



Cyber Security in Container Terminals



PEMA PAPER
2025

```
(000103AA) -----  
RUS stdcall DverEntr  
signed nt v2; // eax@2  
LSA_UNICODE_STRING Destnat  
unsigned nt; // [sp+14h]  
CPPEH_RECORD ms_exc; // [s  
ms_exc.disabled = 0; .....  
dword_14624 = 12; .....  
dword_146
```



RMK 02

KVA
SIEMENS

MAERSK

Contents

1.	Introduction & Executive Summary	04
2.	Security Standards	05
3.	Security in IACS	07
4.	Asset Management	09
5.	Risk Management	12
6.	Business Continuity Management and DRP	16
7.	Network Security	19
8.	Access Control	25
9.	Data and Document Management	26
10.	Security Monitoring	27
11.	Cyber Security Across the Supply Chain	29
12.	Personal awareness	29
13.	Recommendations	30
	Appendix: Glossary	31
	About the Authors and PEMA	32

1. Introduction

Document Purpose

Industrial Control Systems (ICS) and Industrial Automation and Control Systems (IACS) have become increasingly attractive targets for cyberattacks, as successful attacks on such systems can have disastrous consequences in the real world. Unlike attacks on traditional Information Communications Technology (ICT) systems, attacks on ICS/IACS can disrupt essential services and even result in loss of life.

This document focuses on the port and terminal environment and provides guidelines on cybersecurity.

Executive Summary

In the majority of countries, the transportation sector and in this context specifically container terminals, are classified as critical infrastructure. Critical infrastructure (or critical national infrastructure (CNI)) is a term used by governments to describe assets that are essential for the functioning of a society and the economy.

The safe operation of container terminals and their automated systems is the goal of the owners/operators. This can only be achieved if the integrity of the automation system is guaranteed. Cyberattacks on Industrial automation and control systems (IACS) and industrial assets put container plant safety at risk, and the threat landscape is constantly evolving as attacks become more sophisticated. Recently, so-called ransomware attacks have targeted older operating systems, resulting in complete system failures across sectors such as transportation and healthcare. Effective protection is necessary against these risks.

Container Terminals are, by nature, challenging environments, not only with respect to personnel safety but also because of the critical and sensitive information they hold. Furthermore, high availability of systems and equipment is essential to ensure business continuity. Interruption to operations or theft of data has a major financial and reputational impact not only for the terminal itself, but also for national security in cases of Cyber espionage.

One of the key challenges in assessing and managing cybersecurity risks is ensuring the cyber integrity of components sourced from multiple and diverse suppliers. Therefore, the goal is not only the cybersecurity integrity of a terminal when operational, but also the identification and addressing of cybersecurity requirements from the initial design phase and during construction. (Security by Design).

Security requirements must be identified and implemented considering several factors:

- The high increase in the complexity of supply chains and the various threats, such as cyber-attacks (e.g. infiltrating third-party supply chains and embedding malware in critical systems), physical attacks, counterfeiting and theft.
- The growing sophistication of spyware is a major player in the political war.
- The Increase in digitalisation and automation, which is very beneficial from an operational perspective when implemented according to the standards and proper risk assessment.
- Social engineering and the importance of the security awareness of all employees.

This white paper describes cybersecurity procedures that, when implemented, will improve both the safety and security of your IACS.

2. Security Standards

The recent rise in cyber attacks has spurred lawmakers to legislate for cybersecurity by creating rules and regulations. The purpose of these requirements is to protect critical infrastructure, ensure uninterrupted services for its citizens, and maintain the country’s stability.

There are national, international, and industry-specific standards and regulations that govern the protection of critical infrastructure, such as the EU Cyber Resilience Act, the NIS2 directive, and the Machinery Regulation and Radio Directives. All of these standards have a profound effect on how terminals are designed, constructed, procured, and operated. This will also have repercussions for other geographical locations, with more regulations being introduced in the coming years.

For ports and container terminals, IEC 62443 is the most important cybersecurity standard for protecting their operations. The following chapter references, for the most part, address the requirements of IEC 62443.

2.1 International Standards

2.1.1 ISO/IEC 27001 and 27002

The systematic management of information security in accordance with ISO/IEC 27001:2013 provides effective protection for information and IT systems with respect to confidentiality, integrity, and availability. This protection standard supports business processes, the achievement of company goals, and the preservation of corporate values through the trouble-free provision and processing of information.

2.1.2 IEC 62443

The IEC 62443 standard provides detailed guidance on protecting industrial systems throughout the plant’s lifecycle. The implementation of these recommendations must be on a case-by-case basis following the completion of a cyber threat analysis.

Fig 1: IEC 62443 Industrial communication Networks – Network and System Security

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, Concepts & Models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	IACS Security Program Ratings	3-2	Security risk assessment and system design	4-2	Technical security requirements for IACS components
1-3	System security compliance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-case	2-4	Security Program requirements for IACS service providers				
		2-5	Implementation Guidance for IACS asset owners				

EC 62443-1 includes terminology, concepts, applications and models

IEC 62443-2 is addressed to plant owners; it describes the implementation of a security Management system, patch management, etc.

IEC 62443-3 describes security technologies for controllers and network components

IEC 62443-4 is addressed to manufacturers and describes, for example, how to secure the development process

This structure also highlights that cybersecurity is a comprehensive process and that compliance with security standards is required from the component development phase.

Processes

Functional Requirements

As the leading standard, IEC62443 is sometimes adapted or referenced in other industry sectors. It is an internationally recognised standard and considered the most comprehensive cybersecurity standard for industrial systems. It addresses owners, system integrators, and manufacturers of automation systems. Various parts of the standard address processes, technologies, and personnel roles. It stipulates that for protection to be effective, suitable measures must be defined and implemented based on a risk assessment. Equally important is the sustainability of the achieved cybersecurity level over the long term, through regular review of the efficacy of the measures employed.

2.2 National Standards

In Germany, for example, the IT Security Act for “increasing the security of information technology systems” came into effect in July 2015. It requires that owners of critical infrastructure (KRITIS) in Germany, implement specific cybersecurity measures.

The IT Security Act has required certain critical infrastructure providers, such as those involved in water supply and sewage disposal systems, to report cybersecurity-related incidents since November 2016. Full compliance with minimum cybersecurity standards became a requirement on May 2nd, 2018. Should the owner of critical infrastructure experience a reportable IT disruption, the BSI (German Federal Office for Information Security) may also require the manufacturer(s) of the affected IT products and systems to become involved. This includes, for example, the prompt elimination of identified vulnerabilities.

Other countries also have agencies that oversee the cybersecurity of their domestic industries. These include the Agence nationale de la sécurité des systèmes d’information (ANSSI) in France, the National Centre for Security in Critical Infrastructure (NCSC) in Great Britain and the Department of Homeland Security (DHS) in the United States.

2.3 Industry-Specific Standards

There is currently no industry-specific cybersecurity standard available for container terminals and material handling.

2.4 EU CRA Cyber Resilience Act

The Cyber Resilience Act (CRA) is a cybersecurity regulation for the EU proposed by the European Commission on the 15th of September 2022. It aims to improve cybersecurity and cyber resilience in the EU by introducing common cybersecurity standards for products with digital elements. The EU’s Cyber Resilience Act (CRA) was enacted on December 10th, 2024. However, the regulation will not be fully applicable until December 11th, 2027. There are transition periods for specific provisions, such as the vulnerability reporting requirement for manufacturers, which becomes effective from September 2026.

This regulation will be binding for all EU member states and will play an essential role in strengthening Europe’s digital sovereignty.

It is recommended that the industry monitor the ongoing legislation process associated with this CRA as it develops.

2.5 Machinery Regulation EU 2023/1230

The revision of the existing Machinery Directive 2006/42/EC (abbreviation ‘MD’) and its associated redrafting as Machinery Regulation (EU) 2023/1230 (abbreviation ‘MR’) is aimed at updating and modernising uniform European legislation on the safety of machinery to reflect technological developments in the interim. The intent is to achieve an even higher degree of harmonisation within the Member States, to continue ensuring a high level of health and safety protection, and, at the same time, to promote the free movement of goods in the internal market.

This new Machinery Regulation (EU) 2023/1230 replaces the previous Machinery Directive 2006/42/EC and applies from January 20th, 2027.

3. Security in IACS

Cybersecurity – An ongoing process in IACS (Industrial Automation and Control Systems).

Adequate protection against cyber attacks is not achieved with one-off implementation measures, but rather through an ongoing, continuous process.

Starting from an evaluation of risks for the automated processes and IT infrastructure (**Assessment**), measures should be implemented to minimise these risks (**Implementation**). These measures should be monitored (**Management**) and continuously reviewed and evaluated to determine if they need to be revised to address new or changing cyber risks.

In the following chapters, guidelines for technical compliance with industry standards and for securing operations in accordance with IEC 62443 are outlined.

The terminal owner/operator is ultimately responsible for IT and OT security at their facility. It is strongly recommended that the terminal owner/operator and their responsible IT representative develop and maintain a customised cybersecurity concept document tailored to their specific needs.

A customised cybersecurity concept for each terminal should reflect the topics mentioned in this document in a format relevant to the specific terminal facility.

The purpose of this document is to highlight the current cybersecurity situation in the Port and Terminal sector and to provide best-practice recommendations for IT managers on how to organise their environments and mitigate the risk of cyberattacks correctly.

3.1 Security Policy and Goals

Each terminal organisation should define general rules for an applied cybersecurity policy. Every employee should clearly understand the importance of security-aligned behaviour and the potential impact of cybersecurity attacks on the organisation in the case of misbehaviour.

The goals the organisation aims to achieve with its cybersecurity policy should be clearly defined and understood by each employee and by business partners working with the organisation.

The security policy should be documented and made available to each employee.

3.2 Resources, Roles and Responsibilities

This chapter describes the roles and responsibilities of terminal staff.

