CHAPTER 11
CYBERSECURITY OF OT SYSTEMS

Lecture material for TTK 4175 Instrumentation Systems and Safety at the Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU).

Author: Professor Mary Ann Lundteigen, Department of Engineering Cybernetics

The essence of making industrial plants secure?
Illustration generated by Microsoft Copilot (powered by OpenAI), July 2025

The content is updated regularly to improve precision and ensure relevance, which is reflected in the revision number. Please reach out to mary.a.lundteigen@ntnu.no if you have comments or suggestions for improvement.

Rev: 2.0/2026

Revision tracking (most recent)

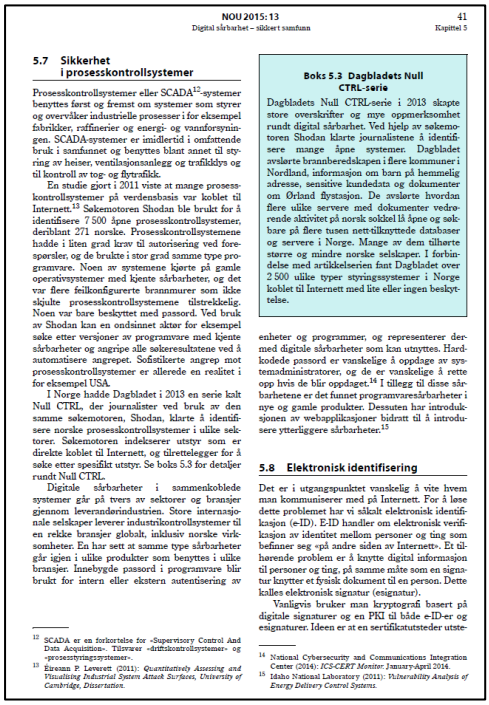
Rev	Date	Modifications
2.0/26	01.07.2026	Updated after the spring semester

Contents

11 Cybersecurity of OT systems

For a long time, it was believed that industrial control and safety systems, being part of the operational technology (OT) network, were inaccessible to external hackers. Control, safety, and IT systems were not very compatible in the past, as OT systems often used proprietary technologies that couldn't communicate with IT systems. Throughout the 1990s, more off-the-shelf technologies were introduced into OT system networks, such as Ethernet-based communication, Windows-based operator interfaces and engineering workstations, and various server types. Remote operation and remote access have also increased. Therefore, as digitalization and new ways of operating increase, OT systems are becoming more connected to IT networks and incorporating more IT technologies.

Therefore, cybersecurity has become a high priority for companies that operate and deliver systems to industrial plants. With the general trend toward digitalization, which requires access to operational data, establishing connections to control and safety systems for monitoring purposes also requires access to the general IT systems and facilities for remote access.



NOU 2015: 13 41
Digital sårbarhet – sikkert samfunn Kapittel 5

5.7 Sikkerhet i prosesskontrollsystemer

Prosesskontrollsystemer eller SCADA[12]-systemer benyttes først og fremst om systemer som styrer og overvåker industrielle prosesser i for eksempel fabrikker, raffinerier og energi- og vannforsyningen. SCADA-systemer er imidlertid i omfattende bruk i samfunnet og benyttes blant annet til styring av heiser, ventilasjonsanlegg og trafikklys og til kontroll av tog- og flytrafikk.

En studie gjort i 2011 viste at mange prosesskontrollsystemer på verdensbasis var koblet til Internett.[13] Søkemotoren Shodan ble brukt for å identifisere 7 500 åpne prosesskontrollsystemer, deriblant 271 norske. Prosesskontrollsystemene hadde i liten grad krav til autorisering ved forespørsler, og de brukte i stor grad samme type programvare. Noen av systemene kjørte på gamle operativsystemer med kjente sårbarheter, og det var flere feilkonfigurerte brannmurer som ikke skjulte prosesskontrollsystemene tilstrekkelig. Noen var bare beskyttet med passord. Ved bruk av Shodan kan en ondsinnet aktør for eksempel søke etter versjoner av programvare med kjente sårbarheter og angripe alle søkeresultatene ved å automatisere angrepet. Sofistikerte angrep mot prosesskontrollsystemer er allerede en realitet i for eksempel USA.

I Norge hadde Dagbladet i 2013 en serie kalt Null CTRL, der journalister ved bruk av den samme søkemotoren, Shodan, klarte å identifisere norske prosesskontrollsystemer i ulike sektorer. Søkemotoren indekserer utstyr som er direkte koblet til Internett, og tilrettelegger for å søke etter spesifikt utstyr. Se boks 5.3 for detaljer rundt Null CTRL.

Digitale sårbarheter i sammenkoblede systemer går på tvers av sektorer og bransjer gjennom leverandørindustrien. Store internasjonale selskaper leverer industrikontrollsystemer til en rekke bransjer globalt, inkludert norske virksomheter. En har sett at samme type sårbarheter går igjen i ulike produkter som benyttes i ulike bransjer. Innebygde passord i programvare blir brukt for intern eller ekstern autentisering av enheter og programmer, og representerer dermed digitale sårbarheter som kan utnyttes. Hardkodede passord er vanskelige å oppdage av systemadministratorer, og de er vanskelige å rette opp hvis de blir oppdaget.[14] I tillegg til disse sårbarhetene er det funnet programvaresårbarheter i nye og gamle produkter. Dessuten har introduksjonen av webapplikasjoner bidratt til å introdusere ytterliggere sårbarheter.[15]

Boks 5.3 Dagbladets Null CTRL-serie

Dagbladets Null CTRL-serie i 2013 skapte store overskrifter og mye oppmerksomhet rundt digital sårbarhet. Ved hjelp av søkemotoren Shodan klarte journalistene å identifisere mange åpne systemer. Dagbladet avslørte brannberedskapen i flere kommuner i Nordland, informasjon om barn på hemmelig adresse, sensitive kundedata og dokumenter om Ørlund flystasjon. De avslørte hvordan flere ulike servere med dokumenter vedrørende aktivitet på norsk sokkel lå åpne og sokkbare på flere tusen nett-tilknyttede databaser og servere i Norge. Mange av dem tilhørte større og mindre norske selskaper. I forbindelse med artikkelserien fant Dagbladet over 2 500 ulike typer styringssystemer i Norge koblet til Internett med lite eller ingen beskyttelse.

5.8 Elektronisk identifisering

Det er i utgangspunktet vanskelig å vite hvem man kommuniserer med på Internett. For å løse dette problemet har vi såkalt elektronisk identifikasjon (e-ID). E-ID handler om elektronisk verifikasjon av identitet mellom personer og ting som befinner seg «på andre siden av Internett». Et tilhørende problem er å knytte digital informasjon til personer og ting, på samme måte som en signatur knytter et fysisk dokument til en person. Dette kalles elektronisk signatur (esignatur).

Vanligvis bruker man kryptografi basert på digitale signaturer og en PKI til både e-ID-er og esignaturer. Ideen er at en sertifikatutsteder utste-

[12] SCADA er en forkortelse for «Supervisory Control And Data Acquisition». Tilsvarer «driftskontrollsystemer» og «prosesstyringssystemer».
[13] Eireann P. Leverett (2011): *Quantitatively Assessing and Visualising Industrial System Attack Surfaces, University of Cambridge, Dissertation.*
[14] National Cybersecurity and Communications Integration Center (2014): *ICS-CERT Monitor*, January-April 2014.
[15] Idaho National Laboratory (2011): *Vulnerability Analysis of Energy Delivery Control Systems.*

Fig. 1. From the report by NOU on digital vulnerabilities (2015)

The increased data transfer capacity and speed enabled new operating methods, including remote access and monitoring. Before 2010, cyber-attacks were not regarded as a significant threat. Still, they required specialized knowledge to hack an industrial control system, and a general attacker would not have that skill set. In 2010, the world experienced the Stuxnet attack against an Iranian processing facility for enriching uranium. From this moment, it became evident that attacks on industrial control systems were carried out not by individuals but by larger groups of experts spanning various disciplines – including advanced skills in OT systems and processing plants. The groups' motivation could be political and economic, but the scariest realization was that such attacks could cause physical harm and potentially also major accidents.

Managing cybersecurity is essential to safeguard critical infrastructure and prevent industrial accidents, as illustrated in Fig. 1 from the Norwegian public studies on digital vulnerabilities (NOU, 2015). The report called for new regulations and methods to manage cybersecurity risks. Since then, regulations in the EU and Norway have been further developed, and international standards are regularly published and updated to respond to technological trends and the threat landscape, though not always fast enough to keep pace with attackers' capabilities.

This chapter aims to raise awareness of the potential impact of cyberattacks on industrial facilities and explores strategies for identifying, mitigating, and eliminating vulnerabilities. It also presents relevant frameworks, standards, and industry practices to support the robust implementation of cybersecurity.

11.1 Abbreviations

(A selection)

ALARP	As low as reasonably practicable
CCE	Consequence-driven cyber-informed engineering
CPS	Cyber-physical system

CSRC	Computer Security Resource Center (NIST)
IDS	Intrusion detection system
IPS	Intrusion protection system
DMZ	Demilitarized zone (in a network)
EWS	Engineering workstation
FR	Foundational requirement (term used in IEC 62443)
IACS	Industrial automation and control system (term used in IEC 62443)
ICS	Industrial control system (term used in ISA TR 84.00.09)
ICT	Information and communication technology
ISA	International Society of Automation
IT	Information technology
NIS	Network and information system. Also, the name of the EU directive on cybersecurity
NIST	US National Institute of Standards and Technology
ML	Maturity level (term used in IEC 62443)
OT	Operational technology
SAS	Safety and automation (system). A term used in the Norwegian industry.
SBOM	Software bill of materials
SCADA	Supervisory control and data acquisition
SIEM	Security information and event management
SL	Security level

11.2 Regulations, standards, and resources

The number of regulations and standards governing OT cybersecurity is increasing. Norwegian regulations are anchored in existing and new EU directives on the topic. Standardization committees and government agencies are taking the initiative to unify cross-sector principles. However, this does not prevent an increasing number of new standards directed to specific sectors and specific products. The overview presented below is therefore just a taste, more than a complete one.

11.2.1 EU directives and Norwegian regulations

In the EU, the following directives are relevant:

- **EU Cyberscurity Act (CSA) (2019)**, established ENISA as a permanent EU cybersecurity agency and created a voluntary EU-wide cybersecurity certification framework for ICT products, services, and processes. ENISA supports the development and maintenance of these certification schemes, but the Act does not itself impose mandatory cybersecurity requirements on products. It remains an enforced EU regulation and continues to form the foundation of the EU's cybersecurity certification framework.
- **EU Cybersecurity Resilience Act (CRA) (2024)** establishes mandatory requirements for all products with digital elements placed on the EU market, including both hardware and software. As recently published, it will enter into force from 2027. CRA provides requirements to secure design, covering the whole lifecycle. Manufacturers are required to always keep a software bill of materials (SBOM) updated for products subject to the directive (from 1st January 2027), while it is optional for end users who modify or make their own software for internal use.
- **EU Directive 2016/1148 (NIS 2 Directive) (2022)**, replacing the previous NIS1 directive, concerns common security measures for a wide range of sectors (industry, food, public administration, etc.). Examples of requirements include responsibility management, risk management, stringent incident reporting, and enforcement of penalties for noncompliance with the directive. It also adds requirements to the reporting of cybersecurity events (of some significance).

Important for industries operating in Norway are:

- **Forskrift om digital sikkerhet** (digitalsikkerhetsforskriften), in force from October 2025. Implements the EU directive NIS2 with the aim of strengthening the digital resilience and security of the Norwegian public sector, organizations, and industries that are essential for societal functions, to prevent serious ICT incidents
- **Forskrift om virksomheter's arbeid med forebyggende sikkerhet** (virksomhetsforskriften). This regulation is anchored in the Norwegian "sikkerhetsloven» and focuses on the protection against threats to Norwegian national interests, such as espionage, sabotage, and terror, where security and cybersecurity can be one of many causes.

Nasjonal sikkerhetsmyndighet (NSM) grunnprinsipper for cybersikkerhet (NSM, 2020) is also often referenced.

11.2.2 Standards and guidelines

Several standards and frameworks have been developed to address cybersecurity in OT systems:

- **IEC 62443 (2009–2025):** Industrial communication networks – network and system security (multiple parts, published in different years)
- **NIST Cybersecurity Framework 2.0 (2024):** A general framework on cybersecurity measures organized into six categories.
- **NIST Guide on OT Cybersecurity SP 800-82 (2023):** Guideline based on NIST Cybersecurity Framework addressing OT systems in specific

Some additional guidelines addressing cybersecurity and safety are:

- **ISA TR 84.00.09 (2017):** A technical report (or guideline) on cybersecurity applied to the functional safety lifecycle, published by the International Society of Automation (ISA). The standard aims to bridge the requirements in IEC 62443 with key requirements in IEC 61511 and IEC 61508, two functional safety standards we introduced in Chapter 9.
- **IEC TR 63069 (2019):** Lifecycle requirements for functional safety and security for IACS
- **IEC PAS 63325 (2020):** Industrial-process measurement, control, and automation - Framework for functional safety and security

The term "sikkerhet" in the two references above refers to security, not safety. The Norwegian language lacks a separate word for safety and security, and "sikkerhet" is used for both, leading to confusion when the context is unclear.

Guidelines, based on standards, developed by institutions in Norway are: I:

- **DNV RP G108 (2017):** Cybersecurity in the oil and gas industry based on IEC 62443 (Can be accessed for free by registering at DNV Veracity)
- **Offshore Norge Offshore Norway (ON) guideline 104 (2026):** Guideline on the minimum requirements expected for OT cybersecurity measures for the petroleum sector. Incorporate requirements from NIST cybersecurity framework, IEC 62443.

11.2.3 Resources

Resources that reflect industry experience and are often referenced and used in the cybersecurity domain of OT are:

- **MITRE attack matrix for ICS (Accessed 2024):** A matrix with interactive links to techniques and tactics that attackers have applied, and which preventive measures can be effective. Developed by MITRE, an American not-for-profit organization with dual headquarters in Bedford, Massachusetts, and McLean, Virginia.
- **ICS Cyber Kill Chain (Assante & Lee, 2021):** A report introducing typical stages ("the kill chain") of OT cyberattacks, building on the Cyber Kill Chain® by Lockheed Martin.

> Published by the Sans Institute, an American *non-profit* company that, among other things, specializes in information security and information security training.

11.3 Terms and central concepts

The use of recognized terms and definitions is important not only for awareness but also for their correct use.

Examples of recognized sources for cybersecurity-related terms are:

- **NIST glossary (Accessed 2025)**: An open database maintained by the Computer Security Resource Center (CRCS).
- **IEC glossary portal (Accessed 2025)** : A similar database collecting many terms and definitions from IEC standards. Unfortunately, many IEC standards are not yet covered by the glossary.
- International standards (e.g., IEC, ISO, and ISA)

11.3.1 OT and related terms

The focus of this chapter is on cyberattacks and cybersecurity as they relate to OT systems, meaning layers 0-3.5 of the Purdue reference architecture (or model) introduced in Chapter 1 and explained in more detail in Chapter 2 of the compendium.

However, OT is not the only term used to refer to systems on the OT side of the Purdue model. Alternatives include:

- Industrial control system (ICS): preferred term in ISA and American guidelines
- Industrial automation and control system (IACS): preferred term in IEC 62443

Even if the terms are defined slightly differently, the meanings are quite overlapping.

11.3.2 Cybersecurity vs safety and security

Cybersecurity, **or cyber security** (as both variants are used), is a general term for the protection of digital systems against unauthorized access and attacks. The word is split into two, cyber *and* security, which may be explained as follows:

- Cyber may have different meanings depending on the context: Cyber can refer to cyberspace, a virtual world generated by computers and networks through the Internet, or to systems that integrate physical systems and computational control to interact with the real world. In the latter case, the term "cyber-physical system" is used. The term "cyber-physical system" can be applied in many contexts. From bank terminals and medical devices like pacemakers to transmitters, controllers, and switches used in manufacturing, power generation, and distribution systems, and the chemical and petroleum process industry.
- The Oxford dictionary defines security as freedom from danger and threat. The term is used in two distinct contexts: freedom from unauthorized digital and physical access, and the provision of reliable, affordable energy to society. In this chapter, the focus is on the term's first interpretation.

IEC TS 62443-1-1 (2009), the first published part of IEC 62443 defines cybersecurity as:

> **Cybersecurity:** Actions required to preclude unauthorized use of denial of service to, modifications to, disclosure of, loss of revenue of, or destruction of critical systems or information assets.

While information and communication technology (ICT) security and cybersecurity are terms with similar meanings, some argue that ICT security is more focused on general-purpose computers, printers,

and servers, whereas cybersecurity is applied to more critical systems. The term OT cybersecurity is applied more consistently to protect operational systems exposed to cyber threats, including cyber-physical systems.

The translation of "cybersecurity" into Norwegian is often "Cybersikkerhet" or "IKT sikkerhet". The use of "sikkerhet" sometimes causes confusion, as Norwegians use this translation for both safety and security, two terms with clearly different meanings.

- **Safety:** The most commonly used definition is "Freedom from unacceptable risk", which from the IEC online glossary.

  Unacceptable risk refers to the potential for the unacceptable frequency and severity of harm to people, the environment, and critical assets arising from unintentional and non-deliberate acts and random events, both external (e.g., floods and storms) and internal (e.g., faults and process/system upsets).

- **Security:** This term does not have *a well-established definition* like safety, and alternatives can be retrieved from, e.g., the ISO online browsing platform. Here, we have chosen the following one: "resistance to intentional, unauthorized act(s) designed to cause harm or damage to a system".

  We note that the damage is the result of deliberate acts by unauthorized individuals, indicating intentional damage. From other definitions of security, it is evident that damage relates to the loss of confidentiality, integrity, and availability.

Overall, the definitions show two of the foundational differences between safety and security, namely the nature of the causes of loss: First, while safety primarily considers random events and unintentional human errors, security considers intentional and unauthorized acts. Second, safety concerns damage to people and the environment, while security (most often) focuses on damage to data and information systems.

11.3.3 Priorities of IT security vs OT security

Cybersecurity may be regarded as a subset of information security. Here, information security has traditionally prioritized the losses in the following order, as shown on the left side of Fig. 2, building on the explanation of terms in IEC TS 62443-1-1 (2009):

1. Confidentiality (C): The assurance that information is not shared with unauthorized individuals, processes, or devices.
2. Integrity (I): The property of a system to preserve correct data, i.e., data and information that have been changed, destroyed, or lost in an unauthorized manner.
3. Availability (A): Ability of an item to perform its functions under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided.

OT systems interface directly with operational facilities, where availability is essential for maintaining safe and reliable production. Their mission, including ensuring safety, is best fulfilled when systems remain continuously available, which is why availability is prioritized as the top concern. In contrast, loss of confidentiality typically has a limited direct impact on operations and is therefore considered a lower priority. Integrity ranks second, as unauthorized modifications to messages could compromise system behavior and, if ICS components are manipulated, lead to a loss of availability. While the three core principles of IT security, confidentiality, integrity, and availability, also apply to OT systems, their prioritization differs, as illustrated in Fig. 2 to the right.

For cybersecurity, therefore, reverses the order of prioritization to:

1. Availability (A) focusing on maintaining control and safety systems operational, including operator interfaces, also during a cyber-attack.
2. Integrity (I) focusing on the ability to avoid or manage manipulated information.
3. Confidentiality (C) focusing on preventing data about control and safety systems from being shared with unauthorized people.

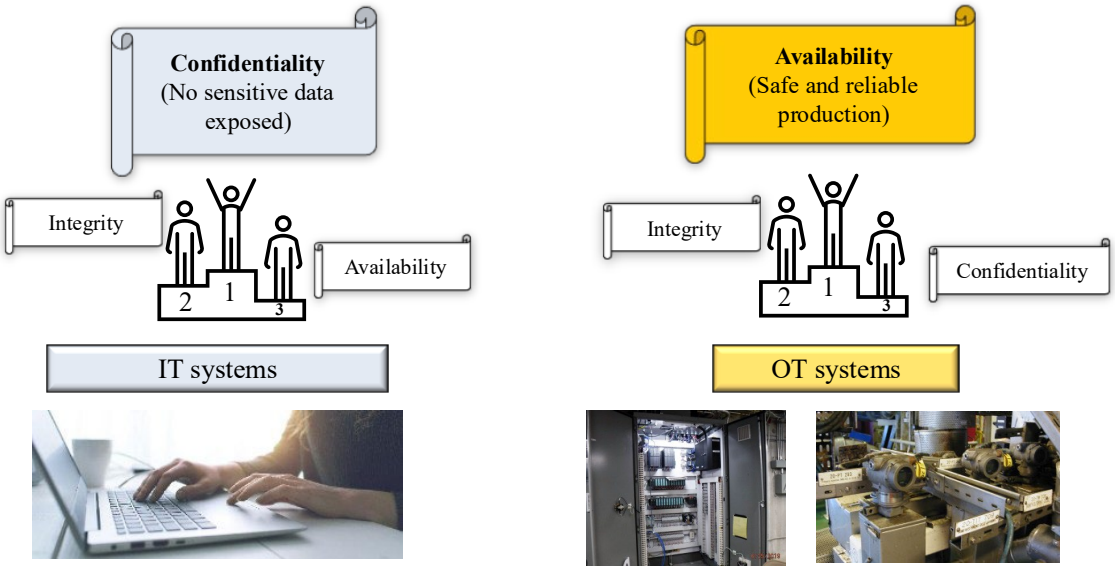


Fig. 2. Comparing IT and OT priority ranking

11.3.4 Cyberattack and threats

A cyberattack encompasses malicious activities that collect, disrupt, deny, degrade, or destroy information system resources or the information itself. For example, the NIST glossary (Accessed 2025) defines a cyber-attack as:

> **Cyberattack:**
> (i) An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure or destroying the integrity of the data or stealing controlled information.
> (ii) Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Some practical examples of what a cyberattack may target at an industrial facility are illustrated in Fig. 3. For example, cyber-attacks can involve unauthorized access to the control room, thereby enabling manipulation or loss of operators' views. An attack may also interfere with communication between the control room and the plant by modifying or preventing commands. Other examples include manipulating alarms, such as disabling a fire alarm, or manipulating processes and safety controllers. Manipulating configuration data may affect intelligent (smart) sensors if the data is accessible via networks.

The executor of a cyberattack can be identified as an adversary or attacker, which by NIST glossary (Accessed 2025) are defined as:

> **Adversary:** Person, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attacker: A party, including an insider, who acts with malicious intent to compromise a system

In some cases, the attacker may take a more active role in luring the organization using a man-in-the-middle attack. The NIST glossary defines such an attack as:

> **Man-in-the-middle attack:** An attack where the adversary positions him/herself in between the user and the system so that they can intercept and alter data traveling between them.

The man-in-the-middle attack requires that a command and control (CC or C2) has been established so that communication can be routed through their machine, allowing them to monitor, modify, and interrupt without the others being aware of a "third person" being in the loop. This would be an alternative or complement to having the malware execute such manipulations.

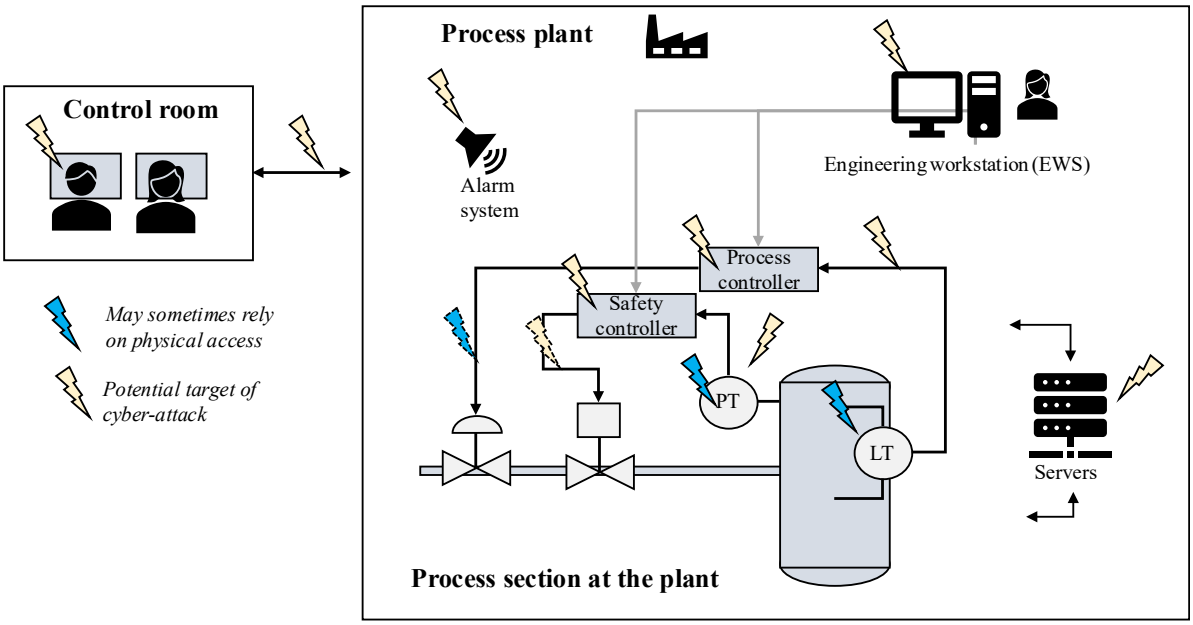


Fig. 3. Cybersecurity and potential impact on control and safety

The persons, groups, or organizations that can conduct a cyber-attack are referred to as threat actors.

> **Threat actor (or organization/group):** An individual or group posing a threat (NIST glossary, Accessed 2025).

