essential. For substations there is currently little need for this export of production data because metering in power grids is separated from automation and protection. For condition-based maintenance, non-critical sensors are installed, but these devices are normally not connected to the substation networks. The need for production data export is expected to increase, so solutions shall be implemented. To achieve 'incipient fault detection' (faults that slowly develop in time, leading ultimately to process failure or an emergency situation), more sensor-data, and substation data collection are required. In practice, data may be exported by an information management system (IMS). A secure IMS as shown in Figure 4-7 involves a collector node at level 3, one-way replication to a shadow node in DMZ and again one-way replication to a shadow node at level 4.

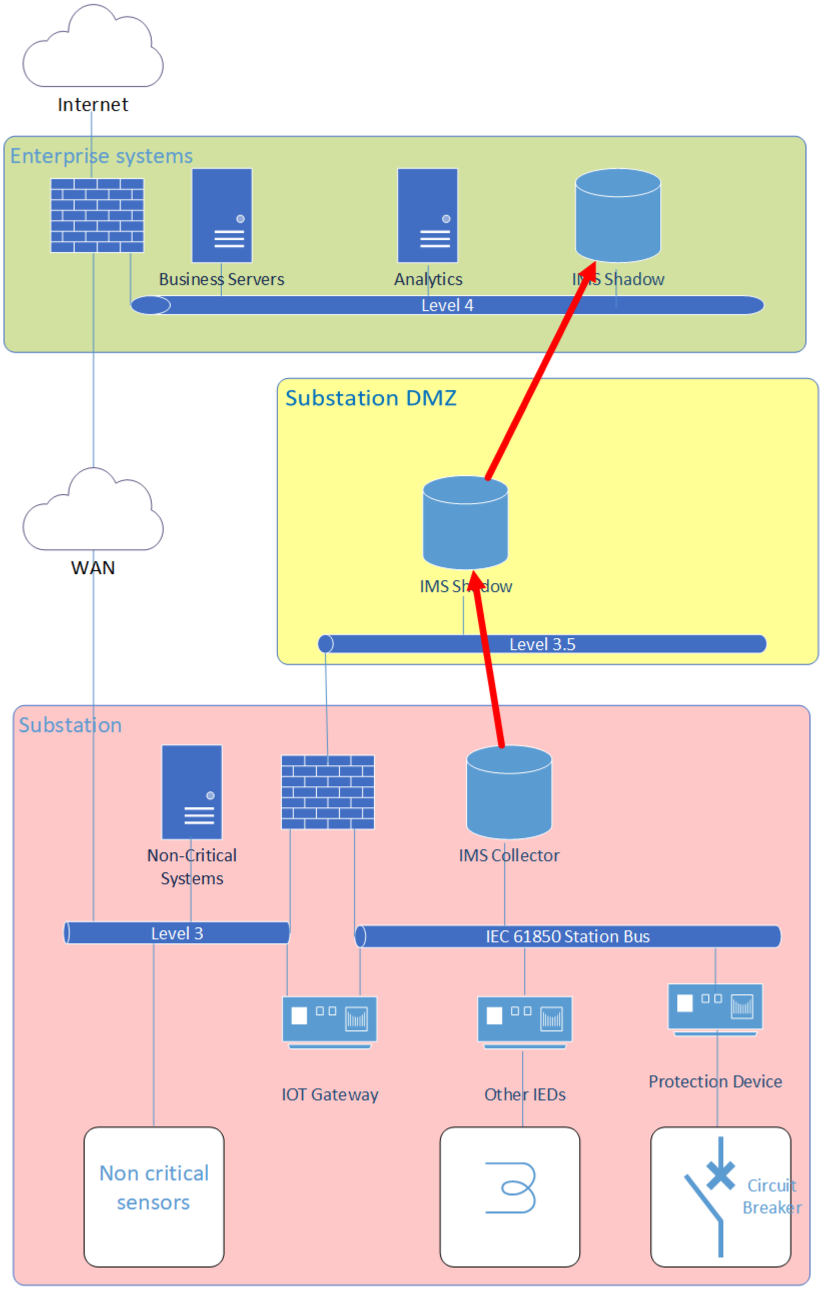

Figure 4-7 Data export

For more information, see Good Practices for Security of the Internet of Things /26/.

4.9 Inventory management

One of the first steps in frameworks like the NIST CSF is to 'identify', and this requires the maintenance of an inventory of hardware and software. To maintain such an inventory for the high number of substations with many generations of systems is challenging. In traditional IT systems, automatic or semi-automatic methods have been used where the server polls agents in the systems to collect inventory information.