In terms of cybersecurity, the users having access to IT and OT systems in their trusted network have different roles and responsibilities:

- Simple application user
- Super user, supervisor, system manager
- Network manager

The specific roles, responsibilities and authorisations should be defined and documented. Each person in the organisation should be aware of his/her role and responsibility. **There should be regular updates for all the security roles and responsibilities to ensure clarity and accountability within the organisation.**

3.3 Role of the CISO: Chief Information Security Officer

A **Chief Information Security Officer (CISO)** is a senior-level executive in a port or terminal organisation responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

The CISO has overall responsibility for ensuring the confidentiality, integrity, and availability of an organisation's information assets, safeguarding against cyber threats, and maintaining a strong security posture.

The CISO is also responsible for operational technology (OT) implemented in his/her area. This includes, e.g., PC and PLC systems, firewalls, access points, and intelligent sensors and devices installed on cranes delivered by third-party suppliers. Typically, OT and IT networks should be separated into different network segments. (Please see also Chapter 8). The CISO directs staff to identify, develop, implement, and maintain processes across the organisation to reduce information technology (IT) and operational technology (OT) risks. The CISO responds to incidents, establishes appropriate standards and controls, manages security technologies, and directs the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance. (e.g., supervises the implementation to achieve ISO/IEC 27001 certification for an entity or a part of it).

The CISO is also responsible for protecting the company's proprietary information and assets, including client and consumer data.

As a primary function, the CISO will continuously monitor and evaluate the status of an organisation's IT security and will establish appropriate measures to address increasing threat scenarios.

He or she must act in accordance with the crisis management plan (CMP), the business continuity plan (BCP), and, in the case of damage, the disaster recovery plan (DRP). These plans should be well prepared and documented to mitigate cyber threats as effectively as possible.

Please refer to Chapter 6 for further information.

3.4 Documentation of the Security System

There is a significant amount of information contained in and associated with a facility's trusted network that must be treated as confidential and protected.

This information might include:

- Personnel usernames and passwords
- Administrator usernames and passwords
- B2B access information used by machines
- Other system account information
- System account information for partnering systems, e.g. FTP servers
- Software license keys
- Network configuration files, including switches and access points
- Configuration and startup files for servers
- Organisations' own E-mail accounts
- E-mail accounts from partners
- Etc.

This information should be permanently updated and stored in a safe location. The documentation of this security-related data should achieve the following:

- Well-organised storage and administration of sensitive access data
- Protection of sensitive data against unauthorised and external access
- Availability of access data for rapid recovery of systems and networks in case of damage.

The documented policy issued by the CISO describing the methodology for the administration and storage of sensitive access information should be kept confidential and available only to a limited number of persons.

4. Asset Management

In information security, computer security, and network security, an asset is any data, device, or other component in the environment that supports information-related activities.

Assets generally include hardware (e.g. servers and switches) and software (e.g. mission-critical applications and support systems) that contain confidential information. In our ever-evolving industry, which includes industry 4.0 standards, IoT, and automation, the group of assets will also include industrial computers (PLC's) and intelligent sensors operating in the trusted networks.

Assets should be protected from unauthorised access, use, disclosure, alteration, destruction, and/or theft, which can result in damage and loss to the organisation and its operations.

4.1 Asset Management and Inventory

IT assets include all software and hardware in the terminal's business environment, across the technical, operational, administrative, financial, and security areas.

This includes computerised industrial hardware, such as intelligent components in cranes and electrical systems, as well as energy measurement sensors and management software.

These components are potential cybersecurity threats and should be subject to inventory management. Such components should be registered in an inventory list with their main characteristics to include:

- Name of the component
- Purpose
- Date of installation
- Release version of software/firmware
- MAC address
- IP address(es)
- Installation environment (e.g. network segment)
- Etc.

https://en.wikipedia.org/wiki/Data_center_management

Regular inventory checks should be scheduled to verify the existence and health of all these components, where possible.

4.2 Automated Asset Inventory

In the continuously expanding IT-controlled and automated business sector, maintaining control of the assets in an internal trusted network is becoming increasingly difficult.

There are software products on the market that allow automated asset management in the local environment. Such software products typically include the following features:

- Automated detection of assets in the network
- Administration of asset properties, license numbers, etc.
- Frequent automatic scans to prove if assets are functioning correctly
- Status monitoring of assets with alarms on potential failure
- Status monitoring of asset vulnerabilities

It is recommended that automated asset inventory control software be implemented to ensure high-quality oversight of all IT assets across the network, requiring minimal input from the IT staff.

4.3 Automated Asset Monitoring

In the previous section, the importance of risk management and the different threat factors were addressed. To ensure that risks are assessed correctly and that systems are patched and vulnerabilities are addressed, it is crucial to maintain a continuous, comprehensive overview of all assets and to implement a secure configuration management plan. To achieve complete real-time control over the efficiency and well-being of all assets, it is recommended to use a tool or a combination of tools that support automated monitoring of the asset landscape.

Several asset management products on the market provide inventory (Chapter 4.2) and monitoring in the same environment. This combination of tools should be selected individually by the port or terminal and may include:

- Integration platforms, ESB - Enterprise Service Bus for interface control
- SCADA systems (System Control and Data Acquisition) to collect and show sensor data
- Business logic to detect and indicate any malfunctions
- Digital Twin systems for visualisation of systems and processes
- Data warehouses and archives with business intelligence and KPI reporting
- Software Component Analysis based on SBOMs (Software Bill of Materials)
- Etc.

These integration and monitoring platforms and products generally serve the purpose of technical supervision of assets and plants, but they can also be configured to perform cybersecurity functions in systems and networks.

4.4 Configuration Management

Configuration management is a common task in IT service management. There are standard procedures available (ITIL 4 framework - ISO 20000:2018) that describe the appropriate activities and certification levels in this area.

The general task of the responsible service manager is to identify and register configuration items (CI's) under his/her responsibility, including IT and OT in the case of industrial assets. These CI's, if they are to be of value, must be documented with the following data:

- Name of the CI
- Version of the CI
- Description and purpose
- Status of CI
- Owner/supplier
- Location of the item
- Installation date
- Date of last update
- SLA responsible
- Link to descriptions
- Link to master software

There should be service-level agreements with IT and OT suppliers that specify the levels for which each party is responsible for maintaining the documented CI's.

A properly managed and updated IT configuration portfolio will help mitigate Cybersecurity risks and avoid, for example, older firmware or other software products being forgotten, which, years later, become an open door for cyber attacks.

As in the case of asset management and monitoring, tools are available in the field of configuration management that help automate the configuration management function. It is recommended to implement such a tool in the organisation, especially considering the rapidly increasing number of CIs appearing with industrial digitalisation 4.0.

4.5 Secure Configuration Management

Secure Configuration Management begins with the secure configuration of the asset during initial construction. Once the system is operational in the production environment, it needs to be monitored to detect any changes to its configuration. The organisation must have a formal process for requesting, reviewing, and approving changes to the originally approved configuration, including procedures for re-establishing baseline configurations. In addition to all assets identified in the asset inventory, the ability to verify integrity, confirm originality, and identify any unauthorised changes must be available.

This requirement is essential when equipment needs to be shipped to different sites, as is the case with terminals.

There are many methods and tools for implementing and monitoring secure configurations in a project or organisation. These include manual configuration, configuration scanner tools, change detection tools, Restricted user access to implement changes, the Security Content Automation Protocol (SCAP), automated vulnerability management, measurement, and policy compliance evaluation of systems, all of which can be deployed in a project or organisation.

4.6 Handling of Media with Sensitive Data

According to the EU regulation GDPR (General Data Protection Regulation), the latest version 2018, sensitive data in a business environment may include:

- **Personal data:** identifiers such as names or identification numbers, physical, physiological, genetic, mental, economic, cultural, or social characteristics. It also includes location data from GPS or mobile phones.
- **Confidential data:** trade secrets, investigations, data protected by intellectual property rights, security, passwords, financial information, national safety, military information.
- **A combination of different datasets** that can be combined into sensitive or personal data.
- **Biological data:** endangered (plant or animal) species, where their survival is dependent on the protection of their location data (biodiversity community).
- **Personal and sensitive metadata.**

Sensitive data should be stored in a trustworthy repository as a top priority. A simple solution is to store such information on mobile media that is not connected to a network and kept in a secure place (e.g., fireproof data safe).

Media with sensitive data, which is not to be used again, should be destroyed in a way that unauthorised use and retrieval of data will not be possible.

5. Risk Management

Risk Management is the foundation of cybersecurity as it enables an organisation to identify, assess, and manage threats to its ICS and IACS environment. To manage risks effectively, an organisation should establish processes for inventory management, risk assessment, vulnerability and patch management, and security baselining.