Dragos is one of the organizations that provides updates on various threat actors and their recent activities in their annual Year in Review reports.

The different ways a threat actor can create unwanted events and risks of harm to an organization can be referred to as a threat, or more precisely, by NIST glossary (Accessed 2025) as:

> **Threat:** The Potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

There may be several potential entry points and paths an attacker can use to gain access to a protected network or systems. These can be named as:

> **Threat vector:** Path or means by which a threat source can gain access to an asset (IEC 62443-3-2).

> **Attack surface:** The set of points on the boundary of a system, a system element, or an environment where *an attacker can try to enter, cause an effect on, or extract data from (NIST glossary).*

Methods used to carry out an attack are sometimes classified as either tactics or techniques. Here, we have adopted the definitions from MITRE attack matrix for ICS (Accessed 2024):

> **Technique:** Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.
>
> **Tactic:** Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Specific examples of techniques and methods are provided in the matrix.

11.3.5 Cybersecurity measures and barriers

Measures for prevention, as well as measures for detecting, responding to, and recovering from a cyberattack, are often referred to as countermeasures (or security measures).

> **Security (or counter) measure** Action, device, procedure, or technique that reduces a threat, a vulnerability, or the consequences of an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective actions can be taken (IEC 62443-3-2).

The definition highlights that security measures can be technical, organizational (assigning roles and responsibilities), and operational (procedures carried out by humans).

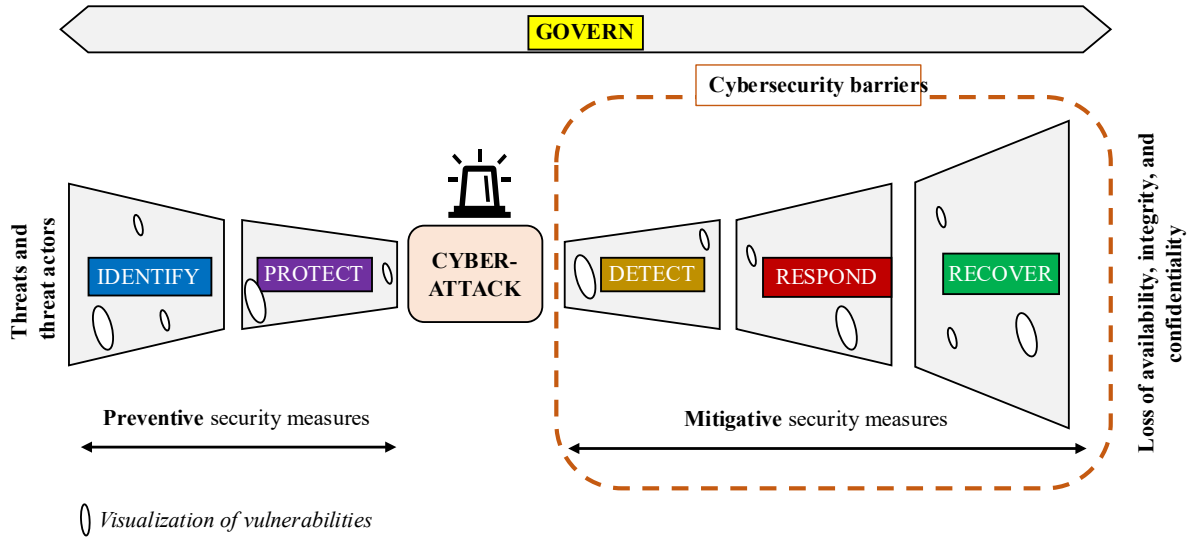


Fig. 4. Combining some of the cybersecurity-related terms

The NIST Cybersecurity Framework 2.0 (2024) identifies several security measures organized into six categories:

- **Govern:** Management and monitoring of the status and necessary improvements related to the other five categories, covering technical, organizational, and operational (human involved) measures.
- **Identify:** Identification of cybersecurity risk related to own asset. Central here is updated inventory system overview, both of hardware, software, and network.
- **Protect:** Implementation of measures that safeguard all software and hardware, by access control, training, and network segmentation as examples:
- **Detect:** Implementation of measures to monitor and detect cybersecurity events and anomalies.

- **Respond:** Preparation for and execution of mitigative activities in case of a detected cyberattack.
- **Recover:** Development of plans and act according to these to restore the capabilities of affected systems

Fig. 4 identifies the security measures in a bow-tie model (see Compendium Chapter 6), specifying how each category of measures listed above is preventive (primarily to prevent attacks) or mitigative (primarily to mitigate consequences, given that the attack is present). The Norwegian oil and gas sector has adopted the term "cybersecurity barrier" in a newly developed guideline on cyberbarrier management for security measures (Øien et al., 2025).

> **Cybersecurity barrier:** A measure intended to a) detect abnormal conditions, b) prevent abnormal conditions from developing, and c) limit the damage caused by cyber incidents.

Security measure categories that can be regarded as cybersecurity barriers are highlighted in Fig. 4. The concept of vulnerabilities being holes in barriers is also illustrated. It is when these holes align that a threat actor can ultimately cause permanent or long-lasting loss of availability, integrity, and confidentiality.

11.3.6 General cyberattack strategies and methods

A cyber-attack may involve a set of stages, as shown in Fig. 5. The first step, referred to as gaining access to a company's network and systems, often involves installing malware.

> **Malware:** Malicious hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose (NIST glossary, Accessed 2025).

Malware may be installed by using one of the following strategies:

- Social engineering, defined as the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust (NIST glossary, Accessed 2025). Social engineering may be directed more generally or towards people expected to be authorized to access key systems of interest of an attack.
- Direct (or physical) access using, e.g., a USB, which relies on physical access to equipment inside the IT or OT system. It can target both the IT and OT systems.
- Exploitation of a vulnerability within IT or OT that has not yet been identified or resolved.
- Conducting supply chain attacks, i.e., adding unauthorized pieces of hardware or software (also referred to as trojans) into the supply chain, for example, a sub-supplier, which will end up inside the IT or OT system when a system is installed.

Social Engineering combines sociological, psychological, and information-gathering techniques used to manipulate people with the goal of:

- Persuade them to release sensitive information
- Perform actions that do not comply with standard security measures
- Getting them to act in a way that allows unauthorized access or use of systems, networks, data, or information

Social engineering techniques include spoofing and phishing. For example, the NIST glossary defines these terms as:

> **Spoofing:** Faking the sending address of a transmission to gain illegal entry into a secure system.

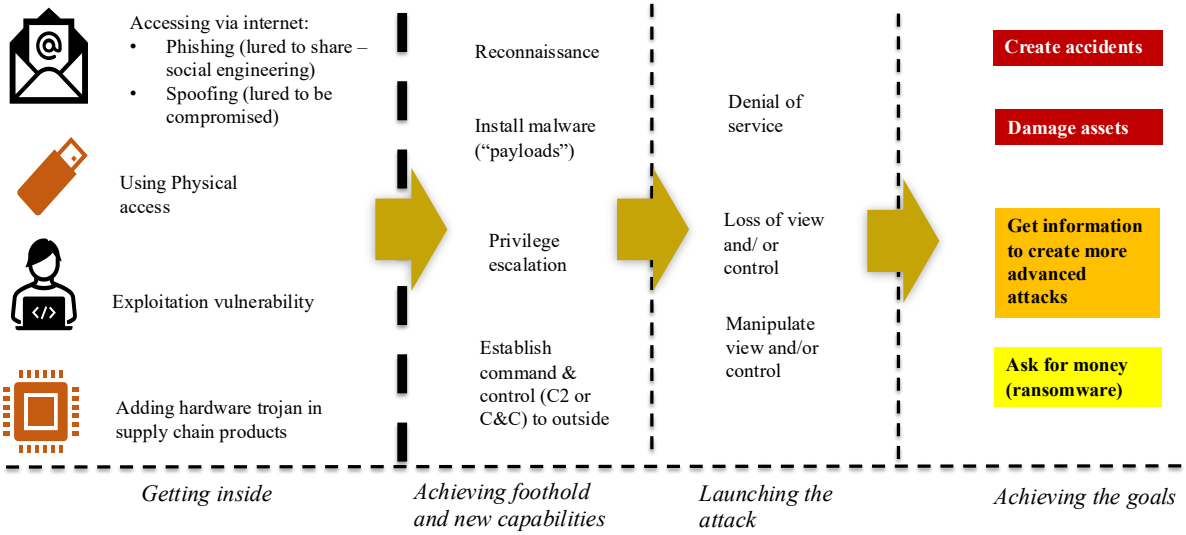


Fig. 5. Generic steps of a cyberattack

Spoofing may involve sending from a fake email address, receiving a call from a fake phone number, or sharing the address with a fake webpage. The main goal of spoofing is to make the recipient believe that the message or link is from a trusted person or source. Phishing is the next step after successful spoofing. Phishing involves luring people into providing sensitive data. The NIST glossary defines the term as:

> **Phishing:** A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

The first stage of what is to become an OT attack may involve a spoofing and phishing campaign targeting company personnel believed to have authorization to access OT systems. Perhaps they use similar passwords and user credentials for several systems. Other targets for spoofing and phishing include webpages likely to be visited by personnel working with OT systems.

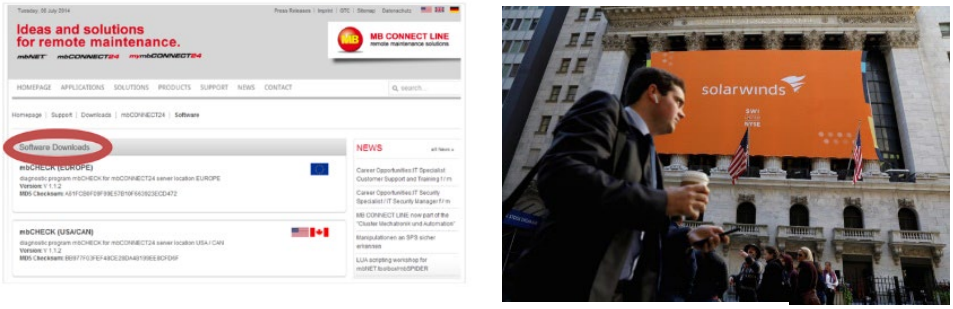


Fig. 6 Companies targeted by supply chain attack

A phishing campaign can target the company directly or indirectly via a supply chain attack. Here, a supply chain attack is defined by the NIST glossary as:

> **Supply chain attack:** Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

A supply chain attack can target suppliers' software or webpages that clients using the products will visit to do prescribed upgrades to new versions. Another approach is to introduce hardware trojans, i.e.,

unauthorized physical circuit modifications. Hardware trojans require a different approach to gain access, as the attacker must physically contact the hardware. Therefore, if creating hardware trojans is a target of an attack, it needs to identify a supplier in the value chain of a larger system with weak points. Weak points can relate to how people are checked before being hired in product development, how physical access to the production process is protected, and how quality assurance is monitored.

Two examples of supply chain attacks targeting software are shown in Fig. 6:

- In 2014, hackers succeeded in installing malware in a VPN gateway software product for remote access by the German company MB Connect Line. After customers downloaded the product, remote attackers could execute arbitrary commands without authentication.
- In 2019, hackers were able to install malware into IT infrastructure management services that the US company SolarWinds delivered to thousands of customers, including public and private companies. When their service platform was hacked, the malware also infected customers' IT systems, allowing hackers to steal customer data for further activities, such as spying.

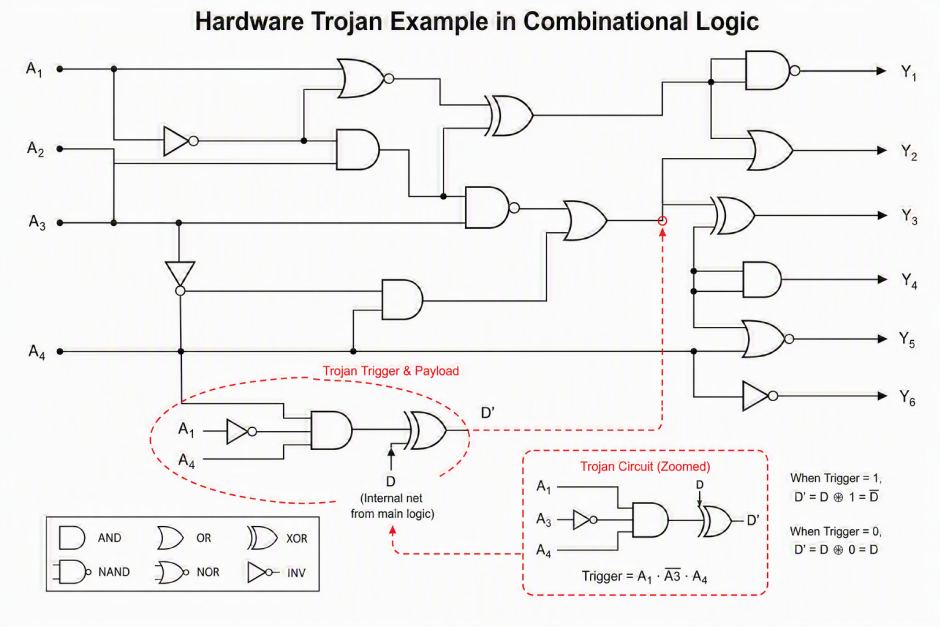


Fig. 7. Example of a (simple) hardware Trojan (red color) added to the logic (generated by Copilot)

With physical access to the hardware or central hardware documentation, an attacker can manipulate as follows:

- Use of a hardware Trojan, which is a non-legitimate/unauthorized physical circuit change on a circuit board. Components added in an unauthorized way to the circuit board, such as transistors, can realize, e.g., (not legitimate) logical AND & OR operations as shown in Fig. 7. A Trojan with a more complex architecture can implement features that shut down the hardware (kill switch), steal information from the legitimate part of the circuit board, and possibly share it further externally.
- Install new instructions to replace or add to existing coded functions and operations. For example, adding a new code to an existing integrated circuit, or adding a new integrated circuit that is triggered externally or on preset conditions, can put the operation into an infinite loop, which has a similar effect to a denial-of-service (DoS) attack.
- Mount extra physical components that capture data that should have been deleted but are in memory.

A more detailed insight into hardware trojans can be found in, e.g., Iyengar and Ghosh (2017) as part of the book titled The Hardware Trojan War by Bhunia and Tehranipoor (2017).

Once inside the IT and, eventually, the OT systems, the attacker can use several techniques to obtain the access needed to execute the attack. A selection of techniques includes:

- Establish command and control (C2): C2 is a technique attackers use to communicate with compromised devices over a network. It involves establishing a one-way or two-way communication channel between the intruded systems and the external attacker.
- Privilege escalation: Adversaries use various techniques to gain higher-level permissions in systems and networks by exploiting vulnerabilities caused by, e.g., misconfigurations and programming errors.
- Evasion: The adversary may use various techniques to remove any indicators of their ongoing activities.
- Creating a backdoor: Adversaries use methods for bypassing standard authentication or encryption. The NIST glossary identifies a malicious program that listens for commands on a specific Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port as one such example.
- Exploit known/standard ports. Attackers can target ports on equipment to insert malware over the protocol without it being perceived as suspicious.
- Masking: The attacker hides malware and executable files using known file names and types, often naming files like the original or legitimate files.

11.3.7 Zero-day vulnerability

The most severe vulnerabilities are, of course, those that are yet unknown, and these are referred to as zero-day vulnerabilities.

> **Zero-day vulnerability:** A vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available (Wiki).

The term "zero days" means (even if unrealistic) that the vendor has zero days to prepare a patch to make the product secure. However, until it is brought to their attention, those who discover a vulnerability can work undisturbed, exploiting it until the vendor is made aware of it. From the vendor's perspective, the clock starts, and the race runs until the repair software (or patch) is published. During the same period, while the patch is being developed, affected users may be notified and given temporary compensation measures.

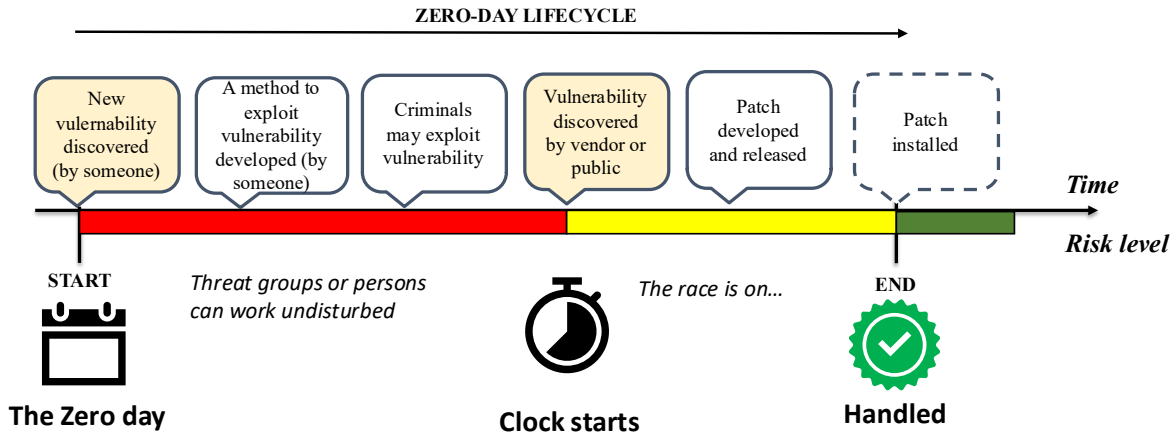


Fig. 8. Zero-day lifecycle

The phases described are referred to as zero-day and are illustrated in Fig. 8

The color coding along the timeline identifies the risk level, with red indicating the period of highest risk of unwanted impact from the vulnerability, yellow indicating medium risk when compensating measures may be put in place, and green indicating low risk after the patch has been published.

A zero-day attack refers to an attack that exploits a zero-day vulnerability, and may occur at any point before the patch has been published (and deployed):

> **Zero-day attack:** An attack that exploits a previously unknown hardware, firmware, or software vulnerability (NIST glossary, Accessed 2025).

11.3.8 Security zones and conduits

According to the NIST glossary, network segmentation is the practice of dividing a network into smaller subnetworks, for example, by creating separate areas protected by firewalls configured to restrict unnecessary traffic. Network segmentation helps reduce the impact of malware, unauthorized access, and other cyber threats by limiting their ability to spread throughout the network.

This definition is commonly applied in traditional IT environments, where firewalls and other network security controls can often be implemented with relatively few operational constraints. In OT environments, network segmentation is equally important, but its implementation must consider additional factors such as safety, availability, operational requirements, legacy systems, and risk:

- **(Security) Zone**: Grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access, or responsible organization.
- **Conduit**: Logical grouping of communication channels that share common security requirements, connecting two or more zones.

In practice, OT network segmentation is not achieved solely through firewalls. While firewalls are commonly used at key boundaries, particularly between enterprise and industrial networks and between security zones, security is also provided through device-level protections, authentication and authorization mechanisms, network access controls, system hardening, and defense-in-depth strategies.

As a result, systems with lower inherent security or greater exposure are often placed behind additional layers of protection, while critical operational assets are located deeper within the network and are accessible only through controlled conduits and security controls.

11.3.9 Vulnerability and vulnerability assessments

A cyberattack often involves exploiting known and unknown vulnerabilities:

> **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (NIST glossary, Accessed 2025).

Regular vulnerability assessment belongs to the “identify” security measure category in Fig. 4, and covers tools and processes related to identifying vulnerabilities and ensuring the effectiveness of the implemented measures:

- **Vulnerability assessment:** Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation (NIST glossary, Accessed 2025).

Examples (slightly reworded) of vulnerabilities mentioned in the NIST Guide on OT Cybersecurity SP 800-82 (2023), Annex C, on ICS security are:

OT network architecture:

- Inadequate incorporation and management of security, so that the network and connected devices are insecure from the beginning or evolving.
- No or insufficient implementation of a security perimeter, like a DMZ.
- Insufficient separation of control networks from non-control networks and traffic, where non-control traffic relates to communication not part of real-time control and safety.
- Inadequate measures implemented to collect event data about incidents, misconfigurations, and other security-related failures.
- Intrusion detection systems (IDS), or intrusion protection systems (IPS), are not installed or are not efficient.
- Firewalls not deployed where they are needed or improperly configured
- Inadequate consideration of how security is managed when insecure protocols are being used (typically at the lower Perdue levels)
- Inadequate authentication between wireless clients and access points

Systems and devices connected to the OT network:

- Lack of an updated asset inventory list and asset management, so that the organization does not know what it has, where the systems are, and what versions of software, hardware, and firmware are being used.
- Late availability of software patches, or vendors not providing them at all (e.g., if systems are no longer supported).
- Lack of sufficient testing of patches before deployment.
- Lack of sufficient testing and approval of configuration changes that could impact security protection
- Poor remote access controls (and privileges), meaning that there is insufficient control over who can access, what they are authorized to do, and to what extent their access and authorities are required.
- Critical configurations are not stored and backed up due to a lack of procedures and support systems.
- Vendor default passwords are used and not modified after installation.
- The need for IDS and IPS on devices is not adequately assessed, and the systems are not correctly implemented and followed up on.
- Unauthorized access to sensors and final elements.
- Inappropriate segmentation of systems used for asset management (monitoring, configuration) from systems used for active control.

Physical access vulnerabilities:

- Lack of physical restrictions for unauthorized personnel to have physical access to equipment
- Lack of protection against unauthorized triggered radio frequencies, electromagnetic pulse (EMP), temporary power outage, static discharge, and voltage spikes.
- Lack of (protection of) backup systems, e.g., power supplies
- Lack of protection or removal of physical ports (like USB).

However, performing a vulnerability assessment once or twice does not ensure protection. It is necessary to determine when or how often a new vulnerability assessment is needed and to ensure that all findings are followed up. This is what vulnerability management is about. For example, Microsoft defines vulnerability management as:

Vulnerability management: The process of continuously identifying, evaluating, treating, and reporting vulnerabilities.

There are many approaches for conducting vulnerability management. For example, Dragos suggests a six-step process to determine the priority of addressing vulnerability. They are, with some minor edits to the wording:

1. Always ensure a comprehensive and up-to-date asset inventory, with all OT assets, including make, model, and firmware versions.
2. Keep updated network mapping, which is crucial for visualizing communication flows to understand potential attack paths.
3. Map your asset inventory hardware and software against the Common Vulnerabilities and Exposures (CVE) registry to identify applicable flaws
4. Decide which vulnerabilities to prioritize for further handling: Prioritization can be done using the Common Vulnerability Scoring System (CVSS) or other similar (and sometimes company-internal) guidelines. Prioritization concludes with one of the following decisions: resolve now, later, or never, depending on the urgency and the extent to which other compensating measures are favored.
5. When patching is not immediately possible for high-risk vulnerabilities, select the most appropriate compensating controls, such as network segmentation or temporary isolation.
6. Make sure to have efficient continuous monitoring of networks implemented, using passive monitoring techniques to detect anomalies and threats without disrupting operations.

11.3.10 Cybersecurity risk and risk analysis

Traditional risk analyses define risk by the probability and consequence of an event that may cause harm:

Risk = Probability (of event) x Consequence (of potential harm)

The events are considered random or unintentional, and the harm is considered to people, the environment, and critical (physical) assets. Some of these qualify as major accidents involving multiple fatalities or injuries, extensive environmental damage, and the loss of valuable physical assets.

The nature of cybersecurity risk differs from traditional risk:

- Cyber-attacks are not random and unintentional events but planned, hostile, and deliberate acts. Therefore, assigning probability or frequency to such events is challenging and less relevant.
- Instead, the term probability is replaced by two other parameters that impact the likelihood: First, a threat must exist, meaning that someone is interested in conducting an attack if they find the opportunity. Second, there must be an opportunity, such as a vulnerability that can be exploited.
- The primary consequences are not physical harm but the loss of confidentiality, integrity, and availability. However, for industrial plants, the secondary consequences could be physical harm.