In industrial systems there has been scepticism about installing such active scanning and allowing data traffic for polling. Some systems are based on a 'passive scanning' concept where a unit sniffs network traffic and analyses the traffic stream to create an inventory. Other systems are use a 'selective probing' concept where selected nodes are probed at e.g. 24-hours intervals to limit probing traffic.

The inventory system should maintain information on all devices, hardware components, software components and communications protocols/ports, including:

- organizational responsibilities
- manufacturer
- vendor
- model
- version numbers
- serial numbers
- revision/patch levels
- network addresses
- history.

The asset inventory should be linked to security bulletins, release notes and other input from vendors to enable risk assessments with regard to detected issues and patch-management.

For more information, see NIST SP 800-128.

4.10 Incident response and recovery

4.10.1 General

It is essential for organizations responsible for substations to have a structured and planned approach to incident response and recovery. ISO 27035 recommends the establishment of policies, plans, procedures and systems to:

- detect, report and assess information security incidents
- respond to information security incidents, including the activation of appropriate controls to prevent, reduce, and recover from impacts
- report information security vulnerabilities so they can be assessed and dealt with appropriately
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

Best practice to plan for incident response and recovery is in summary:

- Create a policy including:
  - the purpose, objectives and scope
  - the policy owner and review cycle
  - a definition of what a security incident is
  - a description of the type of security incidents or categories
  - a description of how incidents should be reported
  - a high-level overview or visualization of the incident management process flow
  - a defined set of roles, responsibilities, and decision-making authority.

- Create a plan describing detailed activities, procedures and information. As a minimum, this should include:
    - planning and preparation:
        - event categorization
        - escalation procedures
        - logging of incident handling
        - testing plan procedures
        - important contact information
    - detection and reporting:
        - the collection of information related to the event
    - response:
        - procedures to reduce the consequences of the event, see [4.10.2] - [4.10.3]
        - procedures to recover from the event, see [4.10.4]
        - procedures for forensics
    - lessons learned:
        - reviewing and improving the information security countermeasures, and the incident response policy and plan
- Create an incident response team, including establishing a relationship with other organizations (CERTs, regulatory authorities, police, etc.).
- Create incident training and awareness.
- Exercise according to the plan and monitor the response capability.

To comply with the EU NIS Directive on critical infrastructure, incident response according to ISO 27035 is required in addition to an ISO/IEC 27001 compliant CSMS, see [4.1].

For more information, see ISO 27035, NERC CIP-008, NIST SP 800-61 and CYPRES /20/.

For substations, some specific topics should be included in the incident response and recovery plan, see [4.10.1] to [4.10.3].

4.10.2 Isolation of substations

When cyber security incidents that may negatively impact the substations are detected, procedures and technical measures should be in place to run substations in 'silent mode'. This involves reducing network traffic to a minimum to ensure the substation can operate. If a local crew has to be on site to perform switching operations, this shall be done from a safe location in the substation taking into account the regulatory aspects of working in/under/near to high voltage installations.

4.10.3 Manual switching of breakers

Procedures should be in place to guide the decision to manually shut down parts of the grid in the case of a serious cyber security incident. The procedure shall define what is a 'safe state' related to incident categories and how breakers can be manually tripped when protection systems are unavailable.

4.10.4 Backup - restore

Recent ransomware infections like Petya and NotPetya have introduced new backup/restore requirements:

Secure backup storage:

The online storage of backups may also be influenced by the ransomware and may be worthless. The only safe option is to store the backup on offline media like removable USB memory or 'write once read many' (WORM) media like a CD/DVD. Storing backup on hidden partitions may help, but this methodology is not a complete guarantee against attacks. There is always the risk that an attacker could find a way to mount the partition and then install ransomware.

Storage of backup in another security zone and the use of separate accounts to access the backup data will reduce the risk of disrupted backup media.

Procedures and regular training for total restoration:

Ransomware infections may lead to 'black screens' and require a total restoration from clean systems. Recovery involves the restoration of operation systems, applications, configuration/settings and data. For virtual systems the underlying virtualization software shall first be restored. Procedures shall be available and regular training shall be conducted on training systems for substation automation.

For more information, see restoration and recovery plans /19/.

4.11 Intrusion detection system

Intrusion detection systems (IDS) have been used in IT systems for decades, but have limited usage in industrial systems. There has been a reluctance to install devices that could influence data traffic, and these devices shall also be updated and monitored. This requires communication in and out of the OT domain. With segregated networks, several IDS may be necessary.