It is recommended to integrate the SCRA (Supply Chain Risk Assessment) into an overall risk management strategy to identify and evaluate supply chain risks arising from the use of third-party technology products and services (figure 2). Ref NIST SP 800-161r1

5.1 TRA: Threat and Risk Analysis

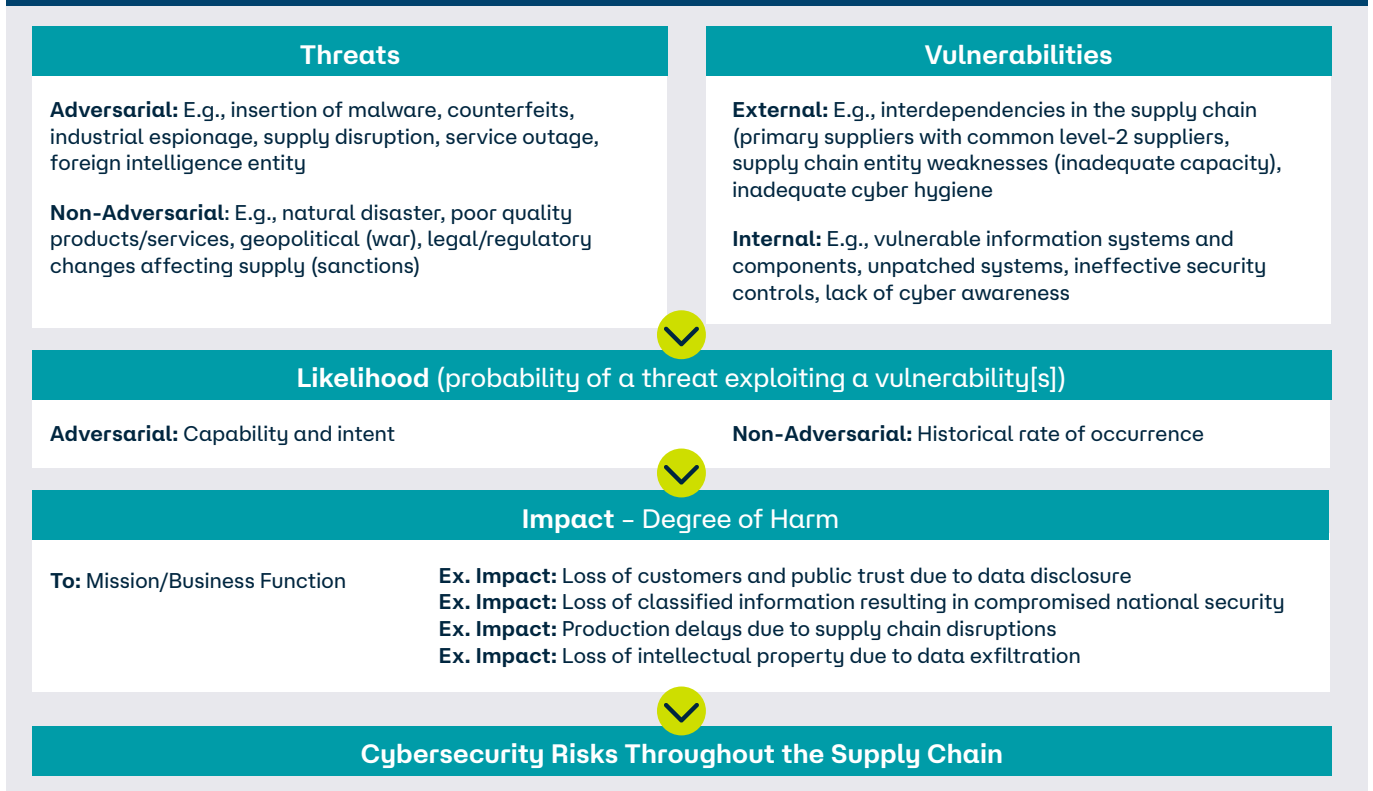
For risk assessment, a commonly used method is the Threat and Risk Assessment (TRA). This methodology should be applied regularly to address cybersecurity risks effectively.

Fig 3: CIA Triangle



With this method, a comprehensive risk assessment is carried out by first defining the effects and hazards that can arise from a cybersecurity attack. A distinction is made here between the impact of threats on the integrity, availability, and confidentiality of assets (terminals or solutions). This is known as the CIA triangle (figure 3). The effect is usually categorised as between disastrous and negligible. This can be considered a protection goal, where the most significant impact requires the highest level of protection.

Fig 2: Cybersecurity Risks Throughout the Supply Chain (Ref NIST SP 800-161r1)



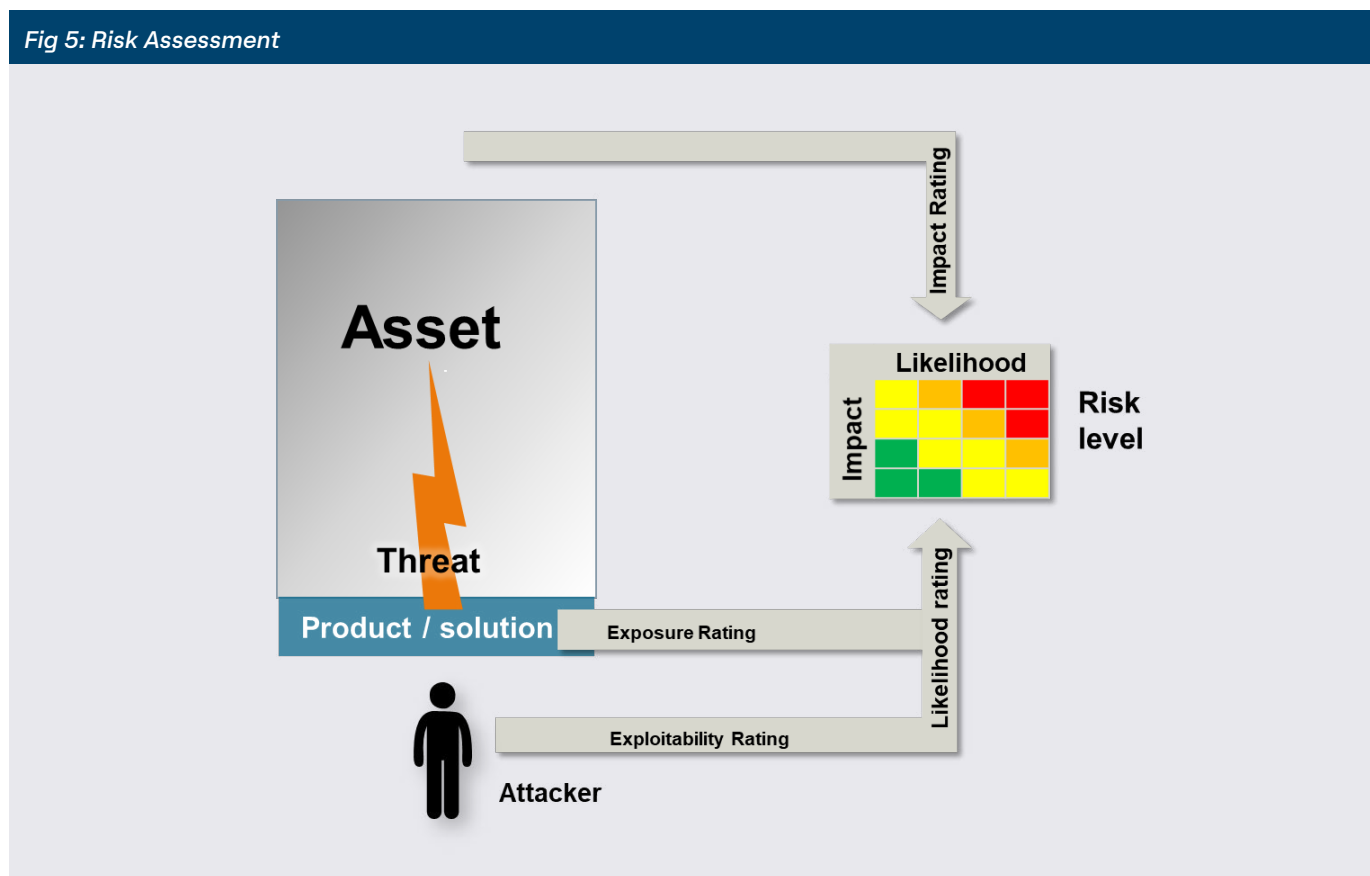
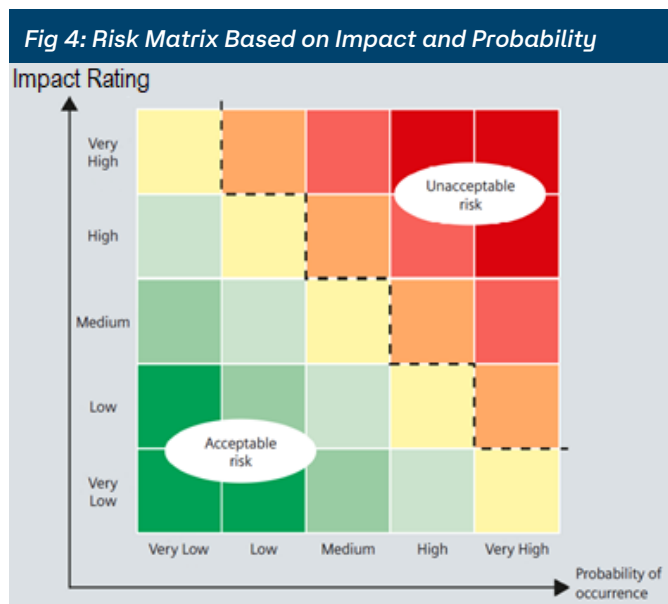
The second step assesses the risk of the probability of an attack. The probability rating can be split into two parts. The first part of the probability rating addresses the likelihood of an attack being attempted. What level of Access does the attacker need? This is known as the exposure rating. How easy would it be to access the assets?

The second part represents the probability that an attempted attack will succeed. This is known as the exploitability rating. How easy is it to perform the attack? What knowledge would be needed by the attacker? Would domain know-how be required?

Combining both steps gives a probability rating for an attack. The probability is usually categorised as High, Medium, or Low.

Combining the impact rating and the probability rating in the risk matrix will provide the risk level. If the risk is unacceptable, mitigation measures must be identified to reduce the risk to an acceptable level.

Mitigation measures should reduce the probability of occurrence, thereby lowering the risk.



5.2 Vulnerability Management

The likelihood of a successful attack is highly dependent on the existing vulnerabilities in the ICS or IACS assets. These vulnerabilities can be exploited by an attacker to infiltrate the company network.

From an infiltrated intranet or office network, the attacker can access the production network, either directly or through a follow-up attack.

The risk of attacks constantly evolves as new threats or vulnerabilities are identified at various stages of the lifecycle. Suppliers and integrators may identify new vulnerabilities by testing or reports issued by researchers or customers. Vulnerability management is the cyclical practice of planning assessments, scanning for vulnerabilities, identifying and remediating them, and finally highlighting potential risks to management.

Monitoring of this risk vulnerability management program is mandatory for ICS and IACS.