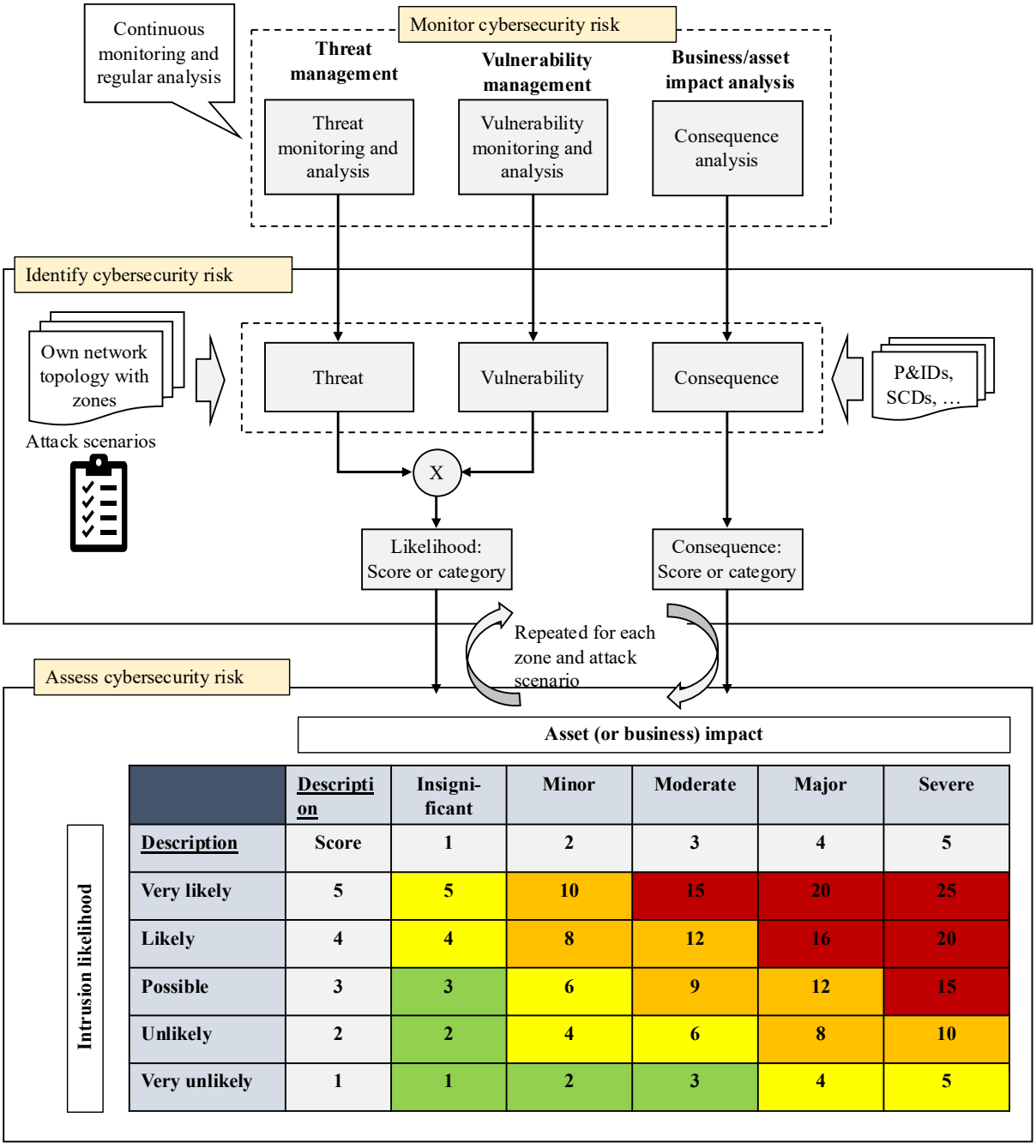
IEC 62443-3-2 (2020), therefore, defines risk in the context of cybersecurity as:

Cybersecurity risk: *Expectation of loss is expressed as the likelihood that a particular threat (T) will exploit a particular vulnerability (V) with a particular consequence (C).*

The corresponding formula can be expressed as:

Cybersecurity risk = Threat x Vulnerability x Consequence

Unlike in traditional risk analysis, likelihood is rarely supported by statistical data, as the events are often too unique to be comparable. Instead, expert judgment is made by considering specific threat and vulnerability zones and per-attack scenarios.



	Description	Insignificant	Minor	Moderate	Major	Severe
Description	**Score**	**1**	**2**	**3**	**4**	**5**
Very likely	**5**	**5**	**10**	**15**	**20**	**25**
Likely	**4**	**4**	**8**	**12**	**16**	**20**
Possible	**3**	**3**	**6**	**9**	**12**	**15**
Unlikely	**2**	**2**	**4**	**6**	**8**	**10**
Very unlikely	**1**	**1**	**2**	**3**	**4**	**5**

Fig. 9. Cyber-risk monitoring, identification, and assessment process

The identified vulnerabilities and their exploitation potential, considering the threat actors' capabilities and network security measures, may conclude on a likelihood on a qualitative scale, such as the example provided in IEC 62443-3-2 (2020), Annex B:

- Almost certain (more than 90% chance)
- Likely (more than 50% chance)
- Moderate (from 10% to 50% chance)
- Unlikely (3%-10% chance)

- Rare (less than 3%)

The likelihood categories can be combined with consequence categories in a risk matrix. Color-coding the cells can identify the combinations of the two that require risk reduction. Fig. 9 illustrates how the cyber risk assessment process can be conceptualized. Here, it is assumed that a company continuously monitors the threat landscape, intrusion attempts, and vulnerabilities, and, on a regular and on-demand basis, updates threat, vulnerability, and business impact analyses.

The outcomes of the three types of analyses can inform cybersecurity risk assessments for specific zones and attack scenarios. The assessment of threat and vulnerability is often combined with the likelihood of intrusion. The consequences are also evaluated and assigned a score or category, based on applicable information about the plant. The figure identifies examples of relevant documentation, including piping and instrumentation diagrams (P&IDs) and system control diagrams (SCDs). A risk matrix may identify, by color-coding following the ALARP principle, at what level cybersecurity risk is broadly acceptable (green region), unacceptable (red region), or acceptable on the condition that additional measures are implemented (yellow and orange regions).

11.4 Loss of safety and loss of cybersecurity

Loss of cybersecurity can directly affect safety, particularly when it compromises the availability or integrity of systems that perform safety-critical functions. When such systems become unavailable or malfunction due to cyber incidents, their ability to prevent or mitigate hazardous events may be impaired, potentially leading to a loss of safety.

In traditional safety engineering, accidents are prevented by safety barriers, which may be human, operational, or technical. These barriers are designed to prevent incidents, detect emerging hazards, and respond effectively when required. If a safety barrier is degraded or unavailable, whether due to technical failure, human error, or external interference such as a cyberattack, its protective function is weakened. This degradation increases the likelihood that a hazard will propagate and escalate, which may ultimately result in an accident.

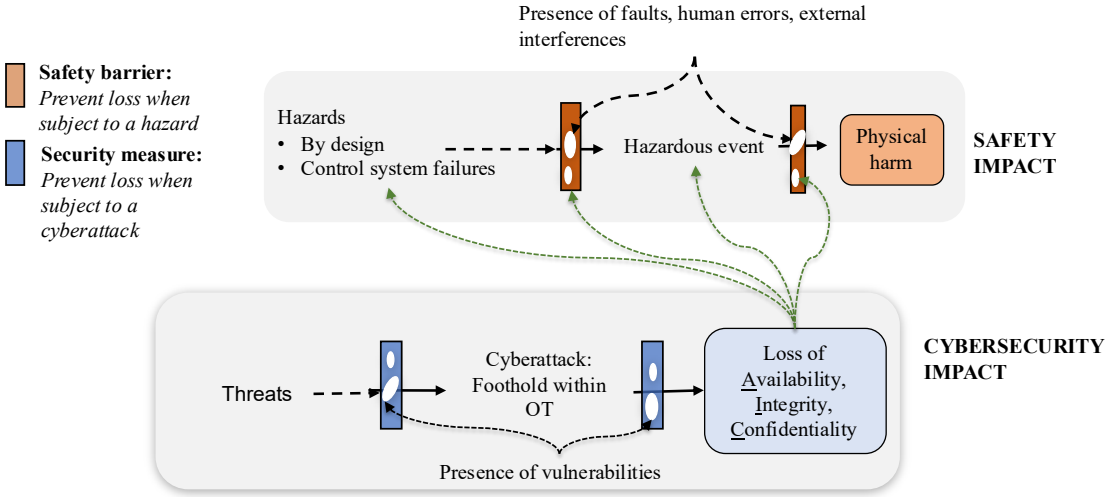


Fig. 10. Examples of how safety may be affected when OT systems are attacked

When evaluating the reliability and availability of safety barriers, the analysis has traditionally focused on factors such as technical failures, human errors, and external interface influences. In this context, the potential impact of cybersecurity has typically not been explicitly considered. However, the increased exposure of OT systems to cybersecurity risks requires recognizing that impairment of cybersecurity measures may also degrade safety barriers. Such impairments can either reduce the effectiveness or

availability of existing barriers or introduce new types of hazardous scenarios that were not accounted for in their original design.

The relationship between cybersecurity measures and their ability to prevent loss of availability, integrity, and confidentiality of OT systems and safety barriers is illustrated in Fig. 10, using the well-known, the Swiss cheese model proposed by Reason (1990). In this model, safety barriers are depicted as layers of defense in the upper part of the figure, each containing "holes" that identify causes of degraded performance. When these holes align across multiple layers, the barriers fail collectively, allowing hazards to pass through unmitigated and potentially result in harm.

Similarly, the cybersecurity measures shown in the lower part of the figure can be understood as layers of defense against cyberattacks and their consequences. Each layer contains "holes" representing known and unknown vulnerabilities. When one or more of these vulnerabilities are exploited, cybersecurity incidents may occur, potentially disrupting system functionality, corrupting data, or delaying critical responses, some of which may create new or enlarge "holes" in the safety barriers. In some cases, such exploitation can also create new types of hazards and hazardous scenarios not designed for with the current safety barriers, as illustrated in Fig. 10.

Fig. 11 extends Fig. 10 with some more information and examples. The figure illustrates how cyber-induced manipulation can affect safety through two main pathways. First, manipulation of computerized systems may lead to loss of availability in both safety and non-safety functions, thereby degrading the performance of existing safety barriers. Second, manipulations such as altering engineering documentation or exploiting inherent limitations in process design may introduce new hazardous scenarios by pushing the system beyond its intended operational constraints. These effects are not mutually exclusive; rather, combining multiple manipulations can further escalate the situation, simultaneously weaken safety barriers, and create conditions not anticipated in the original design. Hazardous events treated as extremely unlikely in conventional safety risk analysis may become more likely when considering that a cyberattack can employ multiple techniques simultaneously.

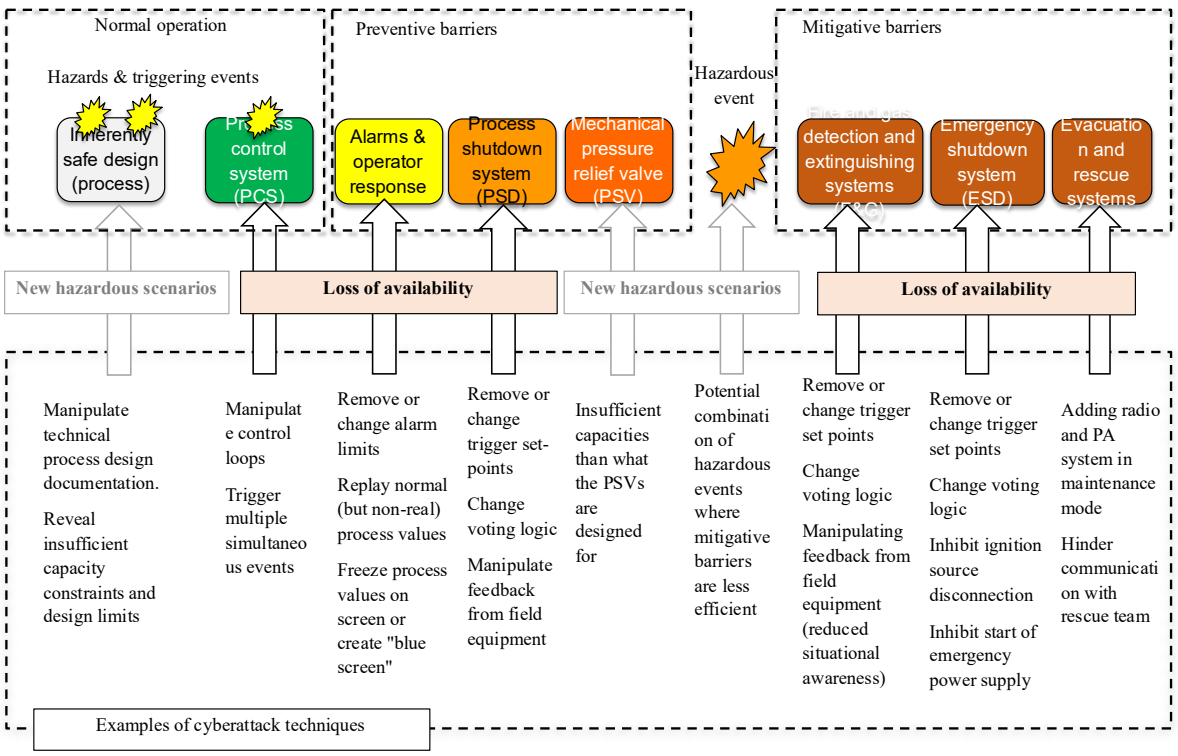


Fig. 11. Examples of how the loss of availability of OT systems may lead to loss of

The Evil bubbles attack (lab demonstration)

Using a lab setup on stage at the Black Hat conference in 2017, Maria Krotofil explained that a cyberattack can damage equipment, in this case, a pump. The attack was called "Evil Bubbles" because the attacker used knowledge of the pump's operating profile to induce cavitation. Cavitation occurs when vapor bubbles form in the pumped liquid and collapse, causing damage to pump components. A failed pump can cause production interruption or a safety-critical situation if it provides fire water or cooling water.

The experimental setup demonstrated that successful access to the control system allowed the attackers to increase the water temperature or decrease the water pressure. The change in parameters led to tiny bubbles in the water flow, which created massive shock waves that could eventually wear out the pumps' impeller blades. Krotofil emphasized that the same knowledge the attacker used could also be applied to detect attacks by identifying measurements (e.g., temperatures) that are unrealistic.

Source: YouTube video of the presentation by Maria Krotofil (last part is about the actual demo rig used to demonstrate – on the stage - an attack on a pump named ("Evil bubbles").

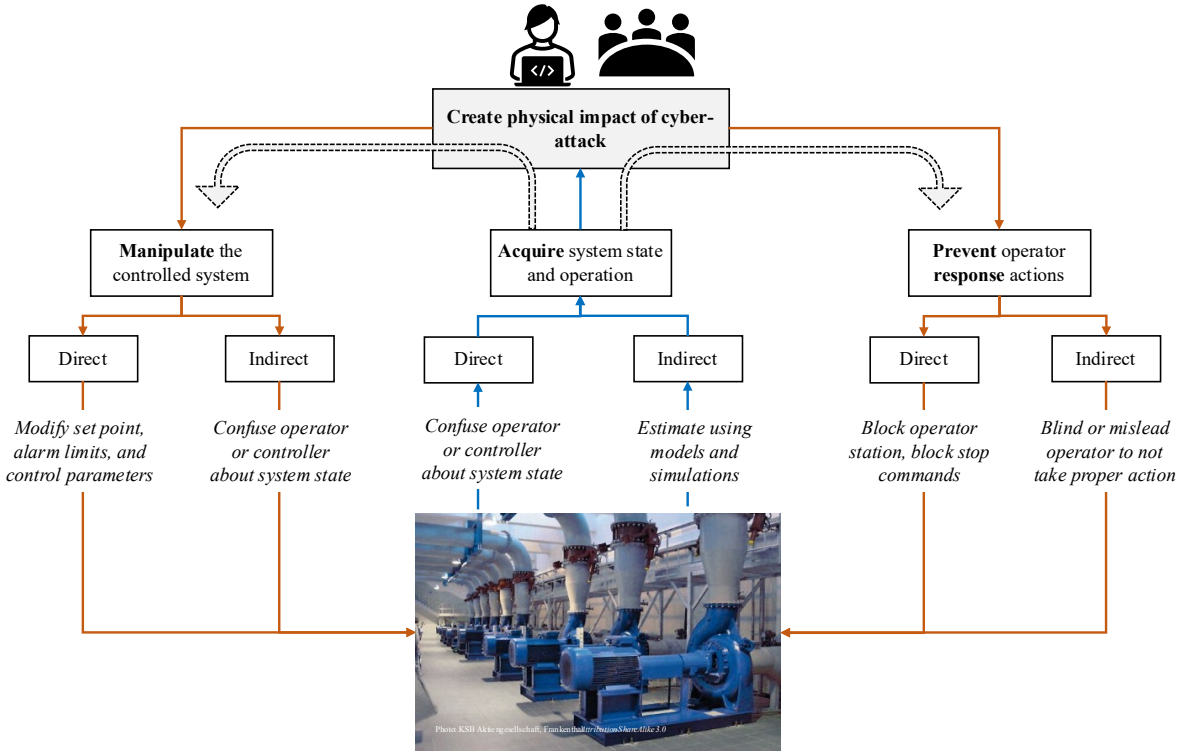


Fig. 12. Possible manipulations with physical impact (inspired by the talk of Maria Krotofil at the Black Hat conference in 2017)

Fig. 12 summarizes three strategies, often used in combination, which attackers may apply if the aim is to cause physical damage:

- Manipulate the controlled system
- Prevent operator response actions
- Capture the system feedback to get insights useful to support the two other strategies

Within each of the three strategies, you can choose a direct, indirect, or combination of these approaches.

11.5 Cybersecurity of the Purdue reference architecture

We have earlier (chapter 1 and chapter 2) introduced the Purdue reference architecture (or Purdue model) as a generic architecture of network layers at a larger facility, as shown in Fig. 13. The Purdue model is ideal for traditional networks in today's industrial facilities. Although there may be discrepancies in how the model is implemented, a form of network segregation and a clear distinction between OT and IT are common across all implementations.

The Purdue model was introduced primarily to visualize a typical network architecture for industrial control systems and their connections to other networks, and where various types of equipment are typically found. Purdue did not have cybersecurity in mind, and the original Purdue model did not mention a DMZ. As we will learn later, the Purdue model uses zones and conduits, some of which are separated by firewalls and one or more DMZs.

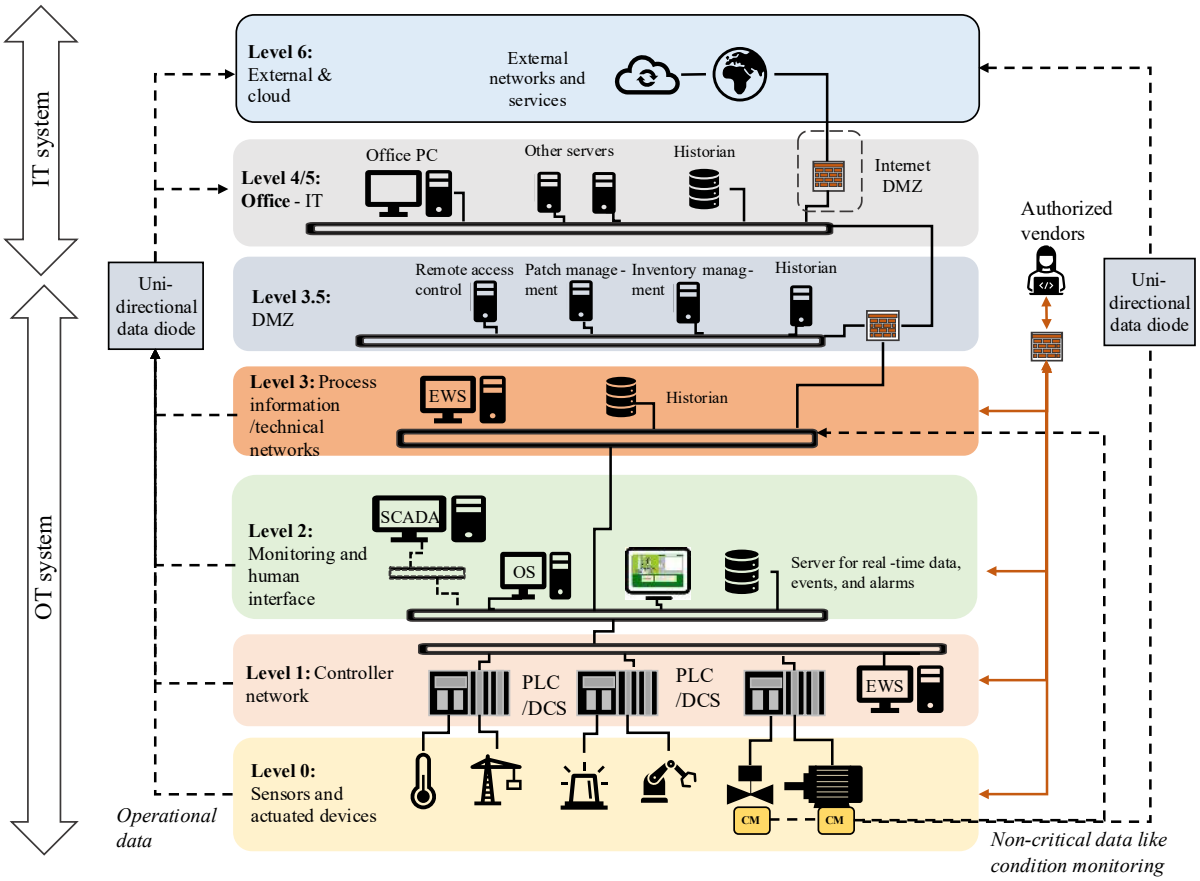


Fig. 13. The Purdue model and the OT system

Examples of network topologies following principles of the Purdue model are provided in the NIST Guide on OT Cybersecurity SP 800-82 (2023) guide on OT security and DNV RP G108 (2017) on the application of IEC 62443 for the oil and gas sector.

The Purdue model is sometimes challenged by those advocating a more flexible *zero-trust* architecture. Zero-trust architecture appears to have been introduced by Kindervag (2010). In such a network structure, it is assumed that all networks will be exposed to threats and that all connections must therefore be secured, for example, with authentication, encryption, and firewalls across all

communication channels. It, therefore, does not make sense to assume that protection is achieved through the segregation of the networks.

Zero-trust architecture is often mentioned in relation to Industry 4.0 technology platforms, where interoperability is highly emphasized. In practice, zero trust is also more of an ideal than a realistic goal. What can be envisaged is a mixture of zero-trust and Purdue, depending on what is considered appropriate and possible to achieve high enough (cyber) security.

	S4 is one of the world's largest and most advanced ICS Security / SCADA Security and Operations Technology conferences, and many of the talks and panel discussions are shared on YouTube. One of these events was a debate on the use of the Purdue model versus zero-trust architectures. See https://youtu.be/KfxPF9xjFrE. S4

11.6 Attackers targeting industrial cyberattacks

Several models in the literature explain the steps and approaches used in cyberattacks. We have chosen to focus on the two that are given the most attention in the industry, according to the author's knowledge:

- ICS cyber kill chain for ICS
- MITRE ATT&CK matrix

11.6.1 The ICS Cyber Kill Chain

The Industrial control system (ICS) Cyber Kill Chain Assante and Lee (2021) is an attack lifecycle published by SANS Institute, developed from lessons learnt from real attacks. The Sans Institute is an American *non-profit* company that, among other things, specializes in cybersecurity and cybersecurity training. Both authors of the report are quite famous in the field of cybersecurity. For example, Robert Lee founded Dragos, a US company with global reach, specializing in monitoring and analyzing industrial cyberattack activity and providing services and tools to help companies handle and prevent intrusions.

ICS Cyber Kill Chain splits the lifecycle into two main stages: Stage 1, focusing on initial compromise and foothold, first in IT and then in OT, and Stage 2, focusing on ICS attack development and execution, aiming for some OT disruption.

The steps within stage 1 and stage 2 are illustrated in Fig. 12 and may be explained in brief words as follows:

- **Stage 1:** Covers preparation and intrusion activities, covering the first IT side and then extending to the OT side. The subphases are:
    - Reconnaissance: The attacker gathers information about the target: systems, people, network layout, suppliers, and weaknesses.
    - Weaponize: The attacker prepares tools or malware tailored to the target (e.g., phishing kit, exploit, payload).
    - Targeting: The attacker chooses specific people, systems, or entry points to attack.
    - Delivery: The attacker delivers malicious content to the target (email, USB, VPN compromise, remote access, etc.).
    - Exploit: The attacker exploits one or more vulnerabilities to gain execution or access (software exploit, credential abuse, misconfiguration).
    - Install / Modify: The attacker installs malware, backdoors, remote tools, or modifies system settings.
    - Establish Command & Control (C2): The attacker creates a communication channel to remotely control the compromised system.

- Act (Internal Actions): The attacker performs internal activities: move laterally, harvest data, map the OT environment, and prepare for the next stage.

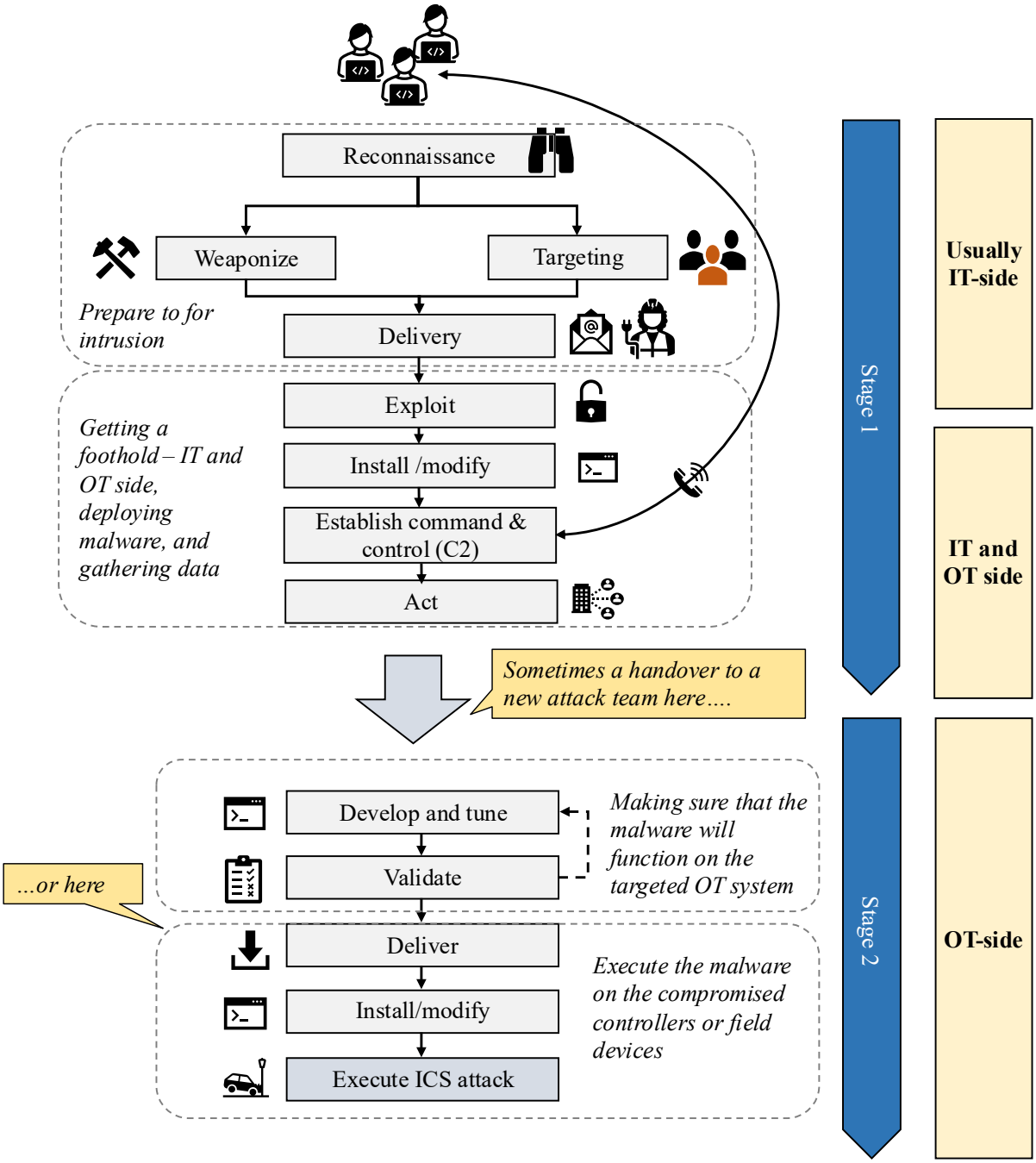


Fig. 14. ICS cyber kill chain stage 1 and stage 2 (Inspired by illustrations by Sans institute

- **Stage 2:** Covers attack development and execution activities on the OT side, such as:
  - Develop and Tune: The attacker adapts OT-tailored malware or tooling to the specific OT environment, based on data collected in Phase 1.
  - Validate: The attacker tests the malware to ensure that it works on a replica (for example, purchased hardware and software of the same type as the one to attack) or in the target system without triggering alarms. Choosing the latter means that the activity is attempted and hidden from being revealed at this stage.