It is of vital importance to be able to detect incidents in the OT networks. If anti-malware and log monitoring are missing then IDS may be the more appropriate option for existing architecture. IEC 62443-2-1 requires that the asset owner shall ensure that the organization periodically uses manual or automated processes to discover and address:

a) undocumented and unauthorized devices/software connected to or communicating within the IACS
b) undocumented and/or unauthorized network traffic
c) undocumented vulnerabilities in the IACS
d) other security anomalies and non-conformities.

An IDS may be used to meet the malware detection or defence requirements of the NERC CIP V5 standard.

IDS may detect incidents based on signature detection or anomaly detection (deviations to 'normal' traffic). They may be passive or active. Active IDS (also called intrusion prevention systems) drop/block illegal traffic and should not be used in industrial environments. IDS may be standalone devices or modules (software/blades) in, for example, firewalls or routers.

An option is to record data traffic at regular intervals on a network 'Tap' and conduct offline analytics.

An IDS is only useful if it is properly configured and monitored. Otherwise it is just a useless extra device in an OT environment sending a high number of false alarms. IDS configuration shall be coordinated with the zone and conduits and firewall setup.

For more information, see NIST SP 800-94.

4.12 User authentication and authorization

Only identified and authenticated users, nodes and applications should be permitted access to systems capable of controlling protection devices.

Local access inside the substation is typically based on static, shared accounts with high privileges. Default passwords may be in use. These passwords shall be changed regularly since operators and service personnel may have left the company.

To administer and monitor local accounts on a high number of systems in a high number of substations can be challenging. The goal should be to implement a common user repository and define roles based on the least required access privileges.

HR systems and processes shall be aligned with the OT domain. Rights allocated to employees who change jobs/leave the company shall be evaluated and removed or changed. The same applies to the onboarding of new employees, the right access shall be granted. Centralized RBAC shall be interfaced with all OT components and based upon open standards such as the 62351-8, or LDAP/RADIUS.

Remote access shall require multifactor authentication. NIST does not recommend the use of SMS based codes.

Remote access for 'read only access' should be used with care due to the risk of privilege escalation.

Access should be given based on needs and only with the minimum privilege necessary to perform the assigned tasks. Performing tasks with full administrative rights should be restricted. Privileges shall be granted and administered based on roles (RBAC).

Software services shall not be granted interactive login capabilities.

Regular audits should be performed to verify that access rights are kept updated.

For more information, see NIST SP 800-63 and NIST SP 800-162IEC 62351-8 RBAC.

4.13 Logging and alarming

Logging and alarming are essential to detect cyber incidents. The availability of logs is an important component when conducting post incident digital forensics.

To establish a logging and alarming regime, security logging shall be enabled in end-systems, the log entries shall be collected for analysis and correlation, and alarms and reports shall be generated. Log entries shall be protected from modification and deletion for example by the use of a protected syslog server. Correlation of events is made possible by log events being time stamped. The use of an accurate and reliable time source is required typically by the use of the network time protocol (NTP) or GPS clocks.

In industrial systems, security logging in end-systems are often disabled due to the possibility of introducing latency. The design requirement to establish log analysis, correlation and alarming in complex industrial systems can be resource intensive but achievable.

As a minimum a logging and alarming system should be established for the systems involved in external communication (RAS, routers, firewalls, etc.).

An IDS (see [4.11]) may be a compensating control for the lack of security logging at end-nodes.

For more information, see Creating a Logging Infrastructure /18/.

4.14 Implementation of protective measures

The protective measures proposed in this section have differing requirements in terms of implementation costs, time and complexity. Some implementations may influence the stability of the substation systems and therefore require downtime. To assist in prioritizing the measures, tables are provided with a high-level indication of the cost, time and complexity. These indicators should be tailored to the needs of the organization, and the risk reduction effects shall be considered.

Table 4-3 provides a list of low-cost security measures that should be implemented. These involve little time/complexity and no expected substation downtime. These measures are considered to be 'low hanging fruit' and may serve as a checklist or a starting point for company specialists to start improving their environment.

Table 4-4 gives a list of more costly and time-consuming security measures that should be implemented over time (e.g. from one to five years).

Table 4-5 gives a list of security measures that will require significant changes to the substation systems and will most probably require downtime. Such measures should be planned and implemented for new systems and for major substation upgrades.