When establishing a vulnerability management program, the following should be included:

- Vulnerability assessment of ICS assets should be performed at regular intervals and:
- After a significant change to the ICS environment.
- After significant changes to the threats or risks faced by ICS, for example, a software vendor announces a critical vulnerability in a product used by the organisation.

One method for determining the severity of vulnerabilities is the Common Vulnerability Scoring System (CVSS). CVSS is used to assess the severity of vulnerabilities, to prioritise the vulnerabilities to be repaired and gauge the impact of the vulnerabilities on the systems.

One way to implement an automated vulnerability scan is to enable a tool that scans one or more targets for at least one vulnerability. Similar to anti-virus software, these scanners contain information on known vulnerabilities in operating systems and/or application software. This can be implemented as plug-ins. Each plug-in represents a known

vulnerability and can be selected by the user. As with a virus scanner, a vulnerability scanner can never be considered up to date because it must be continuously updated.

Given the limitations of individual programs, it is advisable to select a few high-quality security tools that deliver meaningful results.

There are various resources available to search for known vulnerabilities or exploits to be found on the internet, such as:

- **National Vulnerability Database (NVD):** The NVD is a public database operated by the National Institute of Standards and Technology (NIST) in the United States. It contains information about known vulnerabilities, including technical details, severity ratings, and possible countermeasures.
- **Exploit Databases:** Several exploit databases provide information about known attacks and vulnerabilities. Examples include Exploit-DB, Metasploit Framework, and Packet Storm Security.
- **Vendor Security Advisories:** Many software vendors release security advisories or bulletins to inform users about known vulnerabilities in their products and provide patches or updates. It is advisable to regularly check the websites of relevant vendors or subscribe to their security notifications.

5.3 Patch Management

The role of patch management in ICS Systems for critical infrastructures in transportation will be crucial in the future, especially the automation of patch management. The IACS owner needs to provide patch management services throughout the IACS's lifecycle. This service should include timely responses to new vulnerabilities and provide thoroughly tested patches from trustworthy sources.

Testing patches are often more complex and time-consuming in IACS systems. As IACS systems operate in real time and require high availability, patches must be thoroughly tested to ensure they do not negatively impact operations before rollout. In IT, patches can typically be tested more easily and quickly.

Patch management should be coordinated between the system supplier and the final owner/operator. It must be ensured that patches can be rolled out without risk to the system's functionality, and this is achieved through preliminary testing (i.e., Integration Testing).

In summary, patch management in ICS /IACS systems will play a central role in maintaining security and operational capability in the future. Organisations must allocate appropriate resources and establish processes for patch management to minimise the risk of cyberattacks and ensure the integrity of these critical systems.

5.4 Incident Handling

Any IT incidents that occur in the business IT environment should trigger an immediate alarm and be documented and analysed for potential immediate action by the responsible IT staff. All users should be able to report incidents quickly and easily to the responsible CISO. The process for reporting and managing incidents should be documented in a manual accessible to all users. In this manual, incidents should be categorised by threat level, along with instructions on how to respond should a specific category incident occur.

Measures to prevent further damage or to recover from damage events should be described in the DRP (Disaster Recovery Plan); see chapter 6.3. As a reference, the standard document available with more detailed information about incident management is the 'Incident Response Life Cycle' document issued by the NIST.

(National Institute of Standards and Technology, US Department of Commerce)

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

5.5 System Strengthening

System Strengthening Systems used in any business IT landscape should be maintained in an updated and supported condition to avoid vulnerabilities. Frequent vulnerability scans should be performed on all relevant systems to detect and identify unpatched, unsupported software or misconfigured IT systems. Unsupported end-of-life systems pose a risk and should be replaced with modern alternatives. Connections between systems, such as unused applications, should be detected and removed.

Updates and patches for critical IT systems should be implemented within a reasonable time frame, depending on the criticality of the risk. Before updates and patches are installed in the production environment, they should be installed and verified in a test environment.

A centralised configuration management system will help monitor the individual IT systems. Application whitelisting, when applied to servers and workstations, can help prevent the execution of unwanted applications.

5.5 Malware Protection

Malware protection software should be used whenever data (emails, documents, external links) is received via the Internet into the trusted network. This malware software should be installed on all communicating components, e.g. web proxies, servers, workstations and Laptops. Malware protection software should be installed with automatic signature updates.

5.6 Portable Media Control

Portable media (e.g., USB drives, portable disks) pose a high risk of malware transfer between systems. For this reason, unknown external media should never be connected to servers or workstations inside the trusted network without being tested for malware. Consideration should be given to disabling the USB port on sensitive systems to avoid the risk of importing malware via portable media.

6. Business Continuity Management & DRP

6.1 Business Continuity and Countermeasures

Whereas incident management is designed for single events of limited impact, crisis management and business continuity planning are intended to address significant, long-duration events. Such events have a greater impact and require a more complex, longer-lasting response. Based on the risk analysis outlined in Chapter 6, the responsible IT and operations managers should develop a business continuity plan (BCP) and a crisis management plan (CMP). These concepts will consider and describe different scenarios that could severely harm the facility's operations and/or the availability of IT infrastructure and systems.

A crisis management plan would typically address the following topics:

- **Crisis activation policy** – what will trigger the plan
- **Risk analysis** – What could happen
- **Response procedures** – Countermeasures to mitigate the risk
- **Emergency contact list** – Who is to be contacted
- **Communication strategy**

A business continuity plan would focus on measures that could bypass or replace systems or processes that are no longer available. For example, if a gate operation system is inoperative after a major traffic accident, processes should be activated to ensure the continuity of gate operations, utilising mobile applications or a paper-based system.

Cybersecurity insurance for terminals offers benefits such as regular audits by the provider and access to forensic experts within 24 hours of a cyberattack, aiding in continuity management and should be considered in the context of continuity management.

6.2 Processes for Backup and Restore

Cyberattacks frequently target sensitive data within trusted networks. Database encryption that leads to data loss is a well-known example of cybercrime.

One of the most essential countermeasures for such cases is the definition and execution of backup processes for all relevant systems. Backup processes or, in some cases, dynamic snapshots should be set up at reasonable intervals. The media containing backup data should be stored at a location that is not accessible from the Internet and with limited access from the rest of the infrastructure. Although it requires considerable effort from the IT organisation to test restoration processes, it is strongly recommended to test them frequently to be prepared for a real event.

6.3 Disaster Recovery Plan

Adequate preparation for events that could have a major impact on the functionality of the IT infrastructure and the operation of the entire facility is critical. The types of events that might occur at the facility should be analysed and assessed in a risk analysis process, considering the potential impact and the probability of each event. Cyber attacks might result in an event that could severely impact IT and the operation of the Port or Terminal. It is recommended that a specific disaster recovery plan for the facility be developed. This plan should include a CMP (Crisis Management Plan) and a BCP (Business Continuity Plan) containing the following topics:

- Definition of events that might affect IT & operations.
- Definition of measures to mitigate or prevent the impact of such event.
- Definition of EMCON (Emergency Condition) levels for the facility that describe the situation of the facility after an event has occurred or if the risk of a particular event occurring is increasing.
- Definition of measures for each EMCON level to compensate for the loss of certain functionality and to take measures to recover this functionality.

Example for Definition of EMCON (Emergency Conditions) Levels

EMCON 0 Normal Situation

This is a regular daily activity; no special increased risk has been detected. IT management ensures that the general rules for IT security are applied across the entire IT system, and network administration mitigates or prevents harm to system availability and data.

EMCON 1 Potential Threat

Threats are detected that could potentially affect the terminal IT network. As IT management has already implemented strict security rules for normal operations, no further action is required at this stage.

EMCON 2 Imminent Threat

This situation will appear before or after the declaration of a crisis. In this scenario, an increased risk to the availability of IT infrastructure, IT systems and/or terminal communication is detected due to local or country-wide political, economic or other tensions. Should the level of the crisis further increase, as in the case of an active war with possible bomb or terrorist attacks, then the potential impact might lead to physical damage to IT and other facilities. In this case, the alert level should be escalated to EMCON 3 with additional measures to be taken.

EMCON 3 Crisis Disrupting Some Terminal Functions

Should the crisis escalate to a situation comparable to an active war, physical assaults can be expected, potentially causing extensive damage to terminal facilities and assets, IT infrastructure, and systems operations. Moreover, long-term power outages and Internet connectivity issues may occur in this scenario.

EMCON 4 Crisis affecting most/all terminal functions

This scenario assumes that an outbreak of violence, due to war or a terrorist attack, has already occurred and caused damage to the terminal's IT infrastructure and/or core operational systems. Some or all systems are no longer available or limited in capacity. IT resources (IT infrastructure, servers, network, and IT staff) may not be available at full capacity. The terminal Operations and IT departments will focus on maintaining operations with limited resources and simplified processes in accordance with the business continuity plan.

EMCON 5 Crisis affecting all activities with at least temporary abandonment of the terminal

This scenario assumes that severe damage after an outbreak of violence has stopped the terminal operation completely or to a significant extent. Where IT infrastructure and system operations are concerned, the IT organisation's general focus will remain the same: to establish a provisional IT landscape, even if this proves difficult depending on the scale of damage to the terminal.

Example of general preparation and countermeasures to be taken by the IT organisation

In addition to the measures to be applied for the lower EMCON status, the following measures should be considered when EMCON levels rise:

- Ensure availability of IT experts, update the duty plan, and potentially cancel holidays.
 - Reconsider emergency plans, ensure support without external suppliers.
 - Be ready to implement emergency patches in systems if needed.
 - Check if interfaces can be closed which are not critical. Check if lateral movement through the firewalls can be reduced to a minimum.
 - Intensively monitor IT security logs, consider 24/7 monitoring.
 - Prepare and recheck offline backup procedures and data.
 - Make sure that backup recovery is properly tested.
- Investigation and assessment of damage to the IT infrastructure.
 - Develop and implement an intermediate solution to set up a workable IT infrastructure.
 - Organise transport and integration of precautionary purchased IT components.
 - Establish an electric power supply.
 - Set up a preliminary network, including WLAN.
 - Set up a provisional Internet connection, potentially with satellite telephones.
 - Reestablish servers, restore backups.
 - Set up limited operational processes, if needed, with manual data input.
 - Consider reinforcing IT and OPS staff with resources from other terminals if the security situation allows.