- Deliver (OT-side): The attacker places the OT-malware onto the targeted hardware, such as a server, operator station, controller, or engineering workstation.
- Install / Modify: The attacker loads or alters controller logic or malware on the device (e.g., PLC), positioning the malicious changes so they are ready to run but without causing process impact.
- Execute ICS Attack: The attacker initiates the harmful actions enabled by the modified logic, such as changing setpoints, disabling safety functions, manipulating process values, starting/stopping equipment, or causing physical disruption.

Analyses of attacks and threat group capabilities have revealed that some specialize in stage 1 while others in stage 2, as different skills and resources are needed. Attackers may establish collaborations in which one group conducts stage 1 and hands off to the group responsible for stage 2.

11.6.2 MITRE ATT&CK Matrix for ICS

MITRE is an American not-for-profit organization with dual headquarters in Bedford, Massachusetts, and McLean in Virginia. MITRE has developed and is maintaining a database, Adversarial Tactics, Techniques, and Common Knowledge (ATTACK) organized into three types of matrices:

- MITRE ATT&CK Matrix for ICS
- MITRE ATT&CK Matrix for Enterprise
- MITRE ATT&CK Matrix for mobile devices

We are focusing on the MITRE Att&ck matrix for ICS. ICS stands for industrial control system and is MITRE's preferred term for OT systems located at levels 0-3 of the Purdue model.

An extract of the ATT&CK matrix for ICS accessed in 2024 is shown in Fig. 15. The matrix identifies 12 main tactics of the OT attack (stage 2 in the ICS cyber kill chain) in the top row. For each tactic (or column), a set of techniques (methods) is listed vertically.

The explanations that MITRE gives for the 12 techniques are:

- Initial access: The adversary is trying to get a foothold into the ICS environment.
- Execution: The adversary has gained a foothold and is now trying to run code or manipulate system functions, parameters, and data.
- Persistence: The adversary is trying to maintain its foothold in your ICS environment despite restarts, changed credentials, and other security measures that the company must take to avoid unauthorized access.
- Privilege escalation: The adversary is trying to gain higher-level permissions. These permissions could secure access to engineering workstations (EWS), which are essential for escalating the attack.
- Evasion: The adversary tries to avoid security defenses to avoid detection by automatic or manual systems monitoring unusual and unauthorized activities.
- Discovery: The adversary locates information to assess and identify more specific information about the systems' content that is the attack's goal, such as how the safety system controllers are configured and what protocols are being used.
- Lateral movement: The adversary is trying to move through the ICS environment, meaning that authorities are available to access the different controllers, servers, and remote support systems.
- Collection: The adversary is trying to gather data of interest and domain knowledge on the ICS environment to inform its goal. This tactic often overlaps with discovery, but it may also collect additional information deemed necessary.

- Command & control: The adversary tries to communicate and control the targeted systems from their premises (external to the IT and OT environment).
- Inhibit response function: This is the first of three tactics in which the attacker tries to cause physical harm. With the inhibit response function tactic, the adversary attempts to prevent safety, protection, quality assurance, and operator intervention functions from responding to failures, hazards, or unsafe states. In other words, they can manipulate or disable safety and alarm systems.
- Impair process control: The adversary is trying to manipulate and/ or disable the process control system to damage physical control processes. This may be performed in tandem with the inhibit response function.
- Impact: The adversary is trying to build further on the achievements of inhibiting the response function and impairing process control to cause confusion and a loss of ability to regain control. It involves manipulating, interrupting, or destroying ICS systems, data, and their surrounding environment. Examples include the manipulation and disabling of views and operator interfaces.

Complementary information found by clicking a tactic or technique makes this matrix so powerful. The links point to underlying web pages that provide more explanation of what they mean, references to actual attacks where they have been used, and examples of how they can be detected and prevented.

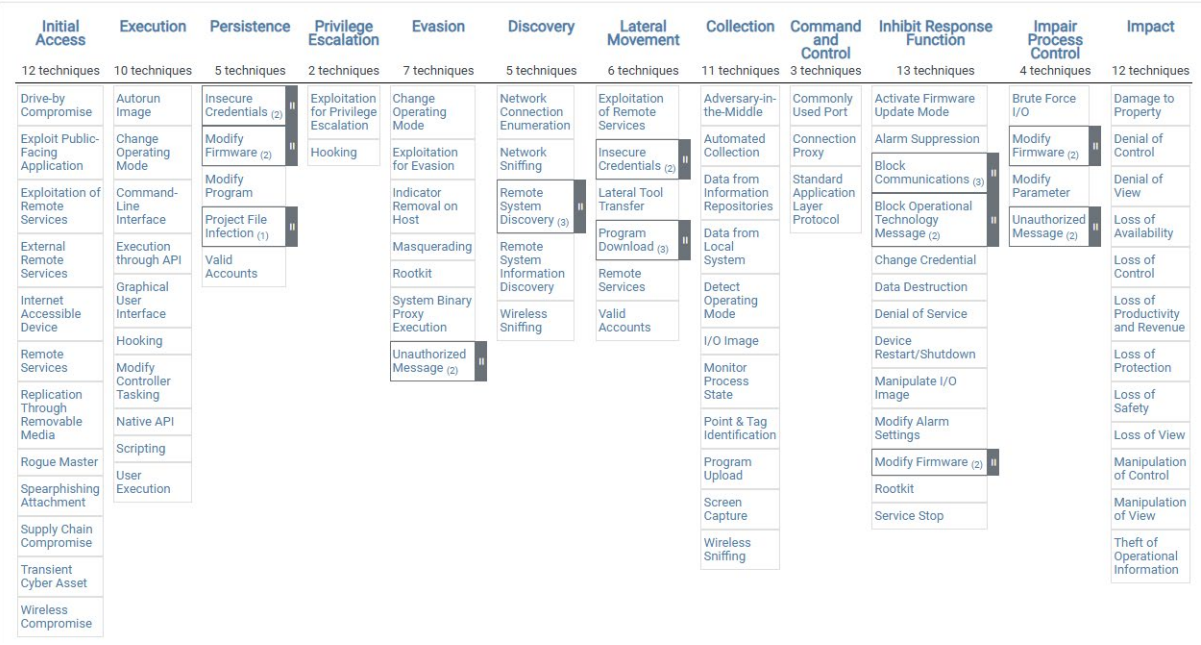


Fig. 15. Mitre Att&ck matrix (https://attack.mitre.org/matrices/ics/)

Within each of the 12 attack method categories, specific methods are listed below. For example, for the inhibit response function, there are 14 listed techniques, including alarm suppression, block serial COM, data destruction, and manipulating I/O image. Explanation and information about each technique are provided by following the links from the table. Examples of information provided for alarm suppression are:

- Alarm suppression is about not notifying operators of critical situations.
- The goals of adversaries may be to either prevent alarms from being raised or prevent alarms from being responded to.
- Methods of suppression may involve inhibiting the alarm so that it is not raised, modifying alarm displays and alarm logs, and modifying memory to present fixed (normal range) values instead of alarm conditions.

- The methods of alarm suppression may be applied to control servers, data historian servers, operator stations, process control systems, and safety-instrumented systems.
- Alarm suppression was applied in known attacks, such as the Ukraine electrical power station in 2016, the Triton/Trisis attack in 2017, and Stuxnet in 2010. It has also been part of ransomware attacks.
- Mitigative measures include a network allowlist to restrict applications that can run on a system, network segmentation to make it more difficult to access targeted systems, and alternative methods to report alarms in the event of communication failure.
- Detection methods include monitoring for loss of expected alarms and unexpected alarm discrepancies.

11.6.3 Impact on OT system network and devices (stage 2)

With adequate techniques and techniques deployed, the cyberattack violates the OT system (network and devices) in several ways, for example, by:

- Denial of Service (DoS): Attacks that disrupt expected device functionality, such as making an overwhelming number of requests to the targeted device.
- Brute force input/outputs: Attacks that modify I/O-signals, such as repeatedly changing a range of I/O point values or a single point value to manipulate a process function.
- Modify parameters: Attacks that involve modifying parameters in the control system or field devices.

Later, we will present the MITRE Att&ck matrix for ICS, which explains several attack tactics (goals) and techniques (measures). MITRE is a US non-profit organization that manages federally funded research and development centers.

11.6.3.1 Example 1: Attacking the alarm system

The MITRE Att&ck for ICS matrix has been used by Wetzels and Krotofil (2019) to explain how alarms can be suppressed (meaning not notified to the operator). The objective of the attack can be to prevent an outgoing alarm from being raised or an incoming alarm from being acted upon. The attacker needs to consider which alarms to manipulate or trigger to achieve the goal.

For example, by knowing which alarms result in a plant shutdown, the attacker can disable those that would ensure the plant's shutdown.

The ways alarms are set and sent, and where the attacker may decide to interact, are:

- Alarms sent by protocol message
- Alarm signals sent as individual input/output signals
- Alarm bit flagged by a software function block

An example of an attack strategy for suppressing an alarm, meaning removing the alarm from the list of active alarms, is to force the alarm status to be permanently false, regardless of the states of measurements that decide the alarm status. A change is made to the code in the controller memory so that the status of output is set to false. The authors also give examples of how to search for the relevant code instructions to modify.

11.6.3.2 Example 2: Attacking of I/O signals

The same authors Wetzels and Krotofil (2019) also provide an example of I/O manipulation explained with techniques from the ATT&CK matrix. They explain that I/O manipulation is influenced by how I/O image tables are populated and how the I/O is connected to the central processing unit.

The I/O values from the transmitter or to the control valve are manipulated by changing the content in the I/Os' own memory-mapped input/output register (MMIO). This register is a memory address that the hardware interprets for read and write operations. Before the values are read, the attacker may access the image tables that the CPU reads from and writes to.

The techniques mentioned for manipulating the MMIO register are:

- Memory breakpoint that adds stops or pauses so that the update of inputs or outputs is halted
- Patch instruction, which is a piece of code added to modify the content of the MMIO register
- Change in memory permissions to make a permanent change in existing code

The result of the manipulation is a seemingly legitimate reading or writing operation of values that have been manipulated.

11.7 Examples of cyber-attacks on OT systems

The first attacks on industrial facilities occurred as early as the 1990s. Fig. 16 shows an overview of cyber-attacks against industrial accidents developed by cyber.airbus.com.

Many of the listed events are followed up with several investigation reports. However, a complicating factor is that many attackers are incorporating measures to remove traces of the attack if they are discovered. Investigation reports may find different explanations, depending on their approach and insight.

Examples of trustworthy organizations that publish information about past cyberattacks on OT systems include:

- Dragos: A company created by the U.S. government and allies to monitor, investigate, and handle attacks targeting OT systems in the industry.
- MITRE: A non-profit American organization that operates several websites with helpful information about vulnerabilities, digital attack incidents, and follow-ups of these. The MITRE ATT&CK webpage provides examples of how methods were applied in real-world attacks.

Four attacks on OT systems are elaborated in more detail in the following.

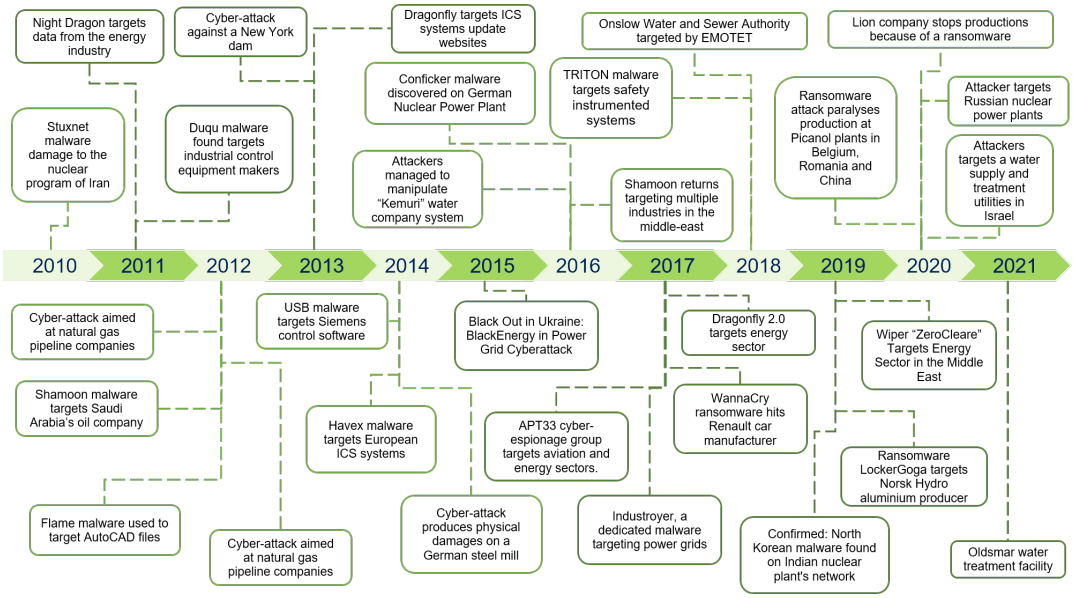


Fig. 16. Timeline for cyber-attacks involving OT (2010-2021) (cyber.airbus.com)

11.7.1 Stuxnet (2005 - 2010)

The Stuxnet cyberattack, discovered in 2010, served as a wake-up call for industry because it was the first specifically designed to inflict *physical* damage on process equipment and instrumentation. The attack targeted a uranium enrichment processing plant in Iran named Natanz, and the malware was named Stuxnet. The attack was developed over a few years and may have begun as early as 2005, as illustrated in Fig. 17.

The attack targeted two different systems at the Natanz facility: first, the cascade protection system (CPS) from around 2007, and later, with more "success," the centrifugal drive system (CDS) from around early 2009. The attack was revealed in June 2010, and due to its complexity, it is sometimes claimed that it was not fully understood until two years later.

The attack aimed to cause the failure of several of the (more than) 1,000 centrifuges (also referred to as pumps) without the plant owners noticing. The complexity of the Stuxnet attack took at least two years to fully understand, even for those with access to its details.

There are many articles and reports about Stuxnet. Dragos has covered Stuxnet in many of their analysis reports. The Langner group, which was involved in the investigation, published a report called "To kill a centrifuge" (The Langner Group, 2013), which explains the manipulations of the control systems in quite detail. For example, the enrichment system was quite complex. Due to sanctions, Iran did not have access to optimal technology for the purpose. Instead, they had to develop a process to use the centrifuges they already had access to. The downside was that this became a complex system comprising 18 cascade processes, each with 15 enrichment stages and 164 centrifuges. Each centrifuge had its own drive (motor) controlled by a Siemens S7-315 PLC.

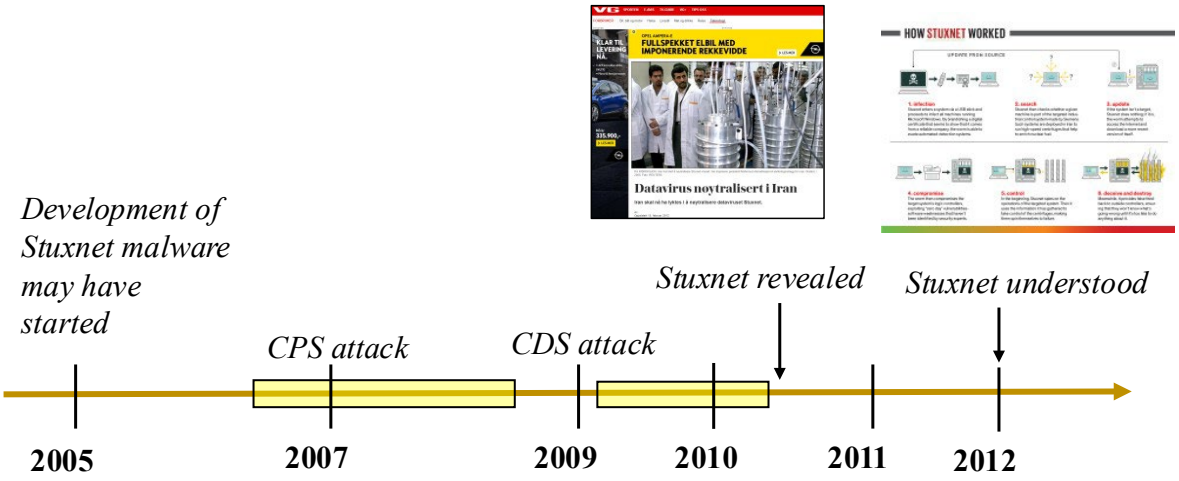


Fig. 17. Development of the Stuxnet attack

There were several operational challenges in operating these centrifuges, and minor deviations could cause them to fail.

The attackers were probably aware of this, and the facility relied on the overall cascade protection system *(CPS),* which used Siemens S7-417 controllers to control exhaust valves. An extract of the cascade processes may be illustrated as in Fig. 18 (under some uncertainty that the process is understood correctly, as the process details are not available).

The first part of the attack targeted the CPS system. An overpressure could be generated by changing the position of the exhaust valves installed with each enrichment stage of each cascade. The strategy to cause a slow, unnoticed pump failure was to close several centrifugal exhaust valves for a short period, increasing the pressure inside the centrifugal pumps. The attackers could monitor the pressure and reopen the valve after a short period. As this system was a pump-protection system, a late reopening of the valves could trigger a shutdown, attracting unwanted attention.

The second version, therefore, targeted the process control system directly through the centrifuge drive system (CDS). Access to the CDS system would enable direct control of the centrifuges via frequency converters. This system utilized S7-315 controllers. With careful precision, one could increase the speed from 63,000 rotations per minute (RPM) to 84,600 RPM in 15 minutes, which would be an ideal increase to accelerate the wear without causing a simultaneous breakdown of all centrifuges. Sudden stops (120 RPM) were also added to increase the load. To prevent the CPS system from triggering a shutdown, the input signals were manipulated to indicate normal conditions.

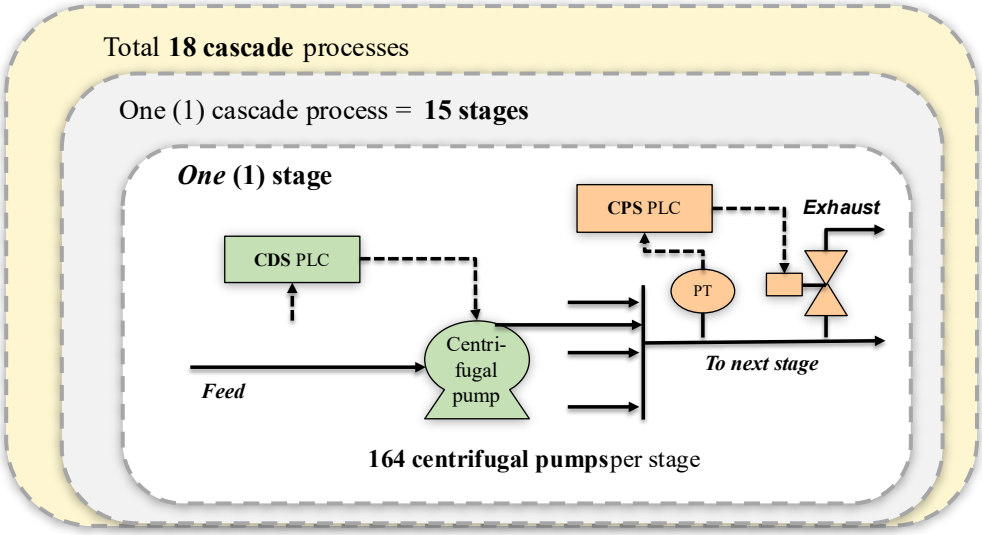


Fig. 18. Centrifugal drive system (CDS) and centrifuge protection system (CPS)

The legitimate program code (including the outputs) was suspended during both attacks while the malware was running. Because the SCADA system only obtained measurement values from the legitimate program, the operator monitors were not updated with information about the abnormal operation of the centrifuges.

Fig. 19 illustrates how the attacks led to physical damage. While the first attack indirectly caused centrifuge damage by changing the position of the isolation and exhaust valves, the second attack directly modified the rotor drives' speed (for shorter periods), leading to a critical (damaging) rotor speed.

The Langner Group (2013) pointed out that many of the widely used cybersecurity measures could not have prevented Stuxnet:

- The anti-virus would most likely not have been effective. The malware was indistinguishable from ordinary (legitimate) programs because it used forged certificates.
- Network segregation, data diodes, and air gaps would not have prevented the attack, as it went through a contractor who had direct access to the OT system and carried infected USB chips and mobile devices.
- Intrusion detection systems (IDS) would most likely be unable to detect or prevent the attack. At that time, IDS systems were primarily rule-based, meaning they could only detect known attack methods. In this case, the attack was designed precisely to avoid this. At this time, no IDS could do more advanced analyses of abnormal traffic.
- One also questions whether patching, i.e., security updates, would have been effective. Firstly, it often takes a long time from the moment suppliers publish safety updates to the moment the plant owner has finished testing them in collaboration with other systems before installing them. Moreover, creating a security patch that captures specially designed attacks is difficult.

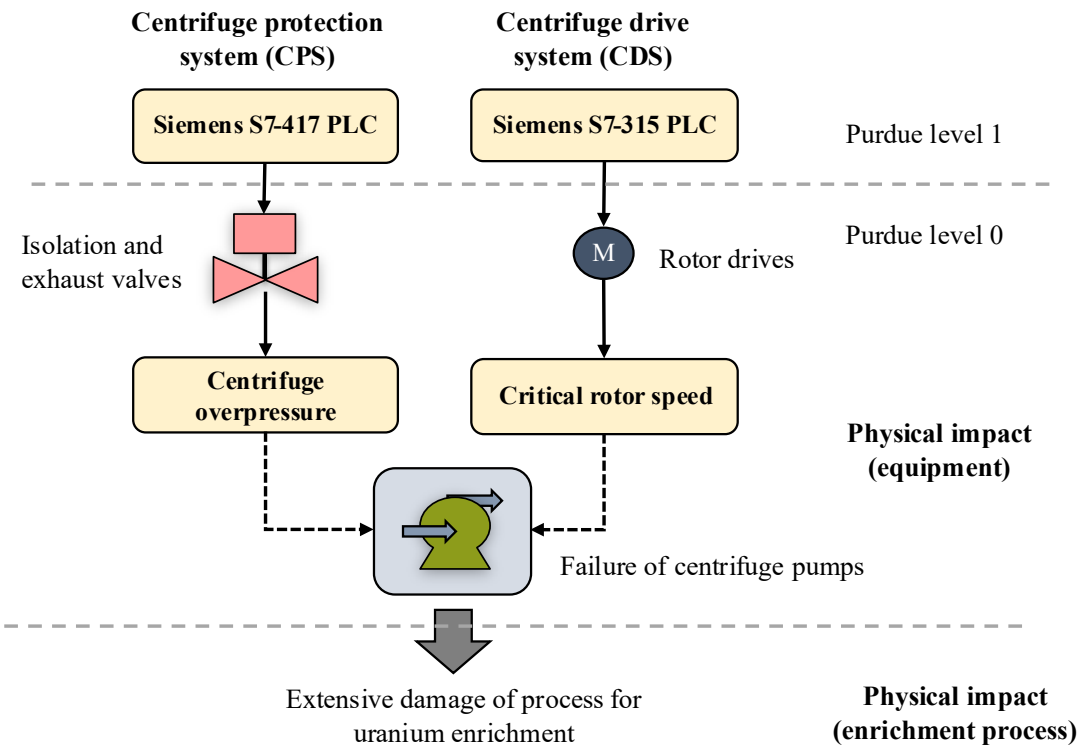


Fig. 19. The two attacks that led to centrifugal damage.