Table 4-3 Implementation of 'low hanging fruit' measures

No.	***Title***	***Subsection***	***Subst. downtime***	***Cost***	***Time / compl.***
1.	Certify the competence of cyber security personnel	[4.1]	No	Low	Low

No.	Title	Subsection	Subst. downtime	Cost	Time / compl.
2.	Regularly train the cyber security awareness of personnel	[4.1]	No	Low	Low
3.	Regularly assess the maturity level of CSMS	[4.1]	No	Low	Low
4.	Define cyber security responsibilities for the substation lifecycle	[4.2]	No	Low	Low
5.	Assign a security level target to zones & conduits	[4.3]	No	Low	Low
6.	Regularly audit (e.g. yearly) firewall rules	[4.3]	No	Low	Low
7.	Regularly penetration test (e.g. yearly) firewalls	[4.3]	No	Low	Low
8.	Implement 'management of change' on firewall rules	[4.3]	No	Low	Low
9.	Regularly audit (e.g. yearly) remote access users and rights	[4.4]	No	Low	Low
10.	Regularly penetration test (e.g yearly) the remote access system	[4.4]	No	Low	Low
11.	Implement 'management of change' on remote access users and rights	[4.4]	No	Low	Low
12.	Regularly test malware detection, alarming and response	[4.5]	No	Low	Low
13.	Establish a system/routines for MAC address inventory (detecting new devices)	[4.9], [4.11]	No	Low	Low
14.	Establish an incident response team	[4.10]	No	Low	Low
15.	Establish incident response and recovery training and awareness	[4.10]	No	Low	Low
16.	Regularly copy on-line backups to an off-line media	[4.10]	No	Low	Low
17.	Implement multifactor authentication for all remote access to substations	[4.12]	No	Low	Low
18.	Regularly audit the local password quality and that passwords are known to a required minimum. Audit admin password use.	[4.12]	No	Low	Low
19.	Establish a regime for firewall log monitoring	[4.13]	No	Low	Low
20.	Do regular spot checking of security log files	[4.13]	No	Low	Low

Table 4-4 Implementation of more time consuming and complex security measures

No.	Title	Subsection	Subst. downtime	Cost	Time / compl.
21.	Implement a CSMS in the organization	[4.1]	No	High	High
22.	Verify cyber security after commissioning	[4.2]	No	Medium	Medium
23.	Secure external IEC 101/104 protocols in VPN tunnels	[4.3]	N/A	Medium	Medium

No.	Title	Subsection	Subst. downtime	Cost	Time / compl.
24.	Establish a common secure remote access system	[4.4]	No	Medium	Medium
25.	Install malware protection software in all systems communicating with substation systems	[4.5]	No	Medium	Medium
26.	Implement a malware protection system and routines for removable storage devices ('sheep-dip-station')	[4.5]	No	Medium	Medium
27.	Implement a file transfer solution in the substation domain including malware protection (may be part of remote access system Ref 24)	[4.5]	No	Medium	Medium
28.	Harden all systems communicating with substation systems	[4.6]	No	Medium	Medium
29.	Regularly patch all systems communicating with substation systems	[4.7]	No	Medium	Medium
30.	Establish a separate infrastructure ('silo') for non-critical sensors and IOT devices	[4.8]	No	Medium	Medium
31.	Establish IMS to export production data for analytics	[4.8]	No	Medium	Medium
32.	Establish an automatic or semi-automatic inventory system	[4.9]	No	High	High
33.	Establish incident response and recovery policy, plan and procedures (part of 21. CSMS)	[4.10]	No	Medium	Medium
34.	Establish IDS on substation DMZ	[4.11]	No	Medium	Medium
35.	Establish a remote access solution with 'true read only' (may be part of remote access system Ref 24)	[4.12]	No	Medium	Medium
36.	Enable security logging on systems communicating with substation systems	[4.13]	No	Medium	Medium
37.	Implement a SIEM for substation systems	[4.13]	No	High	High

Table 4-5 Implementation security measures for new substations or major upgrades

No.	Title	Subsection	Subst. downtime	Cost	Time / compl.
38.	Renew substation zone model	[4.3]	Yes	High	High
39.	Enable substations to run in 'island mode'	[4.3]	N/A	Medium	Medium
40.	Install malware protection software on all relevant substation systems	[4.5]	Yes	High	High
41.	Harden all relevant substation systems	[4.6]	Yes	High	High
42.	Regularly patch all relevant substation systems (consider relevance)	[4.7]	Yes	High	High
43.	Establish IDS on all substation networks	[4.11]	No	High	High