The following is an action plan that the IT organisation could consider as an example for the re-establishment of IT infrastructure and systems after damage occurred at **higher** EMCON levels:



7. Network Security

Network security is a central element of the industrial cybersecurity concept, including the protection of automation networks against unauthorised access and the monitoring of all interfaces to other networks (such as the office network and remote maintenance gateways to the internet). Protecting communications against interception and manipulation (encrypted data transmission and communication node authentication) also falls within the scope of network security.

7.1 Network Structure

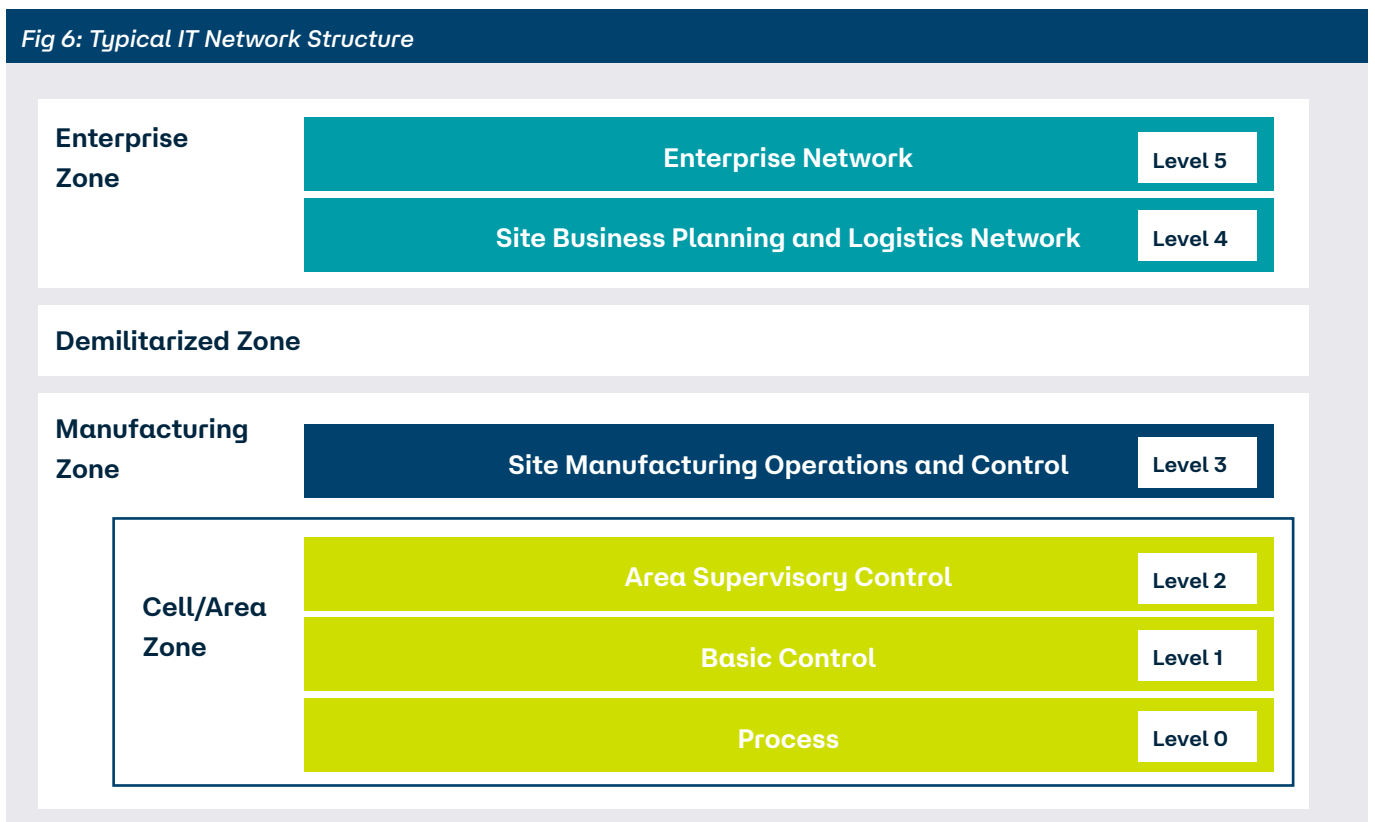
The typical IT and OT network structure consists of the following areas and components:

- Internal or trusted network, home for servers and databases.
- DMZ (DeMilitarized Zone), home for computers connected to the Internet.
- Backbone switches for the main internal cabled network traffic.
- Field switches to connect different areas to the main internal network.

- Routers and firewalls to monitor and secure the network traffic.
- Access points and radio controllers to provide wireless access to mobile users.

OT network segments are typically delivered to a terminal as part of a bigger asset, such as an STS gantry crane. Those OT networks must be integrated into the trusted network in accordance with the security rules for network segmentation, to avoid cyber risks, interference, or damage across the different segments. The following diagram (Fig 6) shows a typical network structure for terminals based on a Purdue model (reference model for the data flow between IT and OT systems). The model shows how the elements of an ICS architecture interconnect, dividing them into zones that contain information technology (IT) and OT systems. Implemented correctly with a DMZ (demilitarised zone), it helps establish an “air gap” between OT and IT systems, isolating them such that an organisation can enforce effective access controls without hindering business.

Fig 6: Typical IT Network Structure



7.2 Network Segmentation

Network segmentation is the practice of dividing the network into smaller, isolated subnetworks or segments to protect sensitive areas from unauthorised access and potential breaches. Each segment is typically separated by firewalls, routers, or switches to control traffic between them.

In a typical network environment in the terminal industry, there are a variety of networks for different purposes, such as:

- Data centre internal network
- Office network (cabled or wireless)
- Networks for separated buildings or facilities
- Outdoor wireless networks with different technologies (e.g. IEEE 802.11, 3G, 4G)
- Radio Access Networks (RAS) in 5G technology
- CCTV networks
- OT networks (e.g. internal network of an STS crane)
- The entire structure can be seen as a 'network of networks' where multiple networks are integrated for data services and network communication between systems and devices

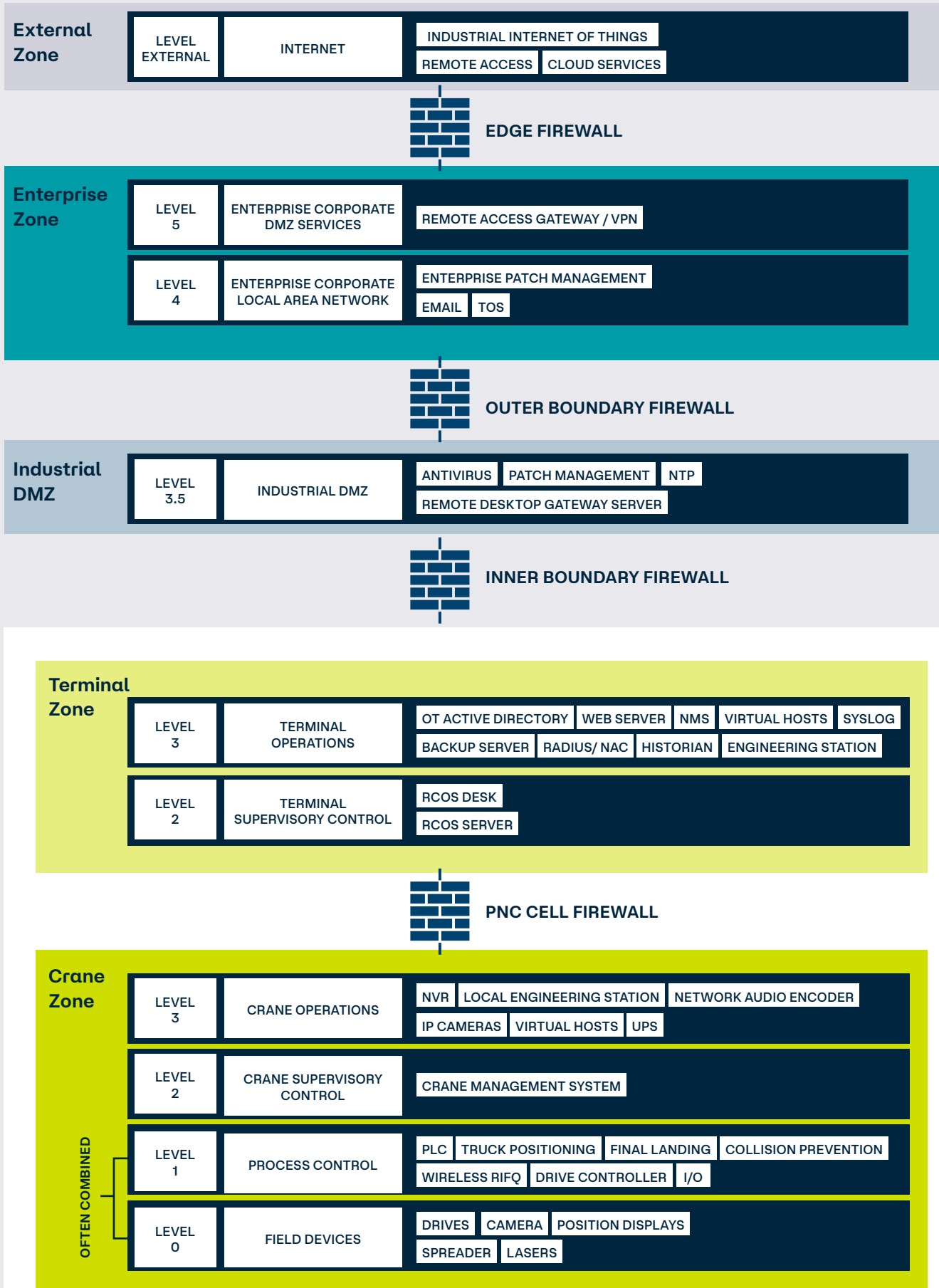
All high-risk network segments, including those processing sensitive data, office networks, and operational technology, should be configured in segregated networks. Network segmentation is a powerful method for separating and protecting different network devices from each other. It mitigates the risk that cyber threats affecting one segment can influence other segments of the network.