A more detailed explanation of the attackers' approach is provided by Makrakis et al. (2021) supported by their illustration in Fig. 20. The following steps were highlighted:

1. Initial access to the facility's IT systems was gained by having a binary (executable files) of the malware with compromised certificates. Hence, the files, when sent to people working at the plant, seemed to be safe (and secure).
2. The Stuxnet malware exploited several zero-day vulnerabilities to spread throughout the system, gaining necessary access and insight to systems at the plant. Because several OT systems, such as the PCS 7 SCADA system, OPC servers, and WinCC workstations for operators, were accessible from the IT system (there was no DMZ), these systems were also infected.
3. The Stuxnet malware also allowed the establishment of a hidden link to the attackers' premises outside the plant. Through this connection, they established a command-and-control (C2) capability that they could also use to push files down to the OT system and receive feedback after the engineering workstation inside the OT system had been infected (see 4).
4. It was important for the attackers to infect and control the engineering workstation at the plant, which could modify the control system and download new versions on the Siemens controllers. Unfortunately (for the attackers), this one was not connected to the internet. It was therefore necessary to have someone install the malware on this computer to gain control over it. By infecting sub-suppliers, such as service engineers, with Stuxnet malware, the malware was carried to the plant EWS via USB flash drives used by these service engineers during work at the plant.
5. Once installed via USB drive, the malware was installed, and attackers got access to control the EWS. The Stuxnet malware was then used to modify the control logic to run short sequences to degrade the centrifuges while replaying the normal operational situation on the operator screen.

6. Before initiating the two versions of the attack, they could monitor the Profibus connection to observe and record data about regular operation. After initiating the attack, they could download maloperation sequences to CPS or CDS systems and monitor the responses from their external premises.

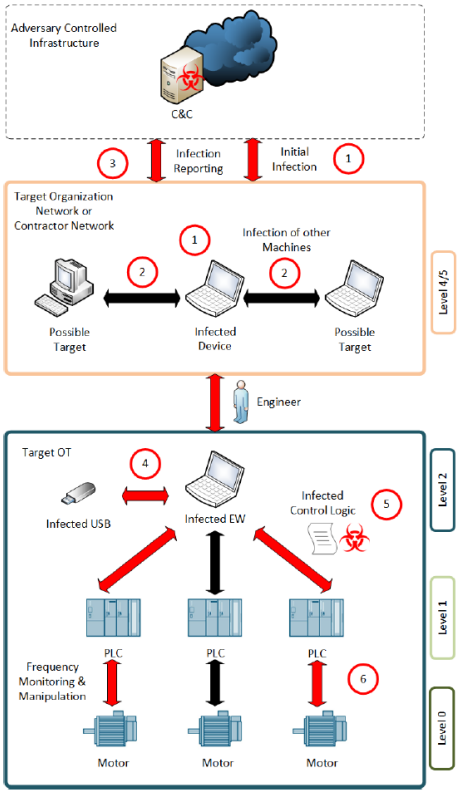


Fig. 20. STUXNET explained with ICS cyber kill chain (Makrakis et al., 2021)

Complementary information about the attack can also be found in the report by Assante and Lee (2021).

11.7.2 Triton/Trisis/Hatman (2017)

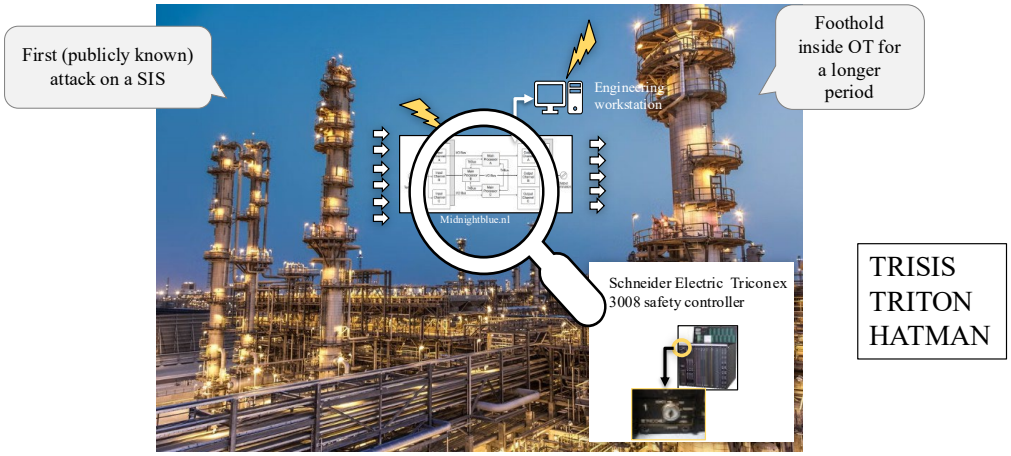
The cyber-attack on the petrochemical plant in Saudi Arabia is known by three different names: Triton, Trisis, and Hatman. The most serious aspect of this attack was its targeting of the emergency shutdown system (ESD), a type of safety-instrumented system (SIS). The description below is based on sources such as Dragos (2017b), Makrakis et al. (2021) and the website of the company Mandiant webpage (2022) (before 2021, known as FireEye). Several sources suggest that the attack was carried out by the Russian Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM).

The malware was the first to be specifically designed to modify a type of safety controller called Triconex, delivered by Schneider Electric. Triconex safety controllers operated the plant's emergency shutdown system and were provided by Schneider Electric. The malware and attack also involved manipulating the process control system, suggesting the goal was to first create a dangerous process situation and, at the same time, to render the safety system unable to act upon this event.

Until the incident occurred, these controllers had (reportedly) operated 600 million hours without any serious incidents. However, in 2017, the facility experienced several unexplained shutdowns, and it was eventually suspected that a cyberattack may have caused them. The company FireEye was engaged in August 2017 to do investigations, and the malware they discovered was named Triton.

While FireEye was working at the plant, Dragos accidentally discovered the same malware through its surveillance systems. At this time, FireEye's work was not officially known, and Dragos named the

malware Trisis. Also, this attack used the engineering station in the OT system to modify the security controllers' programs. The attackers exploited the fact that someone had left the switch shown in Fig. 21 in the "program" position, which allows downloading a new version of the program running on the controllers. Luckily, the revisions made to the program were not entirely successful. Instead of inhibiting important ESD functions, the ESD system detected a fault and shut down the plant. Later, when the US industrial control system cyber emergency response team (ICS-CERT, now integrated into the US Cybersecurity Infrastructure Security Agency [CISA]) published a report on this malware, they introduced it by its third name, Hatman.



SIS: Safety instrumented system. ESD: Emergency shutdown

Fig. 21. The Triconex compromised controllers.

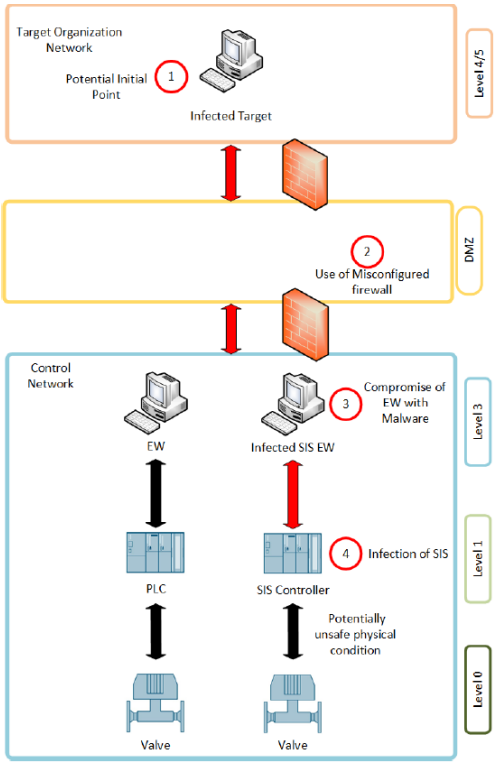


Fig. 22. Cyber kill chain applied to Trisis/Triton (Makrakis, 2021)

Makrakis et al. (2021) has explained the Trisis/Triton attack as shown in Fig. 22. A short summary of the attack, with more details in the paper, is as follows:

1. The attack was made possible by gaining access to the IT network with the malware. Some sources suggest that access was first made in 2014.
2. The network included a DMZ; however, a misconfigured firewall gave a foothold to an SIS EWS, where they delivered the malware
3. The EWS was compromised with malware to communicate with SIS controllers, involving reverse engineering of the TriStation protocol. The attackers exploited a zero-day vulnerability, for which a patch had been made available one year earlier but was not yet installed at the plants.
4. The attackers were able to install the malware consisting of a modified control logic onto the controllers by counting on the key switch being in "program mode". Later, they could modify the firmware so that it would not be dependent on the position of this switch. Fortunately, the malware installation went wrong, and the SIS controllers. Zero-day vulnerabilities associated with the Triconex controllers were exploited.

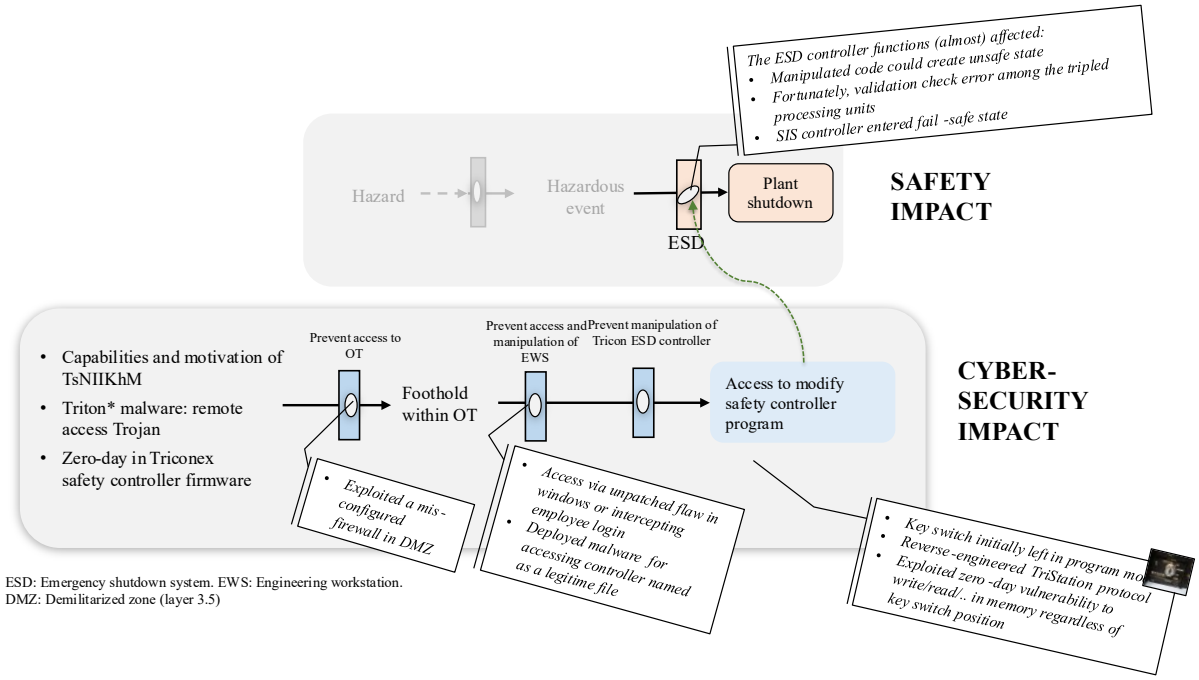


Fig. 23. Illustrating the relationship between cybersecurity and safety impacts, with Trisis/Triton as example

The authors point to a Dragos report (Dragos, 2017b) to further detail the capabilities of the Triton/Trisis malware: (a) shutdown of the process through operational uncertainty, (b) forcing the SIS controller to an unsafe state by maliciously altering the SIS logic, and (c) removing all the fail-safes that exist to prevent damage, thus creating an unsafe physical condition. Fortunately, an implementation error by the attackers caused a fault, which the controllers responded to by shutting down the facility.

The attack on the ESD system was an eye-opener about how a cyberattack could lead to a major accident. For this reason, it is relevant to model the barriers on the cybersecurity and safety sides, and to examine how the exploitation of vulnerabilities on the cybersecurity side could lead to degradation, manipulation, or the full loss of safety barriers for major accident prevention. Such a model can be made generic, showing potential impacts from cybersecurity on safety, or specific, as is illustrated in Fig. 23.

11.7.3 BlackEnergy3 (2015) and Industroyer (2016)

In 2015 and 2016, Ukraine faced two extensive cyberattacks on its power distribution network. The 2015 attacks, named BlackEnergy3, and the 2016 attacks, named Industroyer, are described in numerous reports and articles, for example, reports by Dragos (Dragos, 2017a, 2019) and the article

with references by Makrakis et al. (2021). The book titled Sandworm (Greenberg, 2019) provides good insight into the attacks and is named after the attacker group's name.

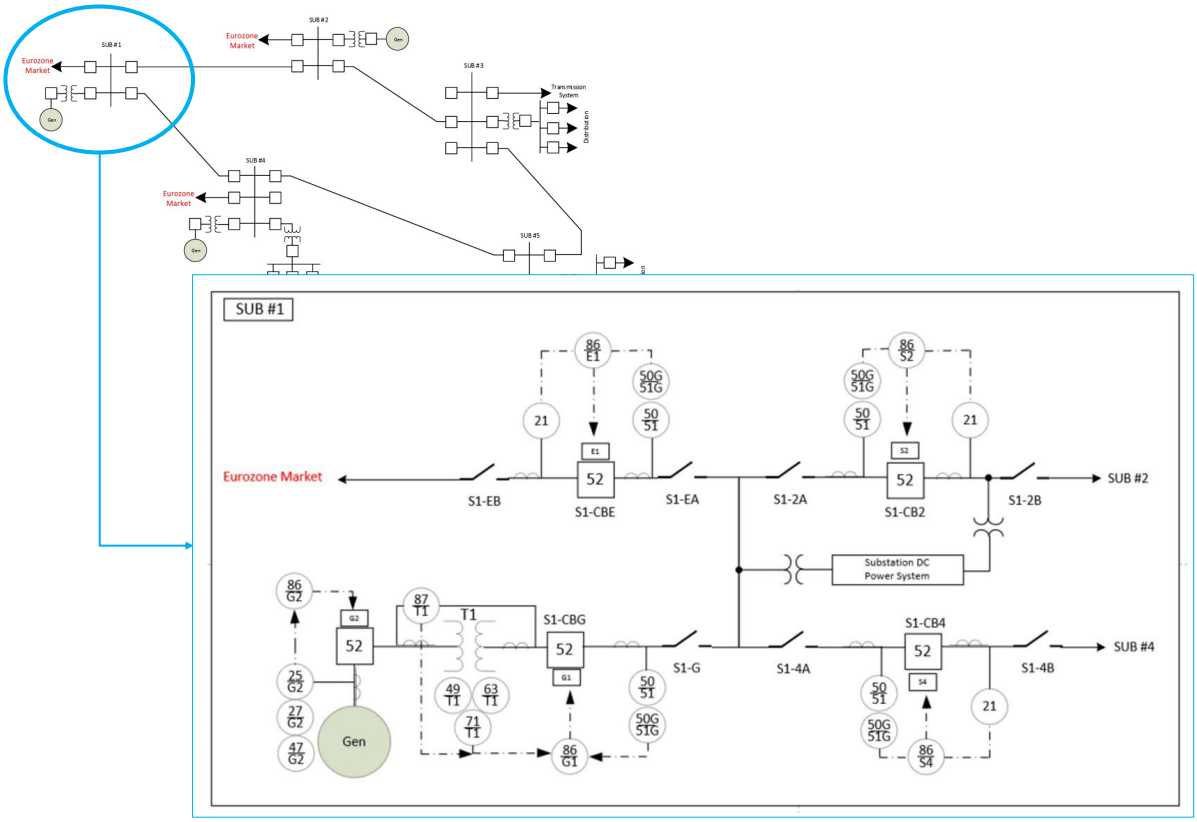


Fig. 24. Power transmission grid with substations and distribution (Gellner and St. Michael (2020)

Although they occurred in two consecutive years (2015 and 2016), the two attacks had different names because the malware was different. Later, in 2022, there was a similar attack attempt, but fortunately, it was stopped.

Being familiar with power transmission and distribution networks is beneficial to understanding the attack better. Unfortunately, we do not have the details available to explain this part of the affected systems in Ukraine. However, a report by Gellner and St. Michel (2020) published by OSTI on a synthetic attack on a power outage of a power substation in a synthetic country called Baltavia, gives some helpful explanations, and a couple of its graphical illustrations shown in Fig. 24.

Power transmission involves distributing high-voltage power over long distances to substations, and the network of substations is often designed to reroute power via an alternative route upon the loss/failure of a transmission line. Within substations, connections to distribution networks supply power to consumers (industry, public services, individual households). The 2015 attack (BlackEnergy3) targeted several substations simultaneously, whereas the 2016 attack (Industroyer) targeted only one. Despite this, Industroyer was found to be the most severe, as it was more intelligent (advanced) and potentially had more severe damaging consequences.

BlackEnergy 3 (2015)

In December 2015, Ukraine was hit by a cyberattack that caused short-term power outages affecting up to 255,000 customers in Ivano-Frankivsk, Chernivtsi, and Kyiv. The attack was carried out by a group known as Sandworm, and the malware was named BlackEnergy 3. In this attack, the attackers accessed the supervisory control and data acquisition (SCADA) and distribution management system (DMS). In this way, the attackers were able to send commands to open circuit breakers installed at around 53

substations. At the same time, the malware disrupted network traffic by initiating a DoS attack on the communication link, preventing the operators from resetting it. The length of the power outage corresponded to the time it took for the manual operators to reset the breakers manually. This attack had severe, but luckily not permanent, consequences, and is nevertheless described as less advanced than the next one, which came in 2016.

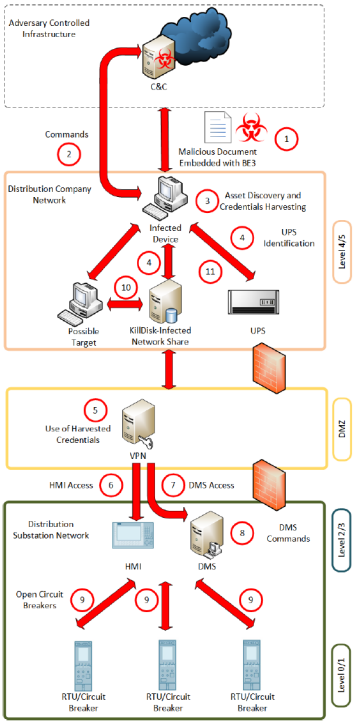


Fig. 25. BlackEnergy3 attack (Makrakis et al, 2021)

Makrakis et al. (2021) have developed a graphical description of the steps of the attacks, as shown in Fig. 25. A simplified description of the steps numbered in the illustration is:

1. The malware was inserted and delivered via MS Word documents embedded with malicious macros.
2. By running these macros (done by someone inside the plant), a command and control (C&C) was established with encryption.
3. During the first period, the attackers reconnoitered the systems to gain information about the IT and OT systems and environments. Several tools were implemented in the malware to steal credentials, perform network discovery and scans, provide remote access, capture screenshots, and log keystrokes.
4. Devices accessible within the IT system for power supply redundancy, communication, and data servers were discovered and reconfigured so that the attackers could disconnect them when they wanted. A KillDisk component was also installed to be triggered during the attack, making restoration difficult for the operators.
5. Stolen credentials were used to provide access to OT/ICS via VPN connection.
6. Attackers used a remote access tool (RAT) to connect to the operator stations (HMI)
7. The attackers then managed to lock operators out of their workstations so they could not perform any action.
8. Attackers then issued commands directly to the distribution management system (DMS) server using the VPN connection for controlling circuit breakers and what was shown on the operator screens.

9. The commands for opening the circuit breakers were sent, causing a power outage in at least 57 substations.
10. The damage was extended by pushing a malicious firmware update to corrupt some serial (Fieldbus)-to-ethernet adapters, preventing operators from monitoring data from the control systems. The KillDisk was also executed to wipe out all content on the operators' PCs/workstations.
11. The connection for the backup power supply (UPS) was disabled from the data and communication servers, causing more confusion to the operators. Attackers further confused the situation by initiating a DoS attack against the telephone center.

The attack relied on a remote connection for the attackers to issue all commands. After the attack, all operations were switched to manual mode to restore. This operation took approximately 6 hours.

Industroyer/Crash Override (2016)

Almost exactly a year after the 2015 attack, another cyberattack occurred at a specific power distribution substation in December 2016. The attack later became known by the following two names: Industroyer and Crash Override. The attack was less extensive than in 2015 when it targeted a limited part of the distribution network.

Nevertheless, it is described as more serious because it was designed more "intelligently" with greater capacity and the ability to strike broadly at power distribution facilities. For example, the malware could issue commands at specific times without requiring remote communication with the attackers. Furthermore, analysis of the malware revealed the capability to operate the protective relays. These relays are critical for protecting the distribution lines from damage caused by short circuits, excessive voltages, and other abnormal events detected in the network, and for operating the circuit breakers and alarming the operation center, as shown in Fig. 26 (left side). While system breakers disconnect and reconnect power lines as part of regular operation, protective relays are safety devices that act independently upon detected abnormal events to reduce the possibility of damage to lines and connected equipment.

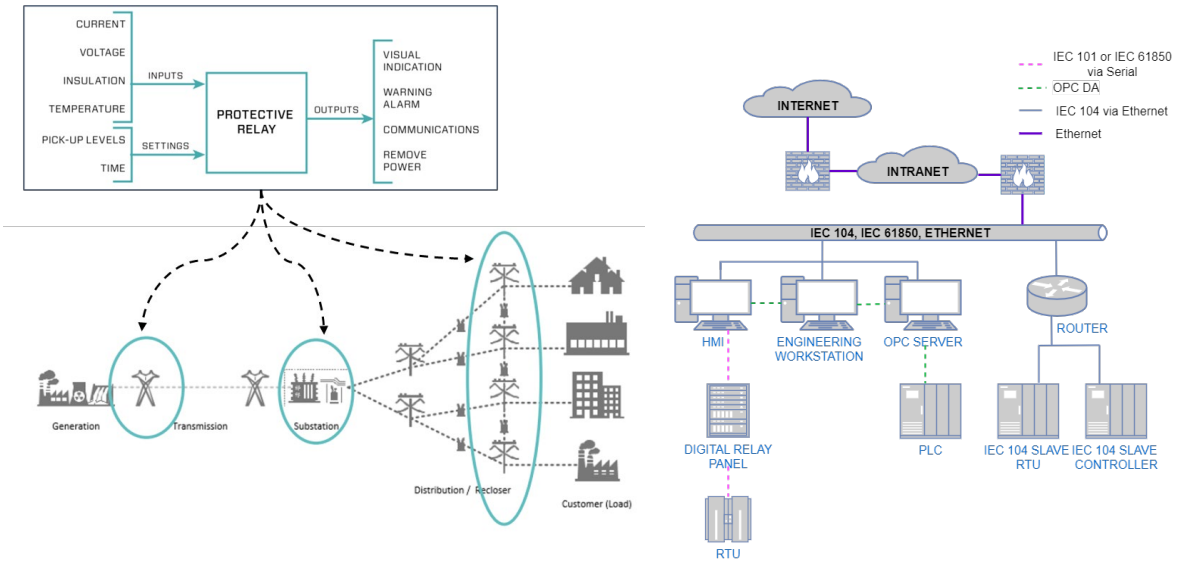


Fig. 26. Left: Protective relay function and location (adapted from Dragos, 2019). Right: Simplified network identifying involved technologies (Haver, 2022)

The reports from Dragos (Dragos, 2017a, 2019) and the article Makrakis et al. (2021) provide deeper insight into these two attacks. For example, Dragos (2019) developed illustrations shown in Fig. 26 about the location and role of the protective relays.

The protective relays targeted in the power distribution plant were reached by adding malicious code to messages communicated over open/standardized protocols, as illustrated by Haver (2022) in Fig. 26 (right side).