No.	***Title***	***Subsection***	***Subst. downtime***	***Cost***	***Time / compl.***
44.	Establish a common user repository (e.g. active directory) for substation access based on roles or attributes (RBAC/ABAC)	[4.12]	No	High	High
45.	Enable security logging on all relevant substation systems	[4.13]	N/A	Medium	Medium

SECTION 5 SECURITY FOR FUTURE SUBSTATIONS

5.1 Digital substations 4.0

The term 'digital substation 4.0' refers to the fourth industrial revolution of substations. The goal is to reduce copper wiring, decrease environmental impact, lower installation costs, reduce engineering times and increase personnel safety. Existing ethernet networks based on IT redundancy protocols cannot be used to handle such time critical real-time data with high availability. The IEC 61850-9-2 process bus has been developed to handle all sample value (SV) and generic object oriented substation event (GOOSE) traffic between the IEDs merging units (MU) and optical instrument transformers.

A common misunderstanding is that a multivendor digital substation 4.0 is not mature enough for production environments as there are still some challenges related to GOOSE interoperability, and correct network design. Edition 2 of IEC 61850-9-2 has solved some of these issues, and IEC 61850 9-2 LE was developed to give guidelines on interoperability.

In order to standardize the implementation of an SV-publisher, the Utility Communication Architecture Internal User Group (UCAIug) has developed a guideline for manufacturers. This guideline (not an IEC 61850 standard) attempts to remediate uncertainties regarding interoperability issues. This guideline only covers the publishing of SV streams, not how to subscribe to them.

IEC 61850-90-4 was written to inform network engineering practices by including redundancy guidelines and IEC 61869-9 was approved to define requirements for digital interfaces for instrument transformers.

SECTION 6 BIBLIOGRAPHY

6.1 Bibliography

Table 6-1 lists other references used in this document.

Table 6-1 Bibliography

Reference no.	*Source*
/1/	Electrical 4 U. Protection Systems in Power System [Internet]. S.l.: Electrical 4 U; 2020. [last updated 2020 October 23; cited 2021 January 28]. Available from: https://www.electrical4u.com/protection-system-in-power-system/
/2/	DNV AS. DNV-RP-G108. Cyber security in the oil and gas industry based on IEC 62443. Høvik: DNV; 2017
/3/	Williams TJ. The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. Research Triangle Park, NC: ISA; 1992
/4/	SANS Industrial Control Systems Security; Electricity Information Sharing and Analysis Center. Analysis of the cyber attack on the Ukrainian power grid: defense use case. Traffic light protocol. White. [Internet]. Washington, DC: E-ISAC, 2016 March 18. [cited 2021 January 28]. Available from: http://ics.sans.org/duc5
/5/	Hauet JP, Bock P, Foley R, Francoise R. InTec: Ukrainian power grids cyberattack [Internet]. Research Triangle Park, NC: ISA; 2017. [cited 2021 January 29]. Available from: Special Section: Ukrainian power grids cyberattack - ISA
/6/	Cybersecurity of critical energy infrastructure [Internet]. Brussels: European Parliament Think Tank; 2019-10-25. [cited 2021 January 29]. Available from: Cybersecurity of critical energy infrastructure - Think Tank (europa.eu)
/7/	CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG). Smart grid set of standards. Version 4.1. [Internet]. Brussel: CEN-CENELEC-ETSI, 2017. SEGCG/M490/G. [cited 2021 January 29]. Available from: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CGSEG_Sec_0042.pdf
/8/	Power System Relaying Committee. Understanding microprocessor-based technology applied to relaying: report of Working Group I-01 of the Relaying Practices Subcommittee [Internet]. Piscataway, NJ: IEEE; 2009. January. [cited 2021 January 29]. Available from: Reports - IEEE PSRC (pes-psrc.org)
/9/	ISF, 2017. The ISF Threat Event Catalogue
/10/	NIST. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 [Internet]. Gaithersburg, MD: NIST; 2018 April. [Cited 2021 January 29]. Available from: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 | NIST
/11/	U.S. Department of Homeland Security; [U.K.] Centre for the Protection of National Infrastructure. Configuring and Managing Remote Access for Industrial Control Systems [Internet]. S.l: CPNI; 2010 November. [cited 2021 January 29]. Available from: https://us-cert.cisa.gov/ics/Abstract-Configuring-and-Managing-Remote-Access-Industrial-Control-Systems