Moreover, all Internet-accessible systems should be segregated from the trusted network in a DMZ (DeMilitarized Zone) or be hosted by a third-party provider.

Some solution providers add a further security layer using NAT (Network Address Translation). NAT is the process of mapping private IP addresses to a single public IP address when information is being transferred via a router or firewall. NAT allows private networks to connect to external networks (e.g., the Internet) but does not allow external networks to access the private network. Therefore, network devices cannot be seen from outside the trusted network, provided that insiders do not publish the translated IP addresses.

Next-generation firewalls (NGFWs) and intrusion detection/prevention systems (IDS/IPS) should be considered. They are advanced network security devices that combine traditional firewall functionality with additional security features, such as application awareness, intrusion prevention, advanced threat protection, and user-based controls. NGFWs exceed the capabilities of traditional firewalls by offering more granular control and visibility of network traffic.

Fig 7: Example of Network Segmentation



7.3 VPN Virtual Private Networks

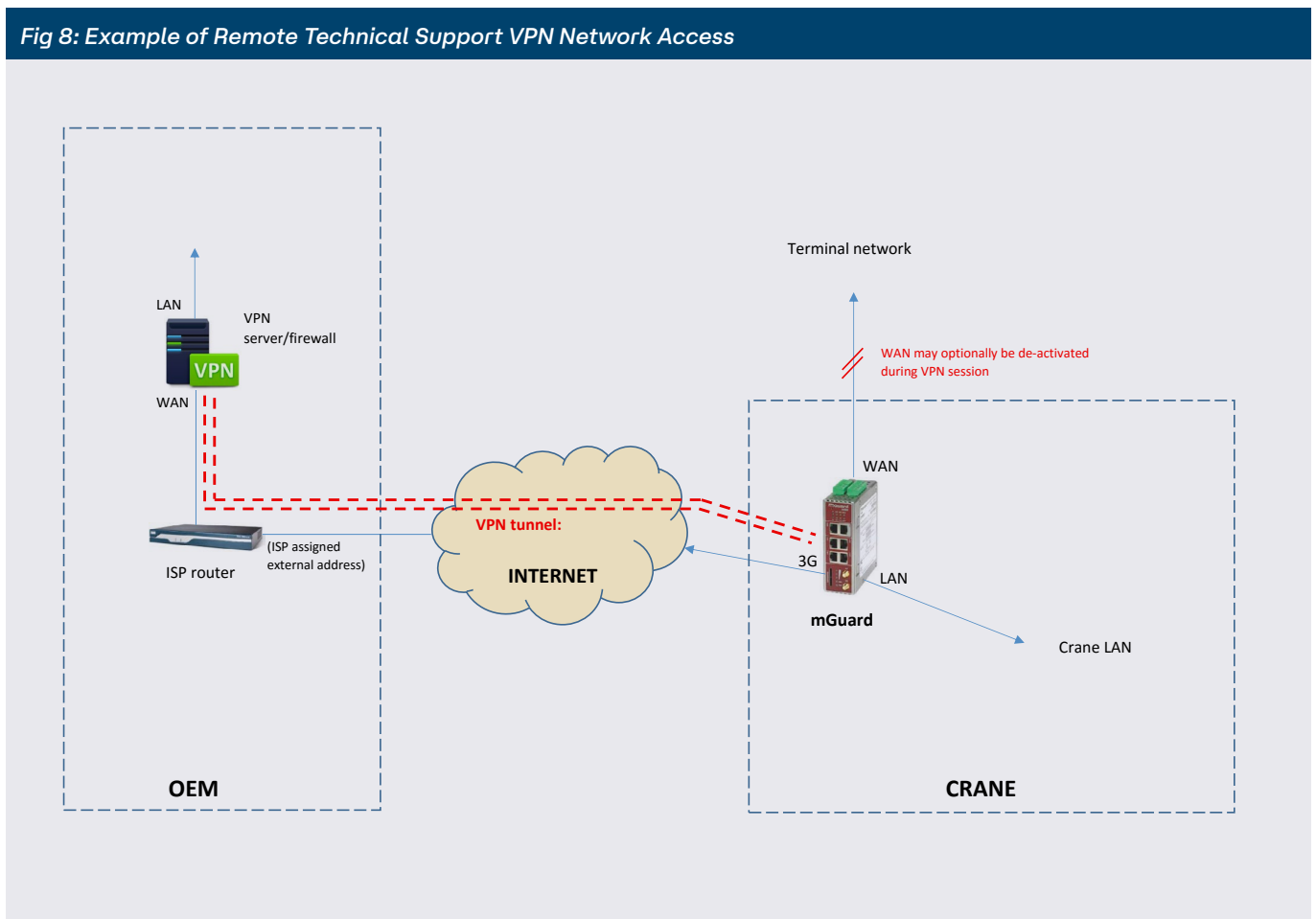
A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection between a user's device and a private network over the internet.

The primary purpose of using a VPN is to provide privacy and security while accessing the internet. When connected to a VPN, all internet traffic is routed through a secure tunnel, preventing anyone from intercepting and accessing data. This is especially important when using public Wi-Fi networks, which are often unsecured and can expose sensitive and personal information to potential attackers.

By using a VPN server, a VPN tunnel establishes a secure, encrypted connection between a user's device and a remote server or network. It is created using VPN protocols and technologies to ensure the privacy and security of data transmitted over the internet.

The VPN tunnel also masks the user's IP address, replacing it with the IP address of the remote server or network. This enhances privacy and anonymity by making it difficult to trace a user's online activities back to their actual IP address.

Fig 8: Example of Remote Technical Support VPN Network Access



7.4 Wireless Communication

Wireless communication is a rapidly growing technology in our industry and our global society. In the next decade, it is expected that several billion devices will communicate using wireless standards, with an increasing quantity of data being transferred. Latest technologies offer a bandwidth of up to 300 Mbps with enormous potential for various new applications and devices to be used:

- Mobile phones
- Tablet PCs and laptops
- Cameras and laser scanners
- Drones
- Smart sensors in all kinds of machines and facilities (IoT)

Various wireless communication standards are available for use in port and terminal environments.

IEEE 802.11

This standard has been used in our industry for many years and mainly operates on the 2.4 and 5 GHz frequencies. It provides a network speed from 50 Mbits/s up to 300 Mbits/s, depending on the signal quality between the access points and the frequencies used. In some countries, the frequency bands used by this standard may be restricted due to military use, or communication could be affected by radar systems.

Link to Wikipedia: https://en.wikipedia.org/wiki/IEEE_802.11

3G/4G/5G

These telecommunication standards have been in use since the 1980s and continue to be developed. Nowadays, a network speed of up to 900 Mbps can be achieved in mid-band frequencies, and higher speeds are possible in the high-band frequencies.

5G is the upcoming standard for IoT applications. It is anticipated that in the near future, some 50 billion devices will operate on 5G technology.

Link to Wikipedia: <https://en.wikipedia.org/wiki/5G>

7.4.1 Cybersecurity Threats in Wireless Communication

Wireless communication, when compared to cabled networks, poses significant additional risks that must be addressed.

Wireless network traffic takes place 'over the air' at various transmission frequencies. These radio signals can be affected by different sources, such as. Radar systems, jammers, other radio systems, etc. The operational impact can be extensive and long-lasting.

4G and 5G networks are supplied by external system providers. These providers are potentially exposed to cyberattacks and espionage actors seeking sensitive data. The end user cannot control these threats; as a consequence, alternative cybersecurity solutions should be incorporated into the BCP (Business Continuity Plan).

Cyberattacks such as DDoS (Distributed Denial-of-Service) may also occur in wireless networks. As a countermeasure, thresholds should be set for the transmitted traffic.

Network administration, user rights, and the configuration of devices, access points, and firewalls for wireless networks should be taken seriously to avoid any intrusion into the trusted network over the air. This is also valid and important for OT networks and the integration between OT and IT network segments.

Because of the additional risks posed by Wireless networks, such networks should only be established if cabled solutions are not possible or too expensive. In the future, the growth of wireless networks, combined with different technologies and integrated with the trusted cabled network, is anticipated. This is an area that should receive special attention from the network administrator.

7.4.2 Special Recommendations for Office Wi-Fi

Wi-Fi office connections are often public, e.g. for visitors. These users require Internet access but should not be connected to the trusted network. If users connected via an office Wi-Fi need to connect to the trusted network, they should do so via VPN.

7.4.3 Recommendations for an Outdoor Wireless Network for Operations

The wireless devices are typically well-known to the IT organisation and do not change very often.

It is recommended that access to the trusted network be granted via the MAC address (physical hardware address). Alternatively, access via HTTPS with certificates is possible. HTTPS connections rely on SSL/TLS protocols to establish a secure connection between a client and a server.

Mobile devices (e.g., mobile terminals using GSM) that are connected to the trusted network via telecommunication technology (3G, 4G) should connect via private APN (Access Point Name) connections. The telecom provider can organise such connections. Alternatively, an IP address whitelist will help avoid mobile remote access from unauthorised parties.

A telecommunication connection to the trusted network can be combined with a VPN connection.

Remote access to the trusted network by third-party suppliers may be required to perform remote maintenance. Remote access to the trusted network should always use MFA (Multi-Factor Authentication).



8. Access Control

8.1 Identification & Authentication

Access by unauthorised persons to vulnerable systems and networks, both locally and via remote access, is one of the main entry points for cyber threats in any IT or OT environment.