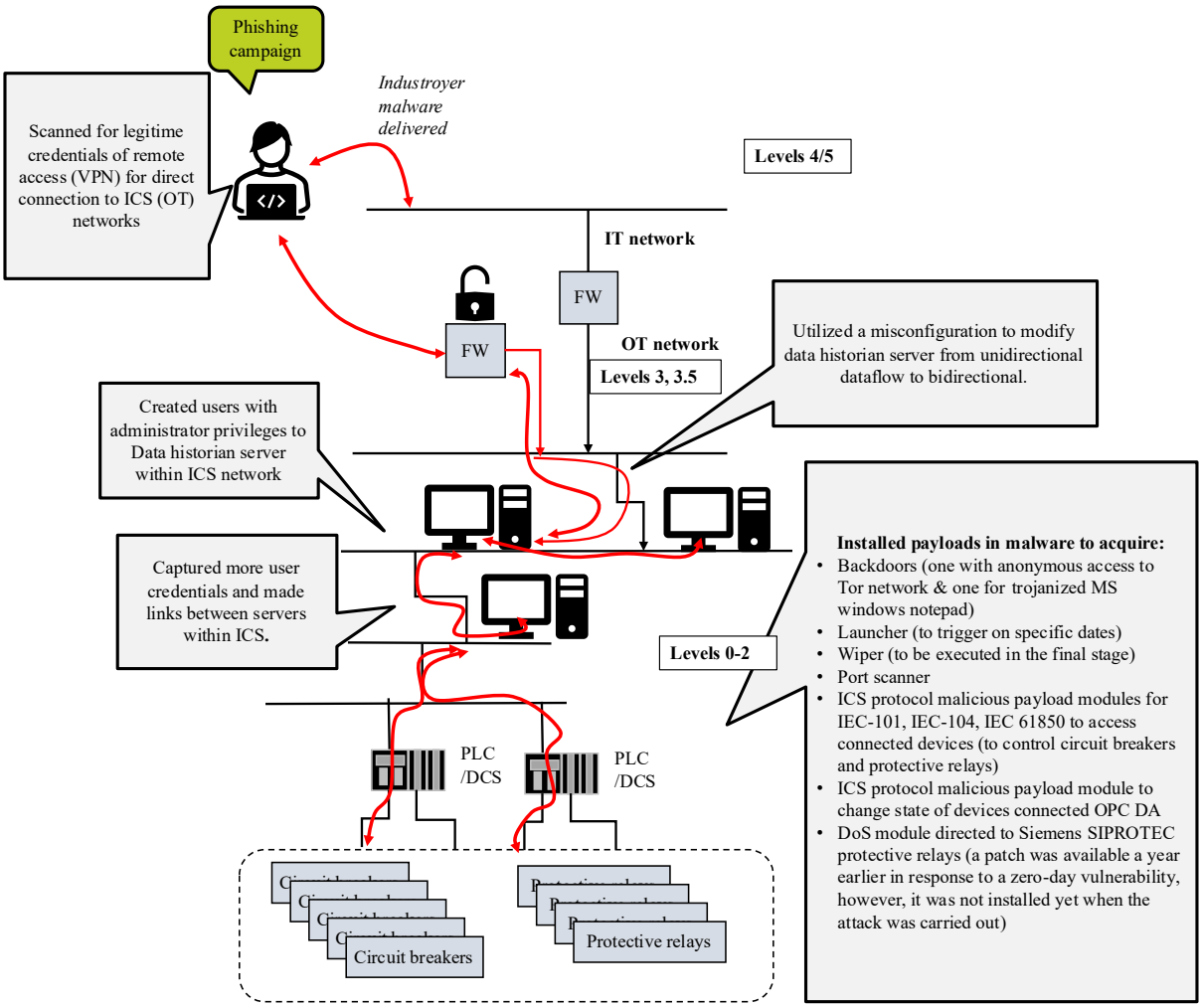


Fig. 27. Summarizing the Industroyer attack

Some highlights made by Dragos (2019) are:

- Unlike in 2015, the attack was designed to be more "vendor independent" when attacking the SCADA system monitoring and controlling the distribution system. This means that the attack could affect equipment from several suppliers. Initially, an OPC protocol was used to obtain information on connected equipment and operator stations. The operator stations provide details of how the network is structured via images at different levels of detail.
- In addition, the malware was able to change commands in three different protocols commonly in this type of facility: IEC 61850, IEEE 104, and IEEE 101. In this way, one could send a command to electronic system breakers to open and thus disconnect the power.
- During the attack, after the system breakers were opened, the malware continuously sent messages over the network to prevent all other traffic, a type of event we call Denial of Service (DoS). The DoS attack prevented the protective relays from working as intended. The DoS

attack prevented the operators from sending commands to open or close the system breakers and protective relays.

- During the attack, possibly because of the DoS, the malware removed the visibility on the operator screen about what was going on, leading to loss of view and control.
- In retrospect, it was revealed that the malware allowed several types of manipulation of the breakers and protective relays: for example, it could be left in an intermediate position – neither open nor closed, which could create dangerous and harmful situations in the network, such as fires.
- Finally, the malware deployed a wiper module to impede recovery and delete configurations and related files that were necessary to restore the infected systems.

Fig. 27 attempts to summarize the attack according to the steps explained in Makrakis et al. (2021).

There are probably several ways to explain the Industroyer attack, depending on the level of detail.

Fig. 28. The Hydro cyberattacks.

11.7.4 Hydro ransomware attack (2019)

On March 19, 2019, Hydro was the subject of a ransomware attack called LockerGoga. Handwritten notices on the front doors greeted employees entering the workplace, as all computers and networks had been shut down to prevent further spread. Examples of how to spread the information to employees are seen on the right-hand side of Fig. 28. On the left is an extract from the Hydro webpage and from foreign newspapers' coverage of the attack.

The attackers encrypted all files containing prescriptions (i.e., recipes for products to be produced) and orders needed to operate the production plants automatically. The OT system was, therefore, indirectly (and not directly) impacted by the attack. Operators with experience operating the plants manually were able to restart some production, but at a lower capacity. Who was behind was not known at the time of writing, but the motivation seemed to be money, as a ransom fee was requested to restore the systems.

More information about this attack is found in a report from Dragos (2020).

11.7.5 Oldsmar water distribution system in Florida (2021)

In February 2021, a water treatment plant in Oldsmar, Florida, was the subject of a cyberattack. The attacker accessed the OT system via a poorly secured remote access mechanism. The attack could have been easily prevented with more awareness of cybersecurity measures. The attack is mentioned for its physical impact. The attacker gained access to increase the dosage of chemicals (sodium hydroxide) used for water purification by one hundred (100) times by changing the setting of the dosing pump. Such concentration could, over time, poison the drinking water. This increase was possible because the pump's capacity was much higher than what was needed.

Fortunately, the on-duty operator discovered the attack. The operator observed that the mouse was moving on the screen and making changes to the control system settings. The operator was, therefore, able to stop the attack and restore settings before the pH alarm detected a concentration outside allowed limits. In this case, one may question what would happen if there were no operator on duty this time and if the attacker could also disconnect the pH alarm or change its settings.

Another lesson learned from this event was that sizing physical equipment is part of cyber defense. The chemical dosing had a far larger (design) capacity than needed. A risk assessment could have revealed the potential severity of having an oversized pump. However, we may suspect that cyberattacks were not considered in the risk assessment, and the scenario may have been disregarded as having very low risk. Fortunately, the attack was quickly revealed, and by chance, the chemical dosing pump was stopped, so it did not have serious consequences.

You can read more about the events in reports from DoE (2021) and Dragos (2022).

11.7.6 Using PLC as a platform for executing attacks

An interesting case is how a PLC can be attacked and weaponized to carry out the attack itself. An experiment from a research lab in which PLCs were exposed to the internet was presented by Sharon Briznov at the DEFCON conference.

	DEF CON 30 - Sharon Brizinov - Evil PLC Attacks - Weaponizing PLCs See video at YouTube.

11.7.7 Generalizing the lessons learned

We may generalize some lessons learned about how attacks are carried out. We start by considering the network architecture in Fig. 29, identifying the following steps:

1. Get inside: There are several ways to get inside the target networks: An attacker could use various social engineering techniques, such as phishing, to reach a person in the organization with relevant access to the OT system. For example, to steal an engineer's credentials authorized to work with OT-related systems, exploit a zero-day vulnerability that exposes an OT device to the internet, and access equipment physically via USB with help from an insider or someone who has been compromised without knowing it. Intrusions can also occur through the supply chain and are referred to as supply chain attacks. Not shown in the illustration, but another way to attack a system is to introduce a hardware trojan (a piece of hardware with software) into a sub-component or subsystem delivered by a sub-supplier. Such an intrusion may affect all products that use the infected component type.
2. Get a foothold: The malware creates a channel out to the attacker, for example, via a cloud solution, and achieves the C2 capabilities. The attacker can use various methods to obtain the same permissions the engineer has, such as by connecting to a server in the DMZ.

   Assuming the attacker has obtained permission from the server in the DMZ, the attacker extends the existing C2 to include a new direct channel to the cloud solution, now within the OT system.
3. From the DMZ, the attacker can try to reach other servers and equipment on the lower layers of the OT system. We can assume that the relevant targets are to gain access to multiple servers, operator stations, and engineering workstations (EWS).
4. If the goal is to manipulate controls in process control and safety systems, gaining access to the EWS is the natural next goal.
5. Once allowed to access the EWS, the attacker can perform modifications and install malware without making any modifications to the EWS itself. From the EWS, it is possible to upload the program running on the controllers without disrupting production, implement changes, and

download a new, modified version. The most vulnerable stage from the attacker's viewpoint is downloading, which may require additional permissions. Some controllers also require that a physical switch be set to "program" mode to prevent unscheduled or accidental downloads while in "run" mode. However, there are examples in which this physical switch has been bypassed through software manipulation.

6. Once installed, the manipulated program can create unforeseen scenarios and difficult-to-explain performance drifts. The impacts can be severe to safety and production, as the manipulated programs can cause critical equipment, such as power generators and turbines, to fail.

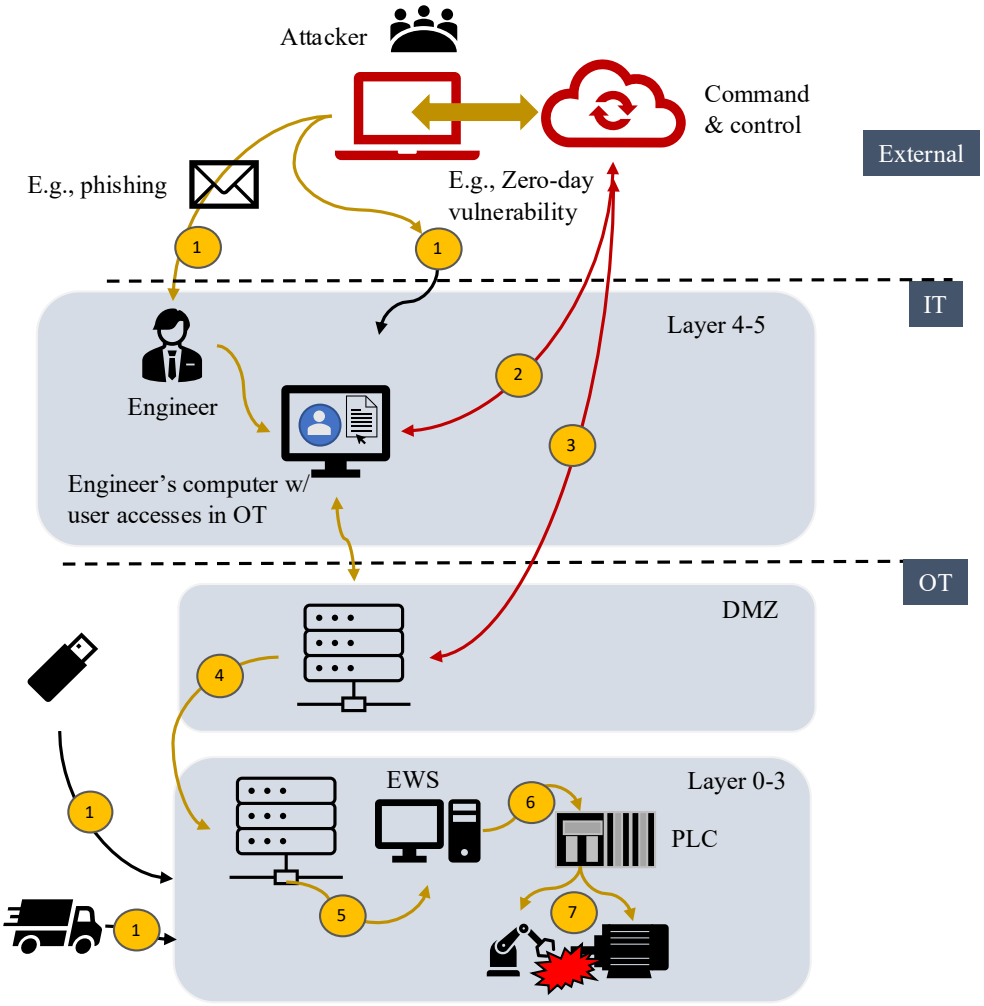


Fig. 29. Typical steps in an OT attack (adapted from DNV)

We may also generalize some lessons learned about the scenarios attackers may plan for if their goal is to cause physical damage. To illustrate, we use Fig. 30 showing a two-stage separation process. The first vessel separates fluids and gases at a higher pressure, and the second (downstream) vessel separates them at a lower pressure.

- It is assumed that hydrocarbons flow at a high pressure into the first stage separator, where gas is separated from oil and water.
- In the second-stage separator, the pressure is reduced to separate more gas. It is important to note that the second-stage separator is designed to tolerate a lower pressure rating than the first-stage separator.

- Both vessels have a mechanical pressure relief valve (PSV) that, when opened, can route gas to the flare if the pressure in the tanks exceeds the PSV setpoints.
- The process control system (PCS) controls the level and pressure, and a process shutdown system (PSD) will close a set of valves if the level or pressure exceeds PSD setpoints. Because the 2nd-stage separator operates at lower pressures, it is designed to withstand lower pressures than the 1st-stage separator.

The traditional design philosophy for such processes is to ensure that control and safety systems can manage the process under foreseeable normal and abnormal operational situations, excluding deliberate and adversary acts. An attacker may therefore plan for a scenario that is not possible without manipulation, as such a scenario would fall outside the design envelope.

Fig. 30 shows (by numbers) a set of manipulations that the system is not designed to handle:

1. The control valve in the 1st stage separator is forced fully open.
2. The control valve in the gas outlet is forced to close, increasing the pressure and level in the first-stage separator.
3. The outlet valves of the second-stage separator are forced to close.
4. The shutdown valves in and out of the first-stage separator are forced into open position, reducing the separator's pressure and level. In contrast, the pressure and level in the second-stage separator increase quickly.
5. The control valve in the line from the first to the second stage separator is forced open, and the pressure and level continue to increase in the second stage separator beyond what it is designed for.

The manipulations are carried out so that the setpoint for opening the pressure relief valve (PSV) for the first-stage separator is not reached. Instead, they intend to wait for the pressure safety valve (PSV) of the second stage separator to exceed its setpoint, and this is when the dangerous scenario occurs: This PSV is not designed for pressure and flow rating as the first stage separator, and the PSV is not able to depressurize the second stage vessel before a rupture takes place. The rupture leads to gas leakage, which may be ignited by a hot surface or a spark from electrical equipment.

Manual intervention by operators may be possible. However, the attackers may have manipulated the information shown on the operator screens. It may be too late to respond when the operators eventually receive an alarm about a gas leak or fire.

We have deliberately chosen not to focus on the motivation and resources behind the attacks. Instead, we are interested in understanding how cyber-attacks can contribute to a loss of control and safety by manipulating OT systems.

From the attacks that were addressed above, we can summarize some learning points:

- Intrusions into the systems often occur for some time before being uncovered. Many attacks have exploited zero-day vulnerabilities where defenses are not yet in place.
- Attacks on OT require extensive planning and traditional engineering resources. The attackers must understand the physical process, instrumentation, and other OT technologies, including controllers, communication protocols, and servers. They may also need to build teams with expertise in process, mechanical, electrical, automation, and technical safety engineering.
- Attackers do not always succeed in reaching their goals. Analyses of past attacks show they had greater potential for damage than the damage that occurred.
- Cybersecurity threats reduce the willingness for openness and sharing of experience and knowledge. Safety improvement has relied on sharing knowledge and learning from one another. Concepts, design principles, risk assessment experience, and operational experience relevant to safety are often shared at conferences and on networks. With the cybersecurity threats to OT, this openness can become dangerous. Technical documentation, such as P&IDs,

SCDs, and C&E matrices, can be exploited if it falls into the "wrong" hands. Insight into hazards and risk assessments can provide attackers with important information about design assumptions that can be exploited to identify weaknesses.

- Safety barriers have been dimensioned to handle incidental events, usually assuming that the most critical ones are not likely to happen simultaneously. A cyber-attack can be designed to create simultaneous events.
- Supply chains are attractive targets for cyberattacks. If malware is introduced early in the value/supply chain, some cybersecurity measures in OT systems will not be effective.
- The risks of cyberattacks can cause operators to have less trust in the control and safety systems, which could potentially lead to less efficient handling of situations where cyberattacks are not present.

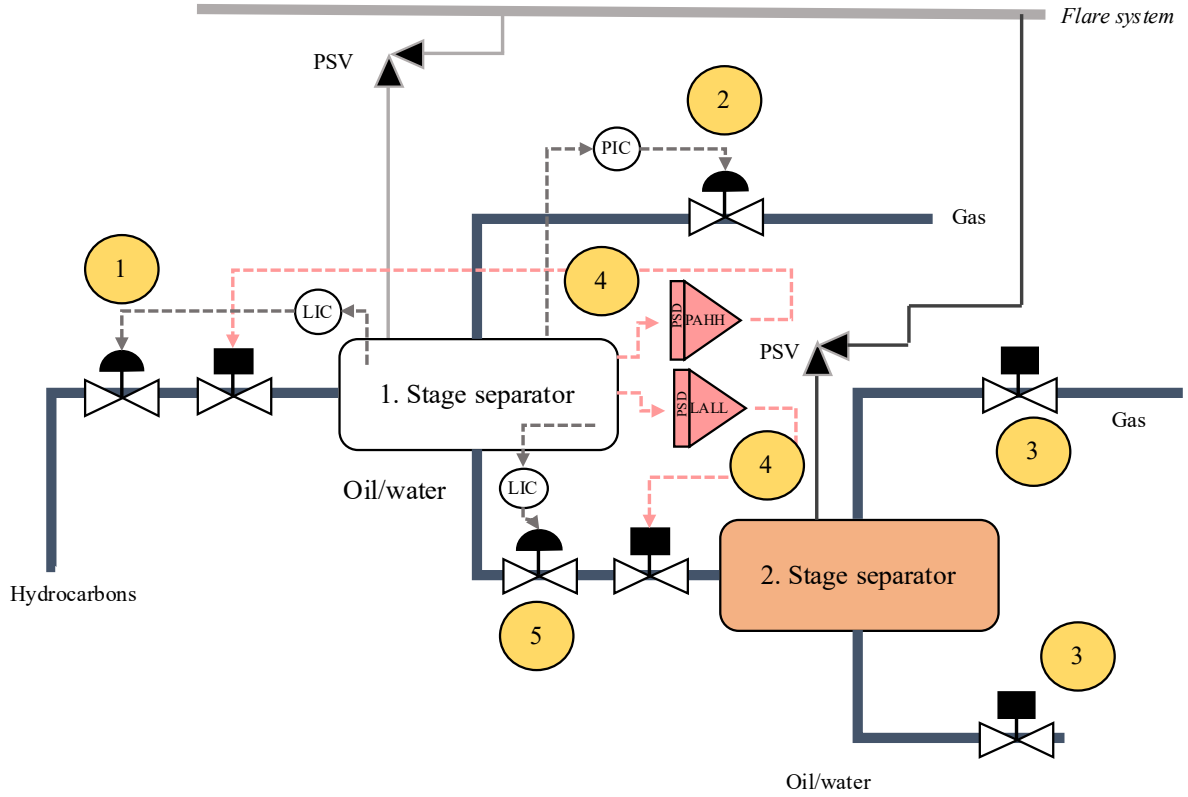


Fig. 30. Example of a process involving two separators

Governments, industries, and organizations are making considerable efforts to improve cybersecurity management in OT systems. We will present some of the regulations, frameworks, and standards currently in use for this purpose.

11.8 Identification and examples of cybersecurity measures

This section provides examples of industry standards and guidelines used to identify applicable cybersecurity measures, examples of security measures, and broader approaches to managing cybersecurity, including engineered measures that are not dependent on, or are less dependent on, computerized systems.

11.8.1 The general NIST cybersecurity framework (CSF)

The NIST Cybersecurity Framework 2.0 (2024) does, as already mentioned in Chapter 11.3.5, define six categories for cybersecurity measures, or security measures, into six categories (or high-level

functions), also visualized in Fig. 31: Identify, protect, detect, respond, recover, and govern, each accompanied by some examples of measures being mentioned. The same six categories are often seen in companies' descriptions of their own cybersecurity practices.

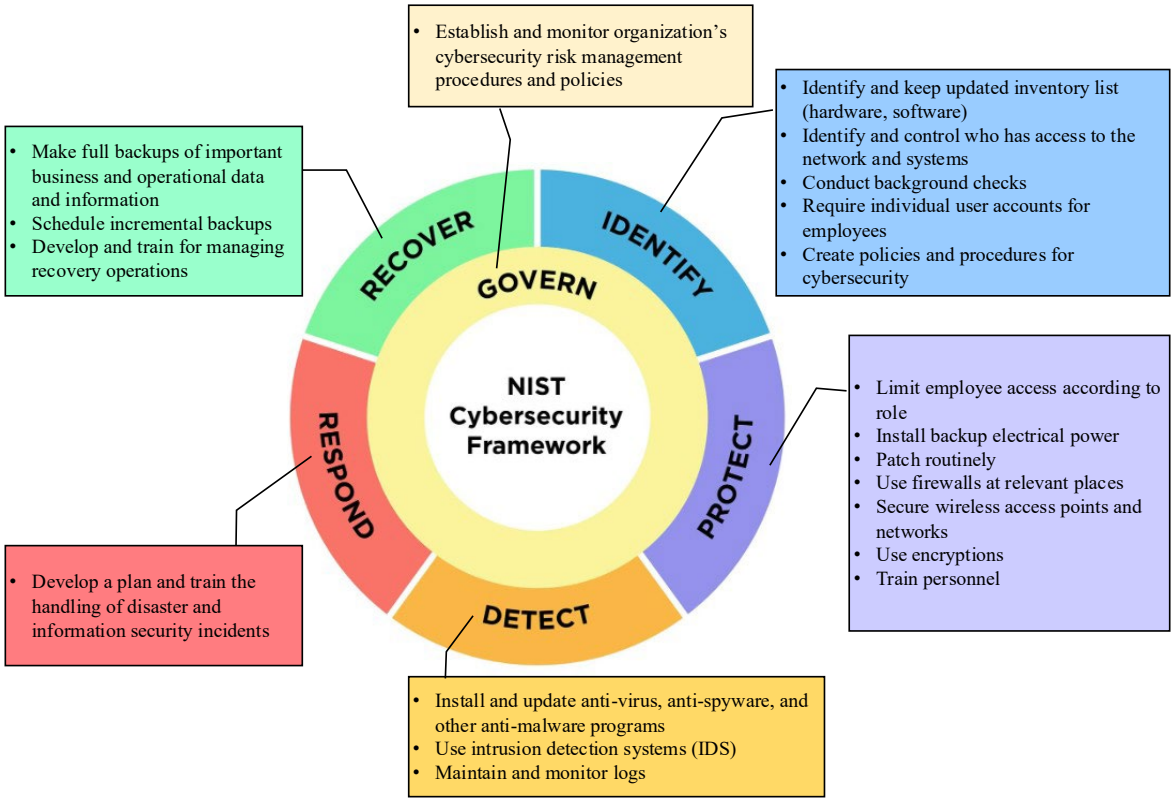


Fig. 31. NIST approaches to cybersecurity (Adapted from NIST CSF)

11.8.2 The NIST guideline to OT cybersecurity

NIST Guide on OT Cybersecurity SP 800-82 (2023) builds on NIST CSF, but with more concrete recommendations for how OT security is handled. For example, the guideline explains many specific considerations that apply to OT, which are not so relevant for general IT. The guideline suggests concrete tasks related to:

- Develop an OT cybersecurity program, identifying the specific OT systems following the structure of the general NIST cybersecurity framework's six security measure categories. An interdisciplinary team should carry out the preparation and implementation to reconcile security and operational needs.
- As part of the OT cybersecurity program, establishing a risk management system for OT systems, including policies and practices to apply over the whole lifecycle, training programs, and special considerations to safety risks and supply chain risks. The risk management program needs to address that many OT systems differ from traditional IT systems and involve hardware and software spanning multiple technological generations.
- It is essential to have an in-depth defense strategy to prevent and mitigate the impacts of cyberattacks.

The guideline identifies five categories of cybersecurity measures:

Layer 1: Security management: This is the implementation of the OT cybersecurity program and also manages the subsequent layers.

- Layer 2: Physical security: This covers measures to protect physical locations (doors, gates, cabinet locks), physical access control, access monitoring systems, and people and asset tracking.
- Layer 3: Network security: This covers network segmentation, isolation, logging and monitoring, and malicious code protection. Zero-trust architecture can be part of this layer, with protection added closer to the device connected to the network. Zero-trust is considered more relevant to Purdue levels 3 and above than to lower levels.
- Layer 4: Hardware security: This covers the protection added to devices to ensure security, such as embedded technologies like Trusted Platform Modules and Advanced Encryption Standards, if these are applicable to the OT system in question. Other examples include monitoring and analysis, secure configuration, hardening, access control, and physical security.
- Layer 5: Software security: This covers the protection added to secure software applications and services, such as patching, application whitelisting, configuration management, and code development review for security issues.

The five types of defenses apply to all six NIST categories of security measures, and examples of specific considerations for OT are provided in Tab. 1. The table is extended with types of baseline requirements suggested by Offshore Norway (ON) guideline 104 (2026) as a minimum, to represent industry-agreed best practice.