Reference no.	*Source*
/12/	European Expert Group for IT-Security [Internet]. Thaining, BA. Germany: IECAR; [2021]. [cited 2021 January 29]. Available from: http://www.eicar.org
/13/	Paulk MC, Curtis B, Chrissis MB, Weber C. Capability Maturity Model for Software (Version 1.1) Pittsburgh, PE: Carnegie Mellon University, Software Engineering Institute; 1993 February. [Cited 2021 January 29]. Report number CMU/SEI-93-TR-024 . Available from: Capability Maturity Model for Software (Version 1.1) (cmu.edu)
/14/	Martin J. A Practical Guide to Enterprise Antivirus and Malware Prevention [Internet]. North Bethesda, MD.: SANS Institute; 2001. [Cited 2021 January 29]. Available from: https://www.sans.org/reading-room/whitepapers/malicious/paper/68
/15/	MITRE ATT&CK. ATT&CK® for Industrial Control Systems [Internet]. S.l.: MITRE Corporation; 2020. [last edited 2020 June 03; cited 2021 January 22]. Available from: https://collaborate.mitre.org/attackics/index.php/Main_Page
/16/	CIGRE. Cyber attack modelling and security graded approach: key elements when designing security architecture for electric power utilities (EPUs) [Internet]. Paris: CIGRE; 2012. [Cited 2021 January 29]. Ref. no. D2-107_2012. Available from: e-cigre > Publication > Cyber attack modelling and security graded approach: key elements when designing security architecture for electric power utilities (EPUs) (e-cigre.org)
/17/	Microsoft Corporation. Windows Server Security Guide. [Internet]. Redmond, WA: Microsoft Corporation; August 2017. [Cited 2021 January 29]. Available from: https://download.microsoft.com/download/5/8/5/585DF9E9-D3D6-410A-8B51-81C7FC9A727C/Windows_Server_2016_Security_Guide_EN_US.pdf
/18/	Todd B. Creating a Logging Infrastructure [Internet]. North Bethesda, MD: SANS Institute; 2017. [Cited 2021 January 29]. Available from: https://www.sans.org/reading-room/whitepapers/logging/creating-logging-infrastructure-38130
/19/	Federal Energy Regulatory Commission [FERC]; North American Electric Reliability Corporation [NERC]. Report on the FERC-NERC-Regional Entity joint review of restoration and recovery plans: Further joint study report, planning restoration absent SCADA or EMS (PRASE). S.l.: FERC, NERC; 2017 June. [Cited 2021 January 29]. Available from: 06-09-17-FERC-NERC-Report.pdf | Federal Energy Regulatory Commission
/20/	Federal Energy Regulatory Commission [FERC]; North American Electric Reliability Corporation [NERC]. Cyber planning for response and recovery study (CYPRES): 2020 FERC, NERC and Res report. [Internet]. S.l.: FERC, NERC; 2020 September. [Cited 2021 January 29]. Available from: https://cms.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf
/21/	NERC. United States mandatory standards subject to enforcement [Internet]. Atlanta, GA: NERC; 2021. [cited 2021 January 29]. Available from: United States Mandatory Standards Subject to Enforcement (nerc.com)
/22/	NIST. NIST SP 800-series [Internet]. Gaithersburg, MD: NIST; c2021. [cited 2021 January 29]. Available from: https://csrc.nist.gov/publications/sp800
/23/	EU Cybersecurity Act [Internet]; 2020 [cited 2021 March 03]. Available from: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

Reference no.	*Source*
/24/	Commission Recommendation on cybersecurity in the energy sector [Internet]; 2019 [cited 2021 April 13]. Available from: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf
/25/	Directive on Security of Network and Information Systems (NIS) [Internet]; 2016 [cited 2021 April 13]. Available from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj
/26/	Good Practices for Security of Internet of Things in the context of Smart Manufacturing [Internet]; 2018 [cited 2021 April 13]. Available from: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
/27/	Communication network dependencies for ICS/SCADA Systems [Internet]; 2016 [cited 2021 June 11]. Available from: https://www.enisa.europa.eu/publications/ics-scada-dependencies

APPENDIX A ALTERNATIVE MODEL

A.1 An alternative Purdue model

The Purdue model was originally developed as a reference model for enterprise architecture in the 1990s. This model is very useful for illustrating the different levels of critical infrastructure used in industrial control systems and production lines as well as how to secure them. As a conceptual model for enterprise architecture and operations control systems, the Purdue model may be adapted to industry, technology, and choice of architecture (e.g centralized vs local). For grid operations, the adaption to the overall system architecture can be illustrated as below.