Port and Terminal operations are considered a mission-critical industry. It is therefore of utmost importance that the trusted persons with high system access privileges are named users and authenticated when they are allowed access to the trusted network. When accessing the systems, only secure authentication protocols should be used. Access to critical systems should be protected with MFA (Multi-Factor Authentication).

Link to Wikipedia: https://en.wikipedia.org/wiki/Multi-factor_authentication

In a segmented network architecture, access to network areas with different protection requirements should be separated using different named administrator accounts. In any case, authentication data should be stored in a secure location and preferably encrypted.

8.2 Authorisation

Every user in the system landscape should be authorised to access systems only to the minimum level required to perform their tasks (least privilege access). Different levels of user authorisation should be defined and documented, e.g. normal users, super users, and system administrators. Users, their roles, and access levels must be documented and updated with every change. Employees leaving the company should be immediately removed from system access.

The number of authorised administrators with full access rights to the systems should be kept to a minimum, ideally 2-3 accounts. Security will be enhanced if the administrators with full access rights can access the systems only from dedicated workstations. Administrator accounts should, in any case, be configured to require MFA (Multi-Factor Authentication).

8.3 Physical Access Control

The building design and layout map for the port or terminal facility should identify and define the areas that require special controls for IT and network security. Typically, these will be data centres or rooms with IT and network components, as well as rooms for administrators. In many cases, these IT-related security requirements will mirror or overlap the security requirements as detailed in the ISPS security plan that every terminal is obliged to have in place. For example, IT-related security facilities should be included in the CCTV surveillance plan and continuously monitored by a CCTV camera by the terminal's security organisation. In addition, physical access to rooms and areas where sensitive IT or network components are located should be restricted to authorised personnel. This level of security can be achieved with protected doors, coded locks, and biometric access systems such as fingerprint scanners, vein scanners, or similar systems. Moreover, alarm systems that identify unauthorised intrusion should be implemented.

8.4 Remote Access

Remote access to the trusted network by port workers has become a widely accepted practice, especially during and after the COVID-19 crisis. IT and network administrators, as well as operational users such as dispatchers and vessel planners, frequently use remote connections to access the company network and perform their daily work from home offices or other locations. To avoid any uncontrollable risk from private or other networks, remote access from the Internet to the trusted network should be granted only via VPN (Virtual Private Network) technology. Furthermore, **multi-factor authentication (MFA)** should be enforced for all remote access requests to safeguard against unauthorised access. There is a potential risk in the Terminal environment that operational users, as well as IT administrators working from home and outside the company's physical control, might be approached by criminal elements and forced or induced to share or manipulate sensitive data from the company's systems. To mitigate this risk, access times and activity logs should be stored for each remote user.

9. Data and Document Management

9.1 Data Storage and Encryption

Increasing amounts of data are stored in IT and OT environments, most of which is sensitive. Different media and storage locations are being used, such as

- Computer main memory
- SD cards
- Data and file servers on-premises or in the cloud
- Database servers
- Data warehouses or data lakes

All of this data needs to be protected by utilising the various methods described in this document. For extremely sensitive data, such as personal data and sensitive contracts, this data should be stored on a computer without a network connection. As the amount of data generated increases, more and more data storage will take place in the “cloud”. This is a potential cyber risk during the transmission and storage of data. Therefore, for cloud storage located outside the business premises and not under its control, encryption of data during transmission and storage is recommended and considered essential. The encryption method selected must be agreed upon with the cloud service provider. There are several encryption algorithms available that use synchronous and asynchronous procedures.

Some examples:

- Synchronous Triple Data Encryption Standard (Triple-DES)
- Synchronous Advanced Encryption Standard (AES)
- Asynchronous Elliptic Curve Cryptography (ECC)
- Asynchronous Rivest-Shamir-Adleman (RSA)

9.2 Electronic Document Management

In addition to the rules applicable to the general protection of sensitive data, greater attention is required when handling sensitive documents. Such documents could contain:

- Proposals
- Contracts, orders or price lists
- Sensitive system access information
- Security plans
- Other business secrets

Electronic documents are typically confidential or very confidential and should be visible only to a limited group of persons. There are several software products available on the market that enable businesses to organise their document management flow, including the signature process and protection against unauthorised access. These documents can be protected with the methods described in this document, such as password protection, MFA multi-factor authentication or be transferred through SFTP servers (Secure File Transfer Protocol). In any case where sensitive documents are stored in the cloud, their encryption is of the utmost importance.

9.3 E-Mail Management

E-mail servers and E-mail exchange are the most vulnerable areas for any organisation in terms of cybersecurity. E-Mails or mail attachments may contain malware that can potentially harm systems in the trusted network when opened if cybersecurity countermeasures are not correctly implemented. E-mails opened carelessly from untrustworthy senders could cause severe and costly damage to IT and OT infrastructure and the overall system landscape. This includes long-term downtime of operations, should systems be corrupted, encrypted or destroyed.

It is recommended to use a Secure Email Gateway (SEG) in combination with the mail server. Such an SEG will filter all incoming mail for phishing spam e-mails or other malware. Any detected threat mail will be isolated and not transferred to the end user. Suspicious senders might be blacklisted. E-mail gateways and safe data transport with encryption and certificates will mitigate cyber risk but will not provide 100% protection. Therefore, the entire organisation must be trained and knowledgeable on the safe handling of e-mails.

Setting up a secure e-mail server in a local environment can be challenging for smaller IT organisations. For this reason, many ports and terminals have migrated to a cloud-based email server solution in which the cloud service provider manages cybersecurity.

10. Security Monitoring

10.1 Log Collection

In the event of any security-related incident, the responsible managers must analyse the situation quickly, identify the cause as soon as possible, and activate measures to mitigate the risk and bring the situation under control.

In the initial phase of any cyber incident, it is crucial to have access to the logfiles, where indications and information about what triggered the incident are available. To support this analysis, any relevant access to the systems (Login/logout of an admin, change of configuration, etc.) should be stored in a log file. Moreover, any changes in system configuration should also be documented.

In critical areas (e.g., TOS), modifications to data should also be logged, including timestamps, the old and new values, and the username.

Note: Data privacy must be considered when generating log file information.

The responsible IT manager should create a catalogue of data and events that includes a permanent logging procedure. To avoid storing an inordinate amount of data, a time limit for logfiles should be set. At the end of the defined time period, the respective logfiles can be overwritten.

10.2 Log and Traffic Monitoring

Logging involves collecting and storing data related to system and network activities. This includes events such as user logins, system changes, application usage, network traffic, and security incidents. Logs are essential for investigating security breaches, analysing system performance and detecting anomalies. Common log sources include operating systems, network devices, firewalls, intrusion detection/prevention systems, and security information and event management (SIEM) solutions.

Traffic monitoring is the continuous observation and analysis of network traffic to identify potential security threats, anomalies, and policy violations. It involves capturing and inspecting network packets to gain insights into communication patterns, identify malicious activities, and detect abnormal network behaviour. Traffic monitoring tools can provide real-time visibility into unencrypted network traffic, help identify potential attacks or vulnerabilities, and aid incident response and forensic investigations.

Benefits of cybersecurity logging and traffic monitoring include:

- Early detection of security incidents and threats.
- Identification of unauthorised access attempts or suspicious activities.
- Compliance with industry regulations and data protection standards.
- Support for incident response and forensic investigations.
- Insights into network performance and optimisation opportunities.
- Enhanced visibility and understanding of network behaviour patterns.

It's important to note that effective logging and traffic monitoring require proper configuration, regular review and analysis of logs, and integration with security analytic tools or Security Information and Event Management (SIEM) solutions.

Organisations should also ensure they comply with legal and privacy considerations when collecting and storing network traffic data.

Implementing logging and traffic analysis tools is recommended to detect and respond to incidents promptly.

10.3 Incident Detection and Management

In the mission-critical environment of ports and terminals, the main goal for IT and operations managers is to keep operations running without disruption and, in the case of a disturbance, to restore normal operations as quickly as possible.

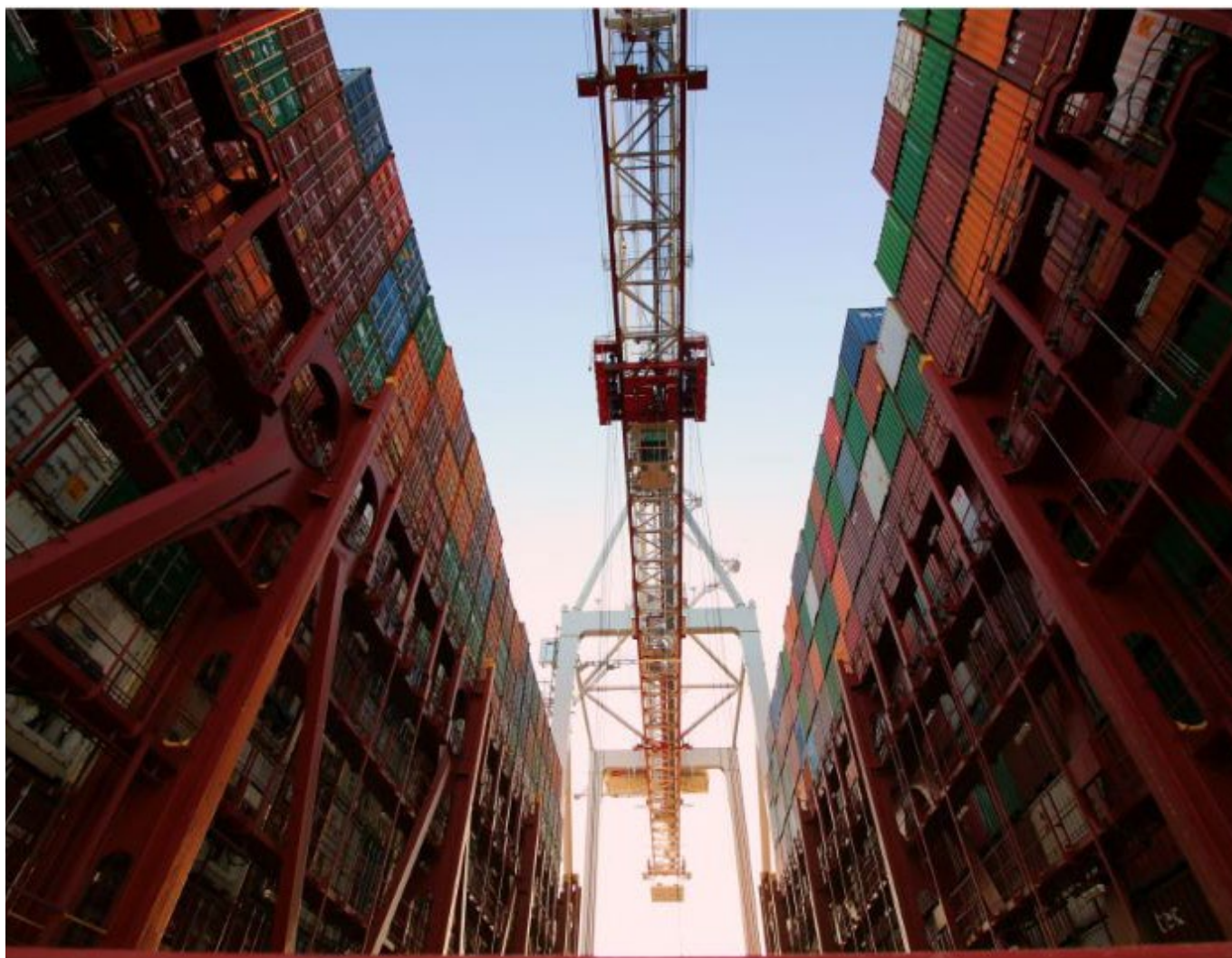
The key to achieving this goal is preparing potential incident scenarios and implementing the identified countermeasures in the event of such an incident. See also Chapter 7, Business Continuity Management.