Tab. 1. Examples of OT security measures

NIST category	NIST OT cybersecurity guideline recommendations	Offshore Norway guideline 104 recommendations
Governance	• Ensure that the cybersecurity program is given sufficient resources on the OT and IT sides. • Establish good communication and coordination between IT and OT personnel, including procedures and processes • Identify roles and their responsibilities and accountabilities. • Establish cross-training in IT and OT to support all parts of the OT cybersecurity program.	• Security policy for OT environment • Cybersecurity risk management • Supply chain risk management • Acceptable use management
Identify	• A manual process for maintaining an inventory list for OT systems may be needed, as automated tools and active scanning may negatively impact the operation. • Review past cyber and non-cyber attacks and attempts to identify new scenarios to consider in hazards and risk analyses. • Consider utilizing an industry-recognized certification process for OT products to support supply chain management.	• Hardware and software inventory • Network topology drawings • Vulnerability and patch management • Change management

		• Operation and maintenance procedures
Protect	• Use of centralized identification and authentication of users • Complement the lack of authentication restrictions on some systems, like HMI for control room operators, which must be available in an emergency, with physical security. • Compensate for or adjust to the operating environment, such as by using equipment suitable for temperature, vibration, and humidity, ensuring the availability of heat and ventilation systems and reliable access to power. • Manage that patches are more complex to install in an OT environment and require extensive testing offline before being rolled out. The risks of introducing a patch must be balanced with the benefits of removing the vulnerability and the possibility of applying other compensating measures. • Manage remote access so that the activity is announced to relevant operating personnel when ongoing, and that the devices used for remote connections are clearly labeled so that disconnection can be made quickly.	• Training and competence • Network segmentation • OT DMZ • Secure remote access • Identity and account management • Security hardening • Malicious software protection • Virtualization
Detect	• Manage that the threshold for intrusion detection systems needs calibration for the OT environment to avoid many false positives. • The use of shared credentials should be monitored. • Consider that tools used for active and passive scanning must be carefully tested for use in OT environment	• Security monitoring and alerting
Respond	• A list of both internal and external personnel (supporting OT and IT technologies) for response handling must be available • Need to consider capabilities to minimize impact until people arrive e.g., remote shutdown or disconnect) if facilities are unmanned and remotely operated. • Insight into the implications of cyber incident measures that may impact the operation, like leading to a shutdown or loss of view for operators.	• Incident response • Island mode • Backup and restore

Recover	• A list of both internal and external personnel (supporting OT and IT technologies) for recovery tasks must be available.	

11.8.3 IEC 62443

IEC 62443 on cybersecurity for Industrial Control and Automation Systems (IACS) has become the primary standard for managing cybersecurity for OT systems internationally, without reducing the popularity of the NIST frameworks for OT cybersecurity, as it is more accessible because it is open source and not dependent on any subscription.

IEC 62443 is not a single standard; there are several, each with a part number added after the primary standard code, as illustrated in Fig. 34. The shaded standards have not been published as of June 2026 and exist only in draft form.

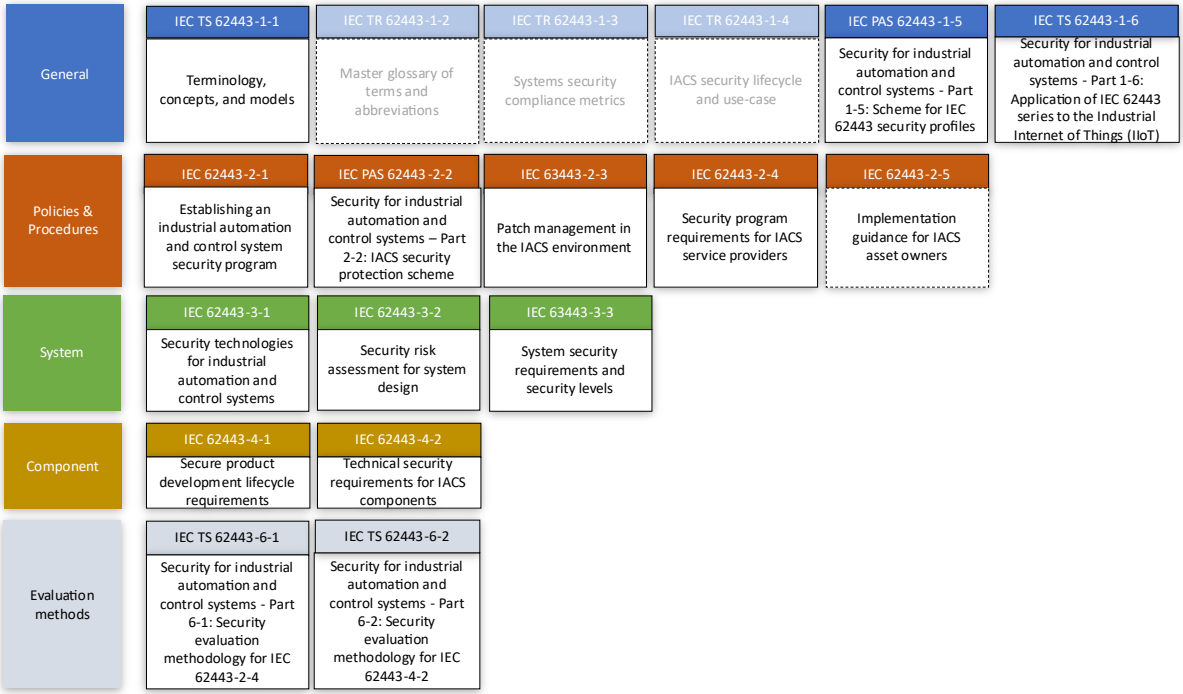


Fig. 32. Overview of IEC 62443

Key topics addressed in the standard are:

1. Cybersecurity lifecycle
2. Cybersecurity risk analyses
3. Security level (SL) for zones, conduits, systems, and products
4. Maturity level (ML) as a measure of the organization's ability to manage cybersecurity
5. Security Program Rating (SPR) as an overall cybersecurity performance measure where ML and SL are combined.

IEC 62443 defines three main stakeholders of the standard, which have a key role in the fulfillment of cybersecurity requirements:

- Asset owner
- Service providers (system integration and maintenance execution)

- Product suppliers

A simplified matching of which parts of the standard apply to which stakeholder is shown in Tab. 2. Within the category of policies and procedures, some parts may be more key to some stakeholders than others.

Tab. 2. How the types of requirements apply to different stakeholders

Category	Scope	Applies to		
		Asset owner	Service provider	Product supplier
General requirements	Terminology, general concept	X	X	X
Requirements relating to process and organization	Requirements for work methodology, competence requirements, roles and responsibilities, and measurement of maturity	X	X	X
System requirements	Risk analysis, network segregation, and defining security level (SL) requirements	X	X	
Component requirements	Development process, technical requirements for configuring the product			X

The following sections describe some selected concepts and approaches advocated in the standard.

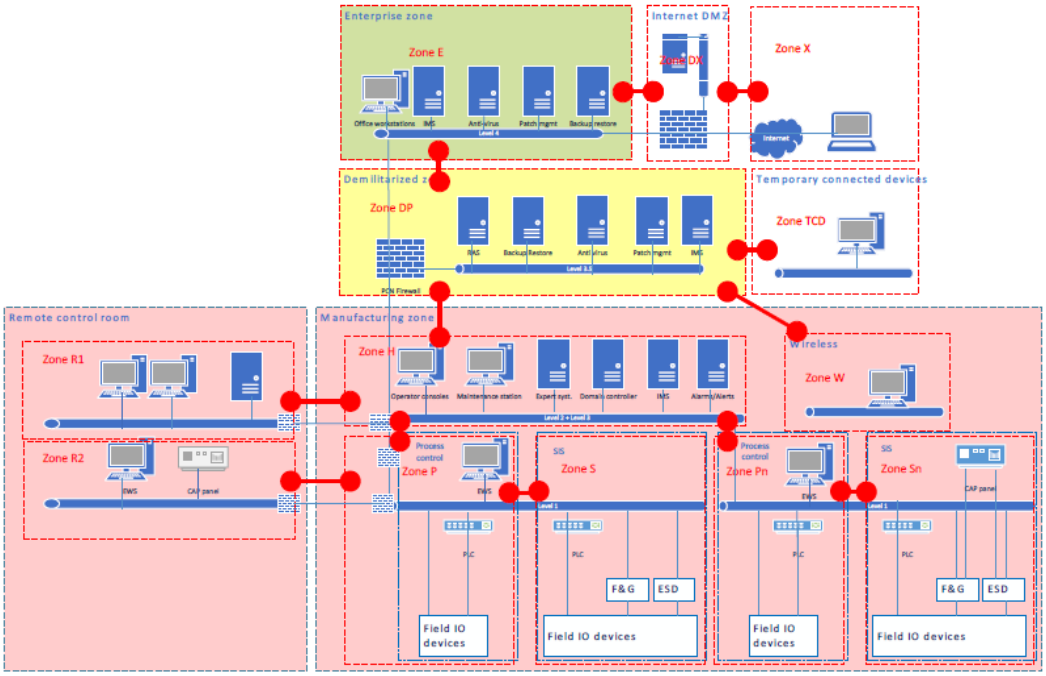


Fig. 33. Example of zones and conduits of a network architecture (Source: DNV RP G108)

11.8.3.1 Security zones and conduits

Two concepts central in IEC 62443 are security zones and conduits. The security zones are organizing logical and physical assets based on one or more criteria, such as:

- Similar risk exposure

- Same operational function
- Same location
- Same access needs

Conduits are the logical grouping of communication channels connecting two or more zones that share common security requirements. The use of security zones and conduits is part of a network segmentation strategy.

A network topology with zones and conduits marked is illustrated in Fig. 33. Here, conduits are shown as red links, while the zones are stippled.

11.8.3.2 Security level (SL)

Security level (SL) is another key concept in IEC 62443, not to be misinterpreted as safety-integrity level (SIL) that is used for SIS systems. Similar to SIL, SL is split into four levels, depending on strength of the protection measures:

SL	Description
SL 4	Protection against intentional violation using sophisticated means with extended resources, OT specific skills and high motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, OT specific skills and moderate motivation
SL 2	Protection against intentional violation using sophisticated means with low resources, generic OT skills and low motivation
SL 1	Protection against causal and coincidental violation

SL is not applied to security *functions* but to individual OT or IT systems or a group of such systems located in the same security zone or conduit..

SL is used in three different contexts:

- As a requirement - SL-T: The SL target, most commonly defined in a cyber risk analysis.
- As what a system is capable of - SL-C: The SL capability provided with the product by the manufacturer, with basis in configurable security measures that the system supports.
- As what is actually achieved - SL-A: The SL achieved, considering how individual systems or overall for the zone or conduct.

SL-A can also be split into SL-I, which refers to what has been achieved for the implemented SL, and SL-O, where O denotes SL achieved in operation. While SL-I is determined only once, when the system or a group of systems is put into operation, SL-O must be reassessed and monitored throughout its entire operational lifetime.

It follows that SL-A (and SL-I and SL-O) must be no less than SL-T.

11.8.3.3 Cybersecurity lifecycle and cyber risk assessment

IEC 62443 applies a cybersecurity lifecycle, covering both design and operation, as shown in Fig. 34. Two central activities in the first phase of the lifecycle are the initial (high-level) analysis, which focuses on partitioning the system into zones and conduits, and the detailed analysis, which focuses on determining the SL-T for the systems within each of these

Together, the two risk assessments involve:

1. Define the system under consideration (SUC) and the boundaries of the systems and networks that are part of the analysis. SUC is an analog term for Equipment Under Control (EUC) in the context of functional safety; however, SUC primarily applies to network systems, whereas EUC applies to physical systems.

2. Prepare a detailed description of the SUC network architecture and its constituent network segments. A segment should organize ICT equipment by function and role. The Purdue model, with its layers, serves as a suitable starting point; however, one may introduce more than one segment within each layer.
3. Define each segment as a zone or consider grouping some segments into the same zone and defining connections between the zones as conduits.
4. Assess the risk associated with threats for each network segment, considering its location, exposure, and the capacity of the threat actors.

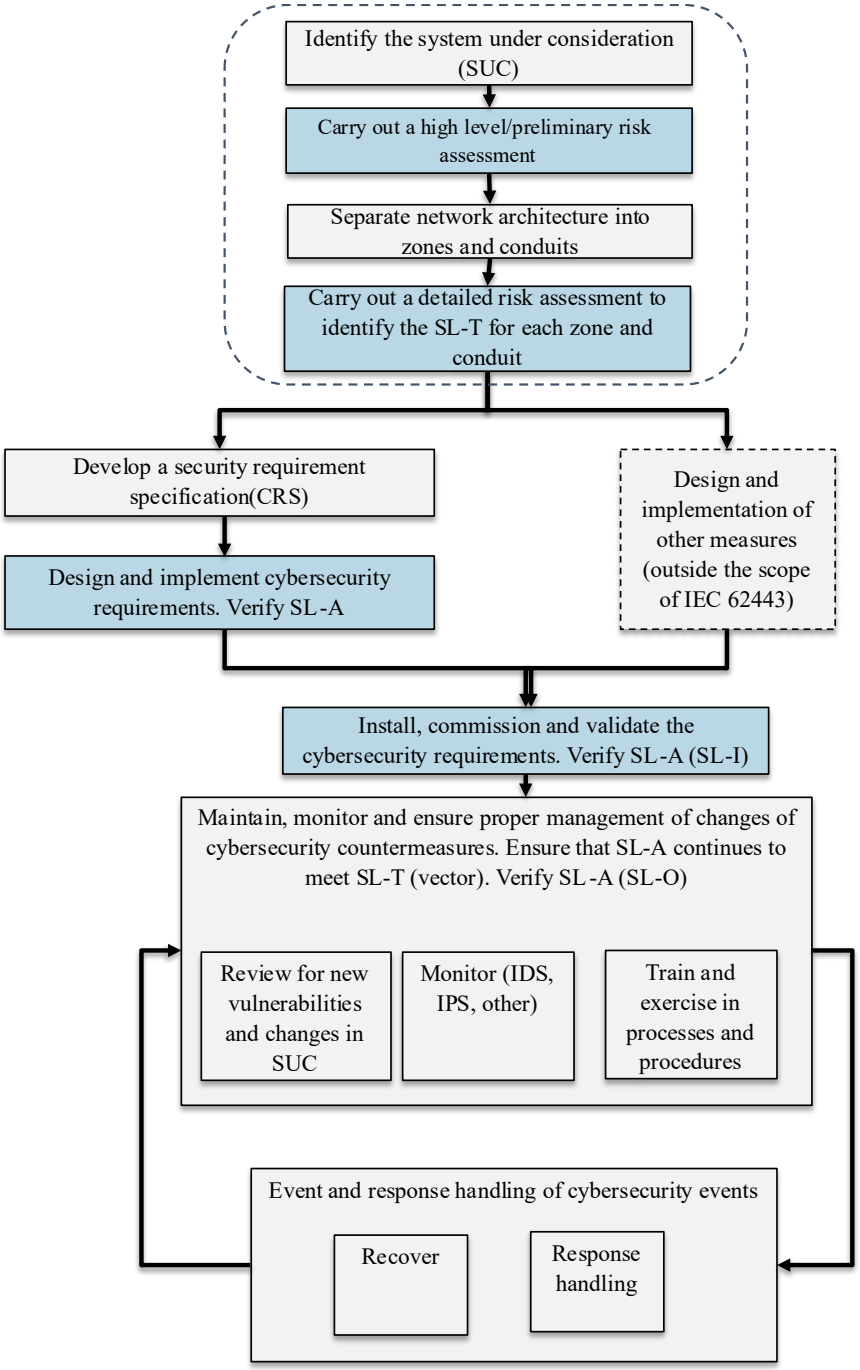


Fig. 34. Complete cybersecurity lifecycle (adopted from IEC 62443)

5. Conduct a risk assessment that evaluates threats, exposure, and general vulnerabilities associated with the zone and conduct, and propose security level targets (SL-T) for systems within the zone. It is not always the same S-T that is applied to every system within the same zone, as their risk profiles can differ. These risk assessments and criteria are often internal to the company and not shared.
6. When all systems and equipment within a zone are configured, an assessment is made about the security level achieved (SL-A) for each of them. To meet the requirement, SL-A must be greater than or equal to the SL-T that has been specified. This, in turn, relies on equipment with a given SL-C (capability) that is configured so that SL-A meets SL-T.

The DNV RP G108 (2017) guideline on application of IEC 62443 for the oil and gas sector suggests that:

- DMZ between IT and OT is generally defined as a single zone
- An internet / external DMZ can be defined as a segment of the company's IT network from which external users are connected via the internet.
- The OT network will often have several zones within the same level (of the Purdue model). For example:
    - PCS and SIS can be defined as separate zones, even though both are at level 1.
    - The local control room and the remote-control room will be placed in separate zones, even if they belong to level 2.
    - Wireless networks that collect non-critical data not involved in control or safety functions may be in a separate security zone at level 0, directly connected to level 3. NAMUR Open Architecture suggests an alternative approach for sharing these data directly with level 4, using a unidirectional gateway.

11.8.3.4 Process for determining SL-T

The SL-T is often determined by a team of experts who systematically evaluate threat actors' capabilities to reach systems, i.e., the systems' exposure within each security zone of the network, and the severity of the consequences if the actors succeed. A risk matrix like the one in Tab. 3 which suggests an SL T value, considering likelihood and consequence, may be used to assist the process.

The colors of the matrix cells indicate the extent to which the risk is unacceptable (red cells), conditionally acceptable (yellow cells), and broadly acceptable (green cells). This approach to expressing risk acceptance by the three regions is known as the ALARP principle (As-Low-As-Reasonably-Practicable), and the yellow zone is often referred to as the ALARP zone. The SL T values are assumed to be chosen so that the risk is sufficiently reduced from a red zone to a yellow zone or reduced sufficiently within the yellow zone. No specific SL T value applies to systems whose risk is already generally acceptable.

Tab. 3. Risk matrix (Tabell B.4 i IEC 62443-3-2) ((with examples of SL-T requirements added)

Likelihood	**Consequence**		
	A (Negligible) (1)	**B (Moderate) (3)**	**C (Severe) (5)**
Likely/certain (5)	Medium (5) **[SL 1]**	High **(15) [SL 2]**	High **(25) [SL 4]**
Possible (3)	Low (3) **[SL 1]**	Medium (9) **[SL 2]**	High **(15) [SL 3]**
Unlikely (1)	Low (1) **[---]**	Low (3) **[SL 1]**	Medium (5) **[SL 2]**

An example of how the results may look after having assessed various types of systems is illustrated in Tab. 4.

Tab. 4. Results of a (fictitious) workshop

Exposure of system	Likelihood	Consequence	Risk	SL-T
Operator station (local)	3	5	**15**	2
Operator station (remote)	3	5	**15**	2
Engineering workstation: PCS SIS	3 3	3 5	**9** **15**	2 (PCS) 3 (SIS)
Historian server (alarms alert + Information management systems - IMS)	3	3	**9**	2
Controllers: PCS SIS	1 1	3 5	3 5	1 (PCS) 2 (SIS)
Firewall in DMZ	3	5	**15**	3
Firewall external/ internet DMZ	5	5	**25**	4

Examples of SL-T levels that have been applied to systems, indicating that some systems may have different SL-T targets depending on their risk profile are:

- DMZ zones :
  - DMZ 3.5 zone : SL-T 4
  - Remote access DMZ: SL-T 4
- Control room zone:
  - Process control read/write (local and remote) HMI: SL-T 2
  - SIS read/write (local or remote) HMI: SL-T 3 + disconnected / stronger conduits
  - Process control/SIS remote Read-only HMI: SL-T 3
- Process control zone:
  - EWS: SL-T 2 + disconnected/stronger conduit
  - Logic solvers: SL-T 1 + stronger conduits
- SIS zone_
  - EWS: SL-T 3 + disconnected / stronger conduits
  - Logic solvers: SL-T 1 + stronger conduits

Here, stronger conduits mean additional measures implemented to monitor conduits. In contrast, a disconnected conduit means the automatic capability to stop communication through the conduit using the firewall's fail-safe or island mode. The results that we assume the workshop ended up with are presented in Tab. 4.

11.8.3.5 Security measure categories and relation to SL T

IEC 62443 applies seven categories (or types) of cybersecurity measures:

1. **FR 1: IAC - Identification and authentication control.** Requirements relating to managing access and authentication ("log in and in").
2. **FR 2: UC—Use control.** Requirements for setting restrictions on who can access systems and data.

3. **FR 3: DI – Data integrity.** Requirements relating to the protection against unauthorized changes of communications and software.
4. **FR 4: DC - Data confidentiality.** Requirements relating to protecting data and software from sharing.
5. **FR 5: RDF - Restricted data flow.** Requirements relating to the limitation and prevention of unnecessary data flow.
6. **FR 6: TRE - Timely response.** Requirements relating to the ability to respond fast enough to act upon detected cyberattacks or cyber incidents
7. **FR 7: RA - Resource availability.** Requirements relating to the availability of network resources that can protect against so-called denial of service attacks

For each FR, there is a corresponding set of cybersecurity requirements (SRs), as illustrated in Fig. 35 and with some additional examples in Tab. 5.

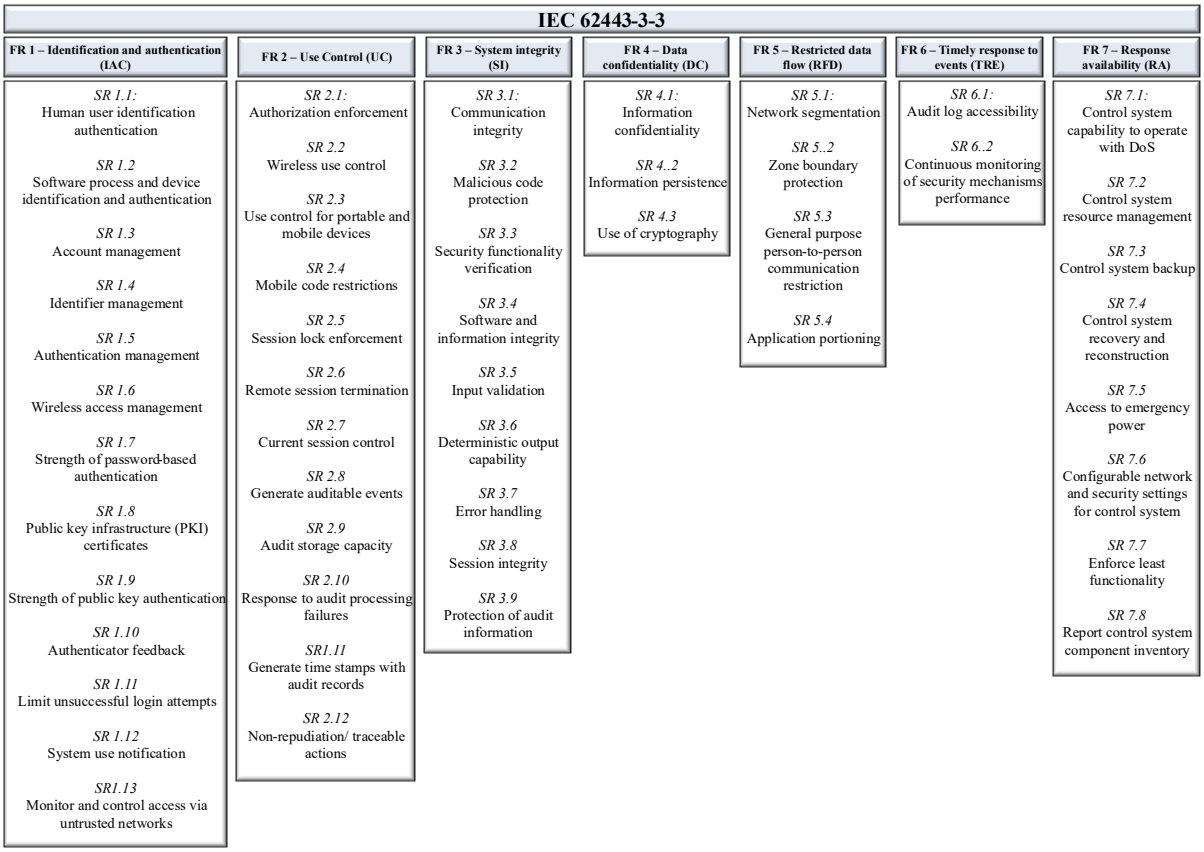


Fig. 35. Overview of FRs and SRs in IEC 62443-3-3

Tab. 5. Examples of security measures per FR category

FR		Example 1	Example 2	Example 3
1	IAC	Identification: Password, biometrics, combination if possible (multifactor). Role-based/user-based access for process-critical	Access management software and equipment: Before access is granted, everything connected must be uniquely identified using a Password, key, or token.	Ensure that codes and access layouts used on the first installation are removed and replaced with new ones. Change passwords and

		operations in control rooms. Time-limited access.		encryption keys regularly.
2	UC	Check that those who attempt to conduct actions after identification have rights to this (according to User Rights Slots). Ensure that roles related to the initiation of critical functions related to plant safety are not prevented (E.g., Supervisor override).	Two-factor authentication for performing particularly critical functions, such as changing setpoint/trip boundaries.	Management of, including any time-limited access, to conduct actions related to temporary equipment (mobile, wireless). Make sure that the wireless equipment that connects is configured with functionality limitations.
3	DI	Encryption and decryption. Virus code provision at all levels, such as fire watchers, one-way gateways, servers,	Monitoring of deviations in data exchange, e.g., against specification. Check the valid format of inputs. Regularly test (manually, automatically) the various security functions: Authentication, user management, and virus protection.	Protection against being able to edit investigation logs and activities generated by the cybersecurity monitoring system Ensure that outputs can be set to a predefined state if regular operation cannot be maintained during an attack.
4	DC	Ensure remote access confidentiality that may involve transmission over unsecured networks (the Internet). Apply encryption/decryption.	Ensure that all data on components that are taken out of operation are deleted. Ex "joint key".	Ensure confidentiality when information passes between zones.
5	RDF	Network segmentation – logically and or physically distinguish control networks from other networks, for example, condition monitoring	Zone boundary protection - have sufficient firewalls, one-way gateways, etc...	Prevent control systems or operator stations from using applications that require remote access: Facebook, photo sharing.
6	TRE	Limited and not direct access to investigation reports from control systems	Use of monitoring tools such as Intrusion detection system (IDS), Intrusion protection system (IPS), malware protection,	
7	RA	Ensure that the instrumentation systems do not get or completely stop in "essential services". That is, prevent "DoS" for critical control and security functions by isolating these when necessary, filtering	Ensure that sufficient resources are available to maintain normal function in the instrumentation systems even if scanning, patching, virus checks, etc., are conducted.	Backup of the control systems and logs in case of damage caused by cyber-attacks or by patching. Ensure that the control system automatically gets the correct security

		data, or using "unidirectional" communications.		values after a recovery and that the necessary patches, configuration, etc., are reinstalled.