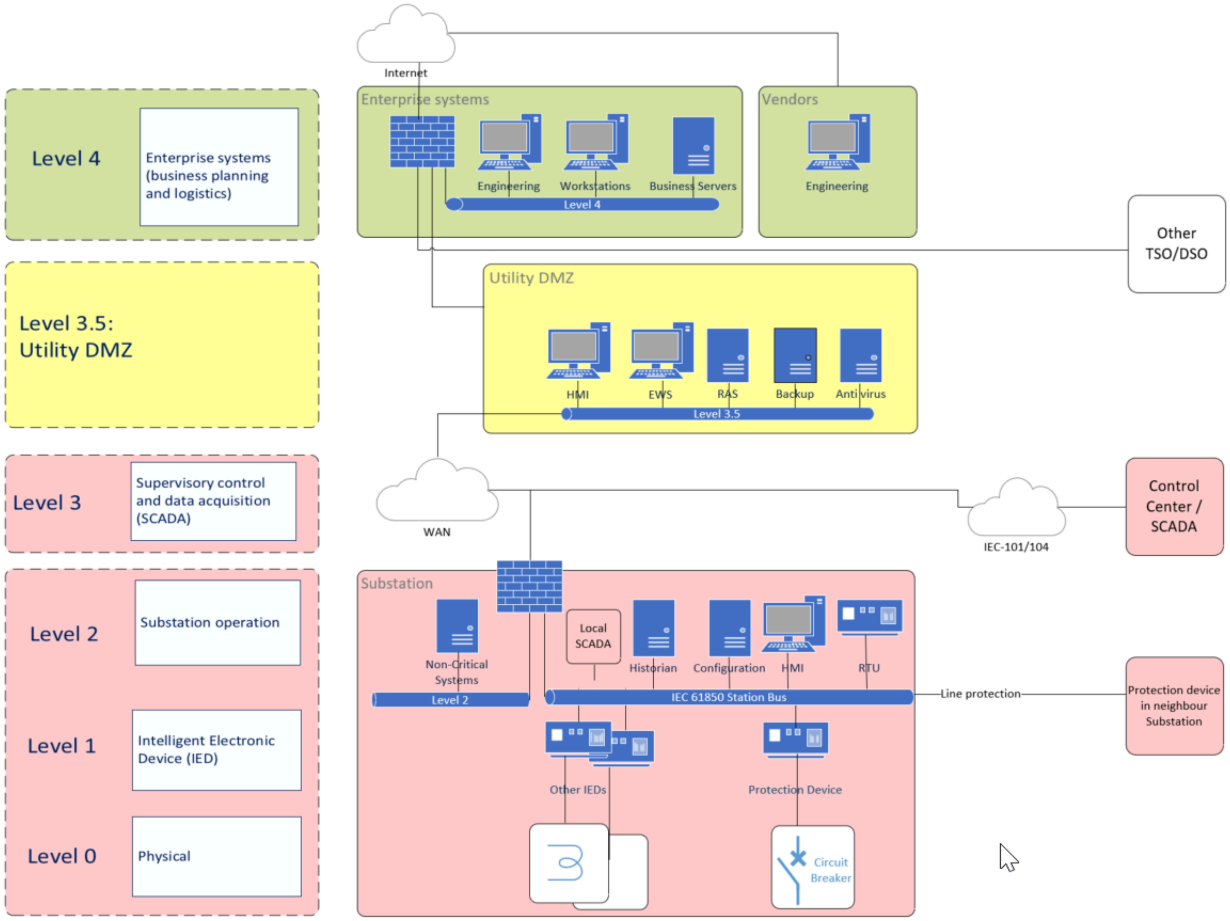

Figure A-1 Alternative Purdue model

APPENDIX B TABLE BASED ON SECTION 4

B.1 Attack surface, threats and mitigation

Table B-1 maps the attack surfaces from Figure 3-1, the attacks that could use such an attack surface to realize a threat, and the mitigations from Sec.4 that may counter the attack.