These potential incidents may arise from various situations across operations, security, or IT/cybersecurity.

Should an incident occur and be detected, the following is an example of actions to be implemented:

- Identification of incident type according to a list
- Threat and impact analysis
- Activation of service staff
- Countermeasures according to the action list
- Inform management and other stakeholders

Establishing an incident management procedure using this approach is recommended. Many security management systems also provide incident management modules that may be used for this purpose.



11. Cybersecurity Across the Supply Chain

Managing cybersecurity across the supply chain involves implementing measures to ensure the integrity, confidentiality, and availability of goods, information, and processes throughout the entire supply chain network. The following are some key considerations and strategies for effective supply chain security management:

- Implement a rigorous supplier selection process that includes evaluating the cybersecurity practices and capabilities of potential suppliers. Conduct due diligence checks to ensure that suppliers meet security requirements and adhere to industry standards.
- Establish precise cybersecurity requirements and expectations through contractual agreements with suppliers. These agreements should include provisions related to data protection, confidentiality, physical security, and compliance with applicable laws and regulations.

- Regularly conduct cybersecurity audits and assessments of suppliers to ensure compliance with security requirements. This can involve on-site inspections, vulnerability assessments, and third-party audits.
- Implement measures to secure the transportation and logistics processes. This includes using tamper-evident packaging, tracking and monitoring systems, secure storage facilities, and proper chain-of-custody protocols.

By implementing these strategies, organisations can enhance supply chain security, minimise risks, and protect their operations, reputation, and customer trust.

12. Personal Awareness

The best technical and organisational protection mechanisms are ineffective if employees are reckless. Cybersecurity training and a clear definition of areas of responsibility are integral components of cybersecurity. As mentioned in the introduction, the responsibility for cybersecurity ultimately lies with the terminal owner.

Data from real-world cybersecurity events shows that the root cause in more than 80% of cases was inadequate training for “daily” users on the dangers posed by devices with external interfaces.

The regular, sustainable training program within the terminal organisation must be a top priority. In this context, an “unannounced stress case/test” should be conducted regularly to ensure the sustainability of the training.

Cybersecurity training is essential and must therefore be repeated regularly to keep cybersecurity awareness at the forefront of people’s minds and address new cyber risks. The content of training sessions must cover the proper handling of installed systems, removable data storage media, and software, as well as incident responses and other potential risk scenarios.

For administrators, the industry standard explicitly requires them to be trained in the proper handling of network components to ensure configurations are performed correctly.

In practice, these security procedures often lead to more complicated and time-consuming maintenance processes. A reasonable balance should be found between efforts to avoid risk and the operational performance of the overall business.

13. Recommendations

As cyber threats become more frequent and more creative, industry players are developing and deploying more sophisticated cybersecurity systems and procedures to meet the ever-changing requirements.

For the terminal owners, it is recommended to:

- Implement a continuous program to deal with cybersecurity threats.
- Establish a human awareness program to sustain security behaviour at the operator level.
- Choose methods from the available standards to ensure completeness and the applicability of the selected measures.
- Choose an automation partner that takes cybersecurity seriously, implements measures at the early phase of system development and offers effective support in the operating phase.
- Choose an automation partner that is certified to IEC 62443.
- Carry out security audits and penetration testing exercises regularly.
- Have a disaster recovery and business continuity plan in place.
- Have an incident response team in place.
- Evaluate the impact of local and global regulations.
- Focus on supply chain security and vendor assessment.
- Have a plan for updates and security patch management.
- Include physical security assessments as part of the cybersecurity program.



Appendix: Glossary

AES – Advanced Encryption Standard	IT – Information Technology
ANSSI – Agence nationale de la sécurité des systèmes d’information (French National Cybersecurity Agency)	KPI – Key Performance Indicator
APN – Access Point Name	KRITIS – Owners of Critical Infrastructure in Germany
BCP – Business Continuity Plan	MD – Machinery Directive (2006/42/EC)
BSI – German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)	MFA – Multi-Factor Authentication
CIA (Triangle) – Confidentiality, Integrity, Availability	MR – Machinery Regulation (EU) 2023/1230
CISO – Chief Information Security Officer	NET – Network Address Translation (NAT)
CMP – Crisis Management Plan	NGFW – Next-Generation Firewall
CNI – Critical National Infrastructure	NCSC – National Centre for the Protection of Critical Infrastructure (U.K.)
CRA – Cyber Resilience Act	NIS2 – Directive on Measures for a High Common Level of Cybersecurity Across the EU (Network and Information Systems Directive 2)
CVSS – Common Vulnerability Scoring System	NIST – National Institute of Standards and Technology
DDoS – Distributed Denial-of-Service	NVD – National Vulnerability Database
DES – Data Encryption Standard	OPS – Operations
DHS – Department of Homeland Security (U.S.)	OT – Operational Technology
DMZ – DeMilitarized Zone	RAS – Radio Access Networks
DRP – Disaster Recovery Plan	RSA – Rivest-Shamir-Adleman (encryption algorithm)
ECC – Elliptic Curve Cryptography	SBOM – Software Bill of Materials
EMCON – Emergency Condition	SCADA – Supervisory Control and Data Acquisition
ESB – Enterprise Service Bus	SCAP – Security Content Automation Protocol
FTP – File Transfer Protocol	SCRA – Supply Chain Risk Assessment
GDPR – General Data Protection Regulation	SEG – Secure Email Gateway
GSM – Global System for Mobile Communications	SIEM – Security Information and Event Management
IEC – International Electrotechnical Commission	SLA – Service Level Agreement
IACS – Industrial Automation and Control Systems	SFTP – Secure File Transfer Protocol
ICT – Information and Communications Technology	SSL – Secure Sockets Layer
IDA – Intrusion Detection/Prevention Systems (often IDS/IPS)	STS – Ship-to-Shore Crane
IEC – International Electrotechnical Commission	TLS – Transport Layer Security
ISPS – International Ship and Port Facility Security (Code)	TRA – Threat and Risk Assessment
ISO – International Organization for Standardization	VPN – Virtual Private Network
	WLAN – Wireless Local Area Network

About the Authors and PEMA

About the Authors

This paper was prepared by:

Alois Recktenwalt

Siemens A.G

Contributing Editors:

Torsten Neubert

HPC Hamburg Port Consulting GmbH

David Moosbrugger

Eberharter Hannes

Enmanuel Mätzler

Künz GmbH

Basit Syed

Konecranes

Daan Potters

BTG Special Products BV

Simon Miao

ZPMC

About PEMA

Founded in late 2004, PEMA's mission is to provide a forum and public voice for the global port equipment and technology sectors, reflecting their critical role in enabling safe, secure, sustainable and productive ports, and thereby supporting world maritime trade.

Chief among the aims of the Association is to provide a forum for the exchange of views on trends in the design, manufacture and operation of port equipment and technology worldwide.

PEMA also aims to promote and support the global role of the equipment and technology industries, by raising awareness with media, customers and other stakeholders, forging relations with other port industry associations and bodies; and contributing to best practice initiatives.

Membership

PEMA membership is open to:

- Manufacturers and suppliers of port and terminal equipment
- Manufacturers and suppliers of components or attachments for port equipment
- Suppliers of technology that interfaces with or controls the operation of port equipment
- Consultants in port and equipment design, specification and operations

Please visit pema.org for more information or email info@pema.org.

PEMA was constituted by agreement dated 9 December 2004 as a non profit making international association (association internationale sans but lucratif / internationale vereniging zonder winstoogmerk).

PEMA is governed by the Belgian Law of 27 June 1921 on 'associations without a profit motive, international associations without a profit motive and institutions of public utility' (Articles 46 to 57).

Company Number/ Numéro d'entreprise/
Ondernemingsnummer 0873.895.962 RPM (Bruxelles)

Registered office: p/a EIA, rue d'Arenberg 44, 1000 Brussels, Belgium

Management and finance office: Via G.B Pioda 14, CH-6900 Lugano, Switzerland



Cyber Security in
Container Terminals

Port Equipment
Manufacturers
Association

pema.org

© 2025 PEMA