Table B-1 Attack surface, threats and mitigation based on Sec.4

No.	*Name*	*Threats*	*Mitigation in Sec.4*												
			[4.1]	[4.2]	[4.3]	[4.4]	[4.5]	[4.6]	[4.7]	[4.8]	[4.9]	[4.10]	[4.11]	[4.12]	[4.13]
1	Attack from internet	- Credential reuse	x	x	x	x	x					x	x	x	x
		- Default/weak credentials	x	x	x	x	x					x	x	x	x
		- Denial of service	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit weak network architecture, barriers and encryption	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Phishing	x	x			x								x
		- Malware	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Man-in-the-middle			x	x	x	x	x	x		x	x	x	x
		- Session hijacking			x	x	x	x	x	x		x	x	x	x
		- Unauthorized network scanning, probing and modification			x	x	x	x	x	x		x	x	x	x
2 3 4 14	Attack from internal networks	- Credential reuse	x	x	x	x	x					x	x	x	x
		- Default/weak credentials	x	x	x	x	x					x	x	x	x
		- Denial of service	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit weak network architecture, barriers and encryption	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Malware	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Man-in-the-middle			x	x	x	x	x	x		x	x	x	x
		- Session hijacking			x	x	x	x	x	x		x	x	x	x
		- Unauthorized network scanning, probing and modification			x	x	x	x	x	x		x	x	x	x
		- Unauthorized physical access	x	x	x										

No.	*Name*	*Threats*	*Mitigation in* Sec.4												
			[4.1]	[4.2]	[4.3]	[4.4]	[4.5]	[4.6]	[4.7]	[4.8]	[4.9]	[4.10]	[4.11]	[4.12]	[4.13]
5	Attack from inter-relay network	- Denial of service	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit weak network architecture, barriers and encryption	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Man-in-the-middle			x	x	x	x	x	x		x	x	x	x
		- Session hijacking			x	x	x	x	x	x		x	x	x	x
		- Unauthorized network scanning, probing and modification			x	x	x	x	x	x		x	x	x	x
		- Unauthorized physical access	x	x	x										
6 13	Attack through vendor/ partner maintenance services	- Compromise suppliers	x	x	x	x	x	x				x	x	x	x
		- Credential reuse	x	x	x	x	x					x	x	x	x
		- Default/weak credentials	x	x	x	x	x					x	x	x	x
		- Denial of service	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit weak network architecture, barriers and encryption	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit system vulnerabilities	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Insecure disposal	x	x											
		- Interpersonal manipulation	x												
		- Phishing	x	x			x								
		- Malware	x	x	x	x	x	x	x	x		x	x	x	x
		- Man-in-the-middle			x	x	x	x	x	x		x	x	x	x
		- Session hijacking	x	x							x	x			
		- Theft of hardware	x	x	x										
		- Unauthorized physical access			x	x	x	x	x	x		x	x	x	x
		- Unauthorized network scanning, probing and modification			x	x	x	x	x	x		x	x	x	x

No.	*Name*	*Threats*	*Mitigation in Sec.4*												
			[4.1]	[4.2]	[4.3]	[4.4]	[4.5]	[4.6]	[4.7]	[4.8]	[4.9]	[4.10]	[4.11]	[4.12]	[4.13]
7 8 9 10 11 12	Attack through internal systems	- Compromise suppliers	x	x	x	x	x	x				x	x	x	x
		- Credential reuse	x	x	x	x	x					x	x	x	x
		- Default/weak credentials	x	x	x	x	x					x	x	x	x
		- Denial of service	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit weak network architecture, barriers and encryption	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Exploit system vulnerabilities	x	x	x	x	x	x	x	x	x	x	x	x	x
		- Insecure disposal	x	x											
		- Interpersonal manipulations	x												
		- Phishing	x	x			x								
		- Malware	x	x	x	x	x	x	x	x		x	x	x	x
		- Man-in-the-middle			x	x	x	x	x	x		x	x	x	x
		- Session hijacking	x	x							x	x			
		- Theft of hardware	x	x	x										
		- Unauthorized physical access			x	x	x	x	x	x		x	x	x	x
		- Unauthorized network scanning, probing and modification			x	x	x	x	x	x		x	x	x	x

CHANGES – HISTORIC

There are currently no historical changes for this document.

About DNV
DNV is the independent expert in risk management and assurance, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry benchmarks, and inspires and invents solutions.

Whether assessing a new ship design, optimizing the performance of a wind farm, analyzing sensor data from a gas pipeline or certifying a food company's supply chain, DNV enables its customers and their stakeholders to make critical decisions with confidence.

Driven by its purpose, to safeguard life, property, and the environment, DNV helps tackle the challenges and global transformations facing its customers and the world today and is a trusted voice for many of the world's most successful and forward-thinking companies.

WHEN TRUST MATTERS