A zone, being exposed to the same risk level, may include systems in which the types of feasible security measures may vary. For example, security requirements related to communication verification and input validation may be practical for a controller but impractical for a server. Having to type individual passwords to access alarm lists in the control room can be impractical and unsafe if operators are locked out due to a forgotten password.

For this purpose, IEC 62443 applies an SL T vector with 7 dimensions, where each FR-category has its own SL T value.

- SL vector: [SL T (IAC), SL T (UC), SL T (SI), SL T (DC), SL T (RDF), SL T (TRE), SL T (RA)]

Examples of how SL vectors may look are:

- SL-T (PCS controller) = [2, 2, 0, 1, 3, 1, 3]
- SL-C (SIS EWS) = [3, 3, 2, 3, 0, 0,1]

11.8.3.6 Implications of SL-T requirements

Using a risk-based approach, IEC 62443 defines which specific security measures apply within each Functional Requirement (FR) category for a given Security Level Target (SL-T). General system-level requirements are outlined in IEC 62443-3-3 (2013) , while more detailed implementation requirements at the individual product level are covered in IEC 62443-4-2 (2019). At the individual product level, systems are distinguished into four categories: Software, embedded devices, host devices, and network devices.

Tab. 6. Mapping of SRs and REs to SL levels for FR1 (Identification and Authentication). Adopted from IEC 62443-3-3.

	SL requirement (SL T)			
Security measures	**SL 1**	**SL 2**	**SL 3**	**SL 4**
FR 5 – Restricted data flow (RDF)				
SR 5.1 Network segmentation	x	x	x	x
RE1 Physical network segmentation		x	x	x
RE2 Independence from non-control system networks			x	x
RE3 Logical and physical isolation of critical networks				x
SR 5.2 Zone boundary protection	x	x	x	x
RE1 Deny by default, allow by exception		x	x	x
RE2 Island mode			x	x
RE3 Fail close			x	x
SR 5.3 General-purpose person-to-person communication restriction	x	x	x	x
RE1 Prohibit all general purpose person-to-person communications			x	x

SR 5.4 Application partitioning	x	x	x	x

An example of how the choice of security measures are selected as a function of SL-T is illustrated in Tab. 6 for the FR5 Restricted data flow (RDF). In the table, SR means security requirement, while RE means requirement enhancement. For example, SR 5.1 identifies that networks are to be segmented into zones and conduits, while RE1, RE2, and RE3, related to SR 5.1, identify specific requirements to how the segmentation is implemented.

The standard explains SR 5.1-5.4, including their RE, as follows (with some rephrasing) as shown in Tab. 7

Tab. 7. Explanation of SR and RE requirements for RDF

Security measure	**System level (IEC 62443-3-3)**	**Component /product level (IEC 62443-4-2)**
Network segmentation	The OT system shall provide the capability to logically segment control system networks from non-control networks and to logically segment critical control systems (i.e., safety systems) from other control system networks.	All component types (software, embedded devices, host devices, and network devices) shall support a segmented network, as specified by the SL T level.
Physical network segmentation	The OT system shall provide the capability to provide the mentioned network segmentation *physically*, not logically.	
Independent from non-control networks	The OT system shall be capable of providing network services to control systems, whether critical or otherwise, without a connection to non-control networks.	
Logical and physical isolation of critical networks	The OT system shall provide the capability for physical and logical network segmentation.	
Zone boundary protection	The OT system shall provide the capability to monitor and control communication at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduit model.	*Network devices* at zone boundaries shall be capable of monitoring and controlling communication.
Deny by default, allow by exception	The OT system shall provide the capability to deny network traffic by default and to allow it by exception.	*Network devices* shall be capable of implementing the listed features as required by the SL-T level.
Island mode	The OT system shall provide the capability to prevent any communication through a specific boundary.	
Fail-safe	The OT system shall be capable of preventing any communication across a specific boundary if the boundary protection mechanism fails (for example, boundary protection hardware failure or power failure).	
General-purpose person-to-person communication restrictions	The OT system shall be capable of preventing general-purpose person-to-person messages from being received from users or systems external to the OT system.	A network device at a zone boundary shall provide such protection by blocking specific communications based on port numbers and source and/or destination addresses, as well as

		performing in-depth checks by application-layer firewalls.
Application partitioning	The OT system shall provide the capability to support partitioning of data, applications, and services. Partitioning may be accomplished physically or logically by considering different computers, different central processing units, different operating system instances, different network addresses, and combinations of these. Examples of applications and services to consider for partitioning are, but not limited to, safety-instrumented systems, closed-loop control applications, operator stations, and engineering stations.	No specific requirements for components, as the chosen solution follows from decisions at the system level

11.8.3.7 Role of maturity level (ML)

Cybersecurity of OT systems is not achieved solely through technical measures. Measures related to organizational factors, such as the availability of procedures, necessary competencies, and personnel training, are equally important. Competence requirements and training are necessary at various levels within the organization, not just for cybersecurity experts. IEC 62443 has therefore introduced organizational maturity as a focus area in addition to the foundational requirements (FRs), and in a new draft of IEC 62443-2-2 (not yet published), the concept of maturity levels (ML) is applied and defined as:

> **Maturity level:** A qualitative method of characterizing the efficiency of an organization to implement security requirements according to documented policies and procedures

Four ML levels are suggested, ranking how the measures have been implemented, and they are explained in Tab. 8. Inspiration may stem from the General Capability Maturity Model Integration (CMMI), a structured approach developed by the CMMI Institute (Wiki) to assess and rank organizations' capabilities.

IEC 62443 has suggested a combined measure, planned to be named Security Program Rating (SPR), that combines the scores (i.e., levels achieved for) ML and SL.

Tab. 8. Maturity levels (slightly reworded compared to the standard)

ML	Description
4	Level 3 with also the performance of measures being monitored and systematically followed up.
3	When it can be demonstrated that all level 2 processes are systematically applied.
2	Documentation exists that describes how to select, implement, and manage cybersecurity measures. However, there may be a significant delay between defining a process and executing/practicing it.
1	Work processes are performed ad hoc and often undocumented (or not fully documented)

11.8.4 Examples of security measures

Some further explanation of applicable security measures mentioned in e.g., IEC 62443-3-1 (2009) and NIST Guide on OT Cybersecurity SP 800-82 (2023), and the Norwegian guideline Offshore Norway (ON) guideline 104 (2026) (for the petroleum sector) are elaborated below.

11.8.4.1 Hardware and software inventory list

Knowing what you have is necessary for providing protection. Therefore, all OT hardware and software need to be clearly identified, registered, and kept up to date so that the seriousness of vulnerabilities, revealed by the company itself or through external notices, can be efficiently evaluated. Such a register is often referred to as a hardware and software (or asset) inventory list.

Keeping such a list updated can be difficult for many reasons. First, it may be cumbersome to identify what is installed across the entire network and to keep the registry up to date with new versions. Second, it may be challenging to reveal all the dependencies that follow the supply chain under which the product has been developed.

What may be helpful is the requirement by the EU Cybersecurity Resilience Act (CRA) (2024) that all manufacturers of products with digital elements must deliver a software bill of materials (SBOM) as mandated from January 1st, 2027. The product can be hardware with software or just software.

- An SBOM is to be a machine-readable inventory of software, covering identification of the component name, version number, and supplier name of:
    - Proprietary code
    - Third-party software
    - Open-source components
    - Top-level dependencies, meaning libraries that the application relies on to execute code
- The product manufacturer is legally responsible for keeping the SBOM updated.

The SBOMs will therefore be integrated with the hardware and software inventory lists that companies use for the available products. When a new vulnerability arises, the SBOMs can be consulted to identify which products are affected.

11.8.4.2 Network segmentation and isolations

Cybersecurity risk assessment is the primary method for segmenting the network into zones based on exposure risk and the importance of systems to plant safety and operation. Below is a brief explanation of some selected generally applicable zones.

OT DMZ: OT DMZ is the network zone separating while linking OT and IT networks. Specific requirements that Offshore Norway (ON) guideline 104 (2026) mentions in relation to OT DMS are:

- All network traffic between IT and OT shall be terminated in the OT DMZ, unless communication flows from OT to IT traverses hardware-enforced unidirectional gateways.
- Components within the OT DMZ shall not initiate communication to the OT system unless initiated by the secure remote access system.
- Systems in the OT DMZ shall be designed to support regular security patching during normal operation and hardened against vulnerabilities.

Secure access or internet DMZ:

Secure access to the internet (or remote access) DMZ may be obtained with Virtual Private Networks (VPNs):

- VPN provides secure and encrypted connections utilizing tunneling, security controls, and endpoint address translation, giving the impression of connecting through a dedicated “line”.
- VPN allows only authenticated and authorized users to access a system over a connection that can be exposed to security threats, such as remote access.

- Examples of common types of VPN technologies mentioned in the NIST Guide on OT Cybersecurity SP 800-82 (2023) on ICS security are:
    - Internet Protocol Security (IPsec)
    - Transport Layer Security (TLS), or Secure Sockets Layer (SSL)
    - Secure Shell (SSH)

SIS zone:

It is common to have a separate SIS zone and not to integrate it with the control (system) zones. In fact, Offshore Norway (ON) guideline 104 (2026) states that SIS networks *shall* be physically or logically segmented from non-safety system networks. However, it is recognized that the SIS needs to connect to other networks, but this must be in a manner that does not disrupt or otherwise compromise the SIS.

Wireless zones:

The need for wireless zones arises as more equipment at plants becomes wireless, including support tools and sensors for condition monitoring. It is natural that such networks are clearly segmented from wired networks and Offshore Norway (ON) guideline 104 (2026) mentions that these boundaries are strictly controlled.

A remark about airgaps:

Air gaps are sometimes mentioned as a segmentation method, meaning either no physical connection between OT and IT (or the internet) or no automated logical connection, so that data is transferred through the interface only manually under human control.

- However, an air gap is more of an ideal than a realistic concept, as there are workarounds that attackers may exploit.
- Designing cybersecurity efforts as if the OT network is air-gapped may increase vulnerabilities to successful attacks, as the organization may operate as if the workarounds are not possible.

Air gaps are therefore not an appropriate means of segregation. Not having a wired connection between OT and IT is unlikely to ensure there is no connection between them, and any unexpected connections are therefore not protected.

11.8.4.3 Network intrusion monitoring

Security monitoring and alerting capabilities are required to detect anomalies and other evidence of potential ongoing cyberattacks or intrusions within OT. Security measures include:

- Intrusion detection system (IDS): An IDS is a system whose aim is to detect ongoing cyberattacks by searching for suspicious patterns and known attack signatures within the network.
    - IDS can be seen as sensors being installed in the network or on a host (device). For this reason, we distinguish between **network-based IDS** and **host-based IDS**, and the two are often combined in OT networks.
    - There are three ways that IDS decides what normal and abnormal activities:
        - **Anomaly-based**: Can be implemented by rules (thresholds for what is abnormal), statistical models, or machine learning (or AI). When implemented by rule sets, it operates similarly to specification-based approaches, but not necessarily with the same rules.
        - **Knowledge (or signature) based:** The IDS looks for a specific piece of information in the transported data (network-based) or among files on a host that can indicate something is malicious. Malware scanning is an example of the latter.

- **Specification-based:** The IDS decides what is malicious or not based on generally applicable rule sets. For example, if a data packet is not structured correctly according to the protocol used, or if someone attempts to modify a file in a folder that is generally inaccessible (like system registers).

- Intrusion prevention systems (IPS): An extension to IDS that, upon the detection of an ongoing attack, attempts to stop it, ideally before it reaches its targets. The main distinction between an IDS and an IPS is that an IPS implements active measures to stop attacks.
- Security information and event management (SIEM) system. Covers the application of various tools for collecting security information and managing discovered alarms and events. It collects information from several systems, like IDS, IPS, firewalls, malware detection systems, and logs.

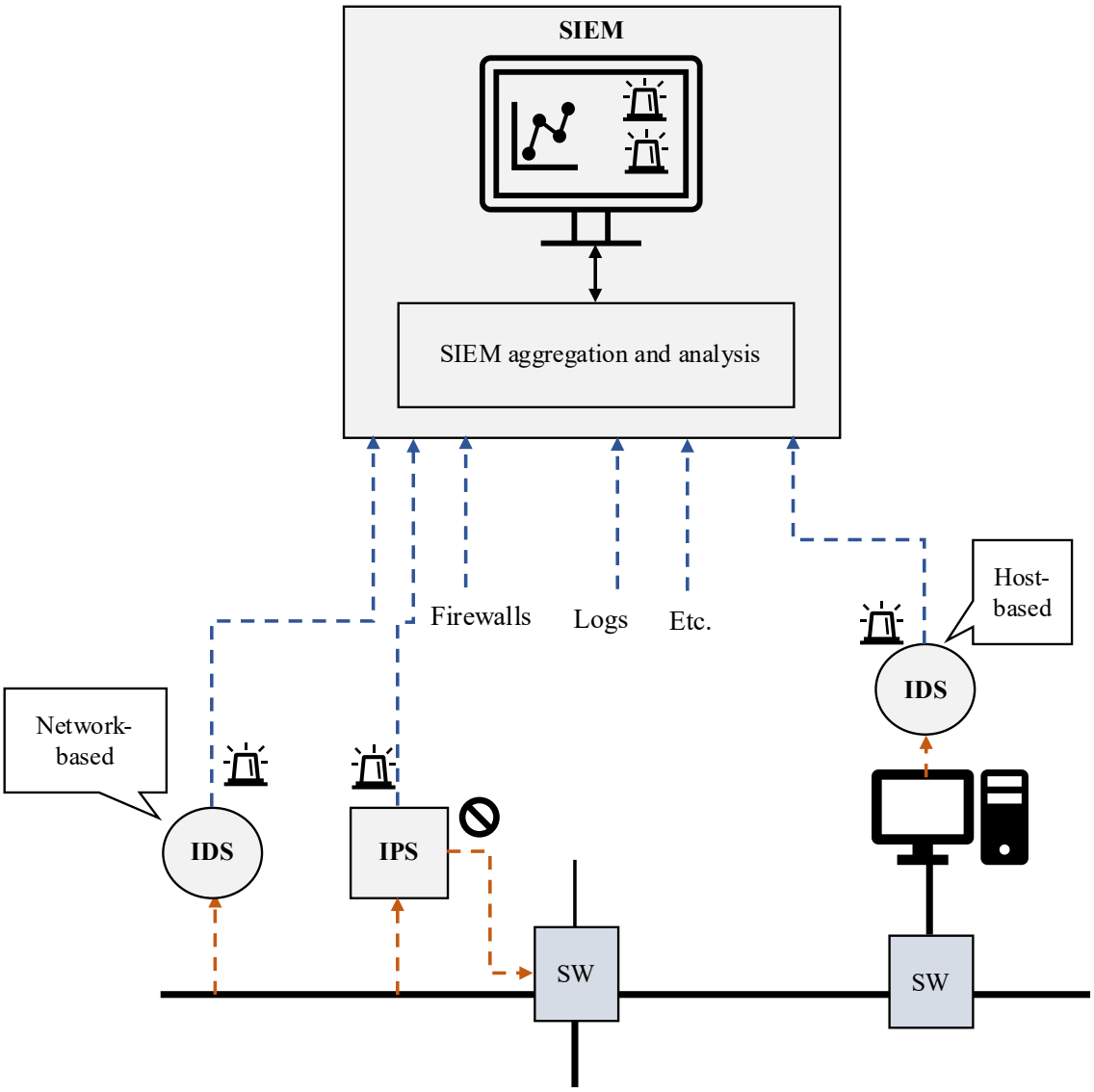


Fig. 36. Relationship between IDS, IPS, and SIEM

Fig. 36 illustrates, in a simplified manner, the roles of IDS, IPS, and SIEM, and their relationships.

Some examples of IDS that are used for or specialized towards OT are:

- ICSNNP
- Snort

- Suricata

The efficiency and applicability of network IDS generally decrease as you move downward in the Purdue reference architecture. For example, scanning may be less efficient for lower levels of the Purdue model (levels 0 and 1) than at higher levels, as it is not easy for these tools to judge what malicious activity is without having insights into the operational situation at the time

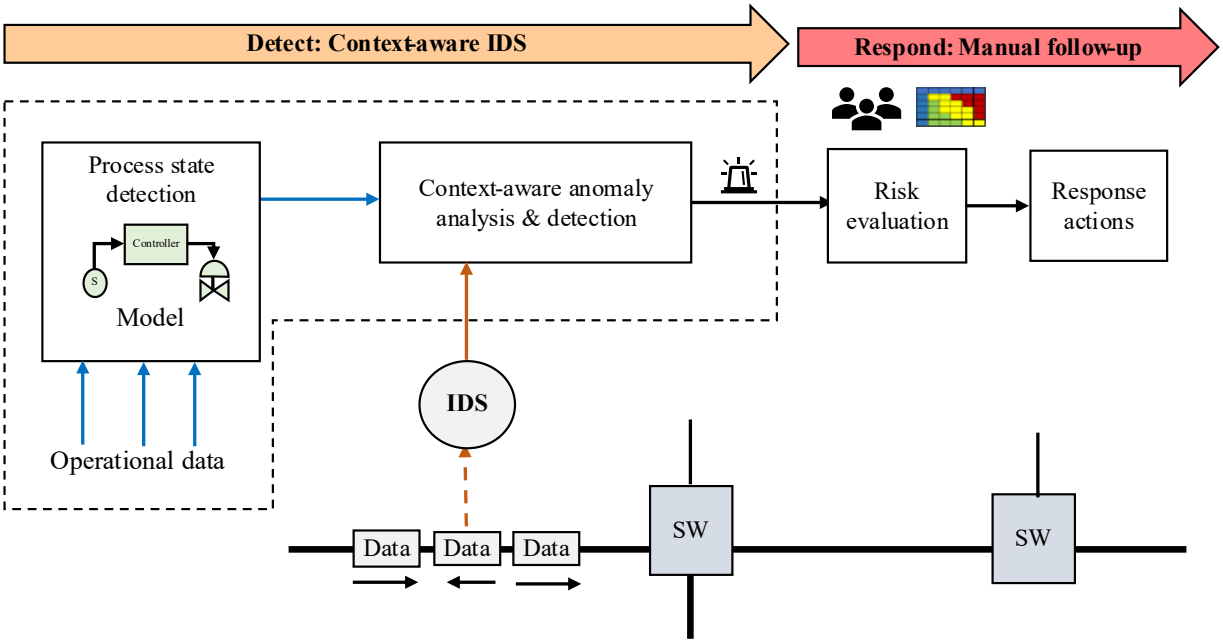


Fig. 37. Context-informed anomaly detection

A context-aware extension to IDS has been proposed as one possible solution for level 0-1 by Houmb et al. (2023). **Error! Reference source not found.** illustrates the basic idea: It combines detection of process state using models and operational data with network-based techniques to determine whether network activity is malicious, given the operational situation. The master's thesis by Vartdal (2025) investigated this approach and applied it in a laboratory setup using a simulated network environment and the software applications Suricata, Factory IO, ScadaBR, Open PLC.

11.8.4.4 Restriction of data traffic

Restrictions on data traffic may involve deciding who can communicate and the direction that communication is allowed to flow. Examples include:

Unidirectional gateways: Network devices that permit data transmission in only one direction and, for this reason, are referred to as data diodes.

- The use of fiber optics is a typical example of hardware implementation.
- In software, it can be implemented using firewall rules and software-implemented functions for unidirectional message routing (e.g., publish-only, consume-only).

Firewall: A system that controls and, as needed, stops network traffic flow in networks and between devices. Firewalls can be implemented as software functions in a gateway or as standalone hardware.

Specific modes of operation that can be implemented with the firewalls and which can be applicable for OT networks are:

- **Fail-close:** The ability to prevent any communication through the boundary of a zone automatically upon failure of the boundary protection mechanism or if the firewall is temporarily unavailable.

This mode may be activated, for example, when the firewall is being reconfigured or upgraded, or when it detects suspicious activity.

- **Island mode:** This mode is activated externally to the firewall, typically when the OT network is detected under attack, to keep critical systems operational. Activation can be manual or by e.g., IPS system. Once activated, affected systems, meaning the systems in the network that were disconnected, can continue to operate. For example, if island mode is activated for the SIS zone, the SIS systems can continue to monitor and automatically shut down the plant. Any manual activation by operators must then be directly wired into the SIS zone, to remain effective.

A simplified visualization of how island mode is activated is shown in Fig. 38. Here, the island mode is triggered either automatically by the intrusion protection system or manually by operators or the company's cybersecurity team. The fail-close mode is also an internal firewall feature that stops (closes) traffic through the firewall.

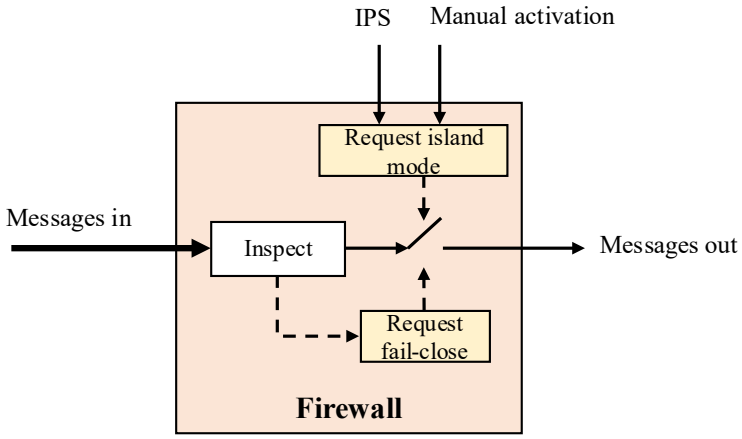


Fig. 38. Simplified explanation of the island mode

11.8.4.5 Hardening

Hardening is the collection of measures applied to reduce the attack surface of an individual system by removing functionality that is not strictly required.

Within OT, hardening is applicable for operator stations, PLCs and DCSs, EWS, and field devices with IIoT interfaces.

- Hardening an EWS can, for example, involve removing software that is not strictly necessary to serve its purpose and disabling hardware functionality, such as USB access ports. Disabling the ability to connect to networks other than the assigned ones and removing e-mail services are other examples.
- Hardening a PLC is to set a physical key, if available, in run modes where downloads of files from EWS to the PLC are prohibited, deactivate unused ports and protocols, and place the PLC into locked cabinets that can only be opened by authorized persons.

11.8.4.6 You and me

We all play an important role in preventing and detecting cyberattacks, even if we do not have a formal role in cybersecurity. For example:

- Control room operators may reveal unexpected or unexplained behavior that does not seem realistic or explainable, considering the state of the plant, and ask the cybersecurity team to investigate it.

- Automation and electrical technicians can double-check how a needed upgrade requiring a download from the manufacturer's homepage can be done in a secure manner.
- Technicians accessing equipment for calibration may consult the cybersecurity team if they discover default passwords in use for accessing devices for calibration.

11.8.5 MITRE D3fend matrix

MITRE is developing a MITRE Defend matrix in a beta version (per 2022) through research funded by the Cybersecurity Directorate of the National (USA) Security Agency. However, this matrix is now more general and not a variant for OT systems. The matrix serves as a defensive counterpart to the ATT&CK matrix. The beta version is published on the MITRE webpage (matrix, Accessed 2024) directed to IT systems in general and not to ICS in particular.

The matrix identifies six main defense tactic categories:

6. Model tactics by applying a suite of security engineering, vulnerability, threat, and risk analyses. A total of 26 techniques is suggested, covering asset inventory management, network mapping, operational activity mapping, and system mapping.
7. Hardening tactics by making computer and network access more difficult. A set of 32 techniques is suggested, covering application, credential, message, and platform (hardware) hardening.
8. Detect tactics by identifying adversary access to or unauthorized activity on computer networks. It covers 74 techniques for file analysis, identifier (e.g., IP addresses, domain names, and URLs) analysis, network traffic analysis, platform monitoring, process analysis, and user behavior analysis.
9. Isolate tactics by applying logical or physical barriers in a system to reduce opportunities for adversaries to create further access. Covers 22 techniques relating to execution isolation and network isolation.
10. Deceive tactic by allowing potential attackers to access an observed or controlled environment (honeypot/net). Covers 11 techniques relating to decoy environments and decoy objects.
11. Evict tactic is about removing an adversary from a computer network. Covers five techniques relating to credential eviction and process eviction.

The D3fend matrix is still under development, and the latest version can be found on the Mitre webpage.

Even if a study has not been conducted, many techniques may be found directly or deduced from the security requirements in IEC 62443-3-3.

11.8.6 Consequence-driven cyber-informed engineering (CCE)

According to the US Department of Energy, cyber-informed engineering is a method for integrating cybersecurity considerations into the conception, development, and operation of physical systems. Industrial plants are typically designed to withstand unintentional events rather than deliberate ones. Cyber-informed engineering recognizes that modifications to design or operations can reduce or even prevent some of the worst-case consequences of events created by deliberate acts of the attackers.

Consequence-driven Cyber-informed Engineering (CCE) is a methodology based on cyber-informed engineering principles developed by Idaho National Laboratory (INL). The entire method is explained in a report by INL (2020) and in a book by Bochman and Freeman (2021). CCE's underlying assumption or claim is that "if a skilled and determined adversary targets a critical infrastructure system, the targeted network can and (at some point) will be penetrated.

11.8.6.1 The four phases of CCE

The four-phase model is consequence-driven, meaning it prioritizes protecting the most critical parts of the plant or infrastructure, with effort allocated accordingly. The model is illustrated in the CCE method, as shown in Fig. 39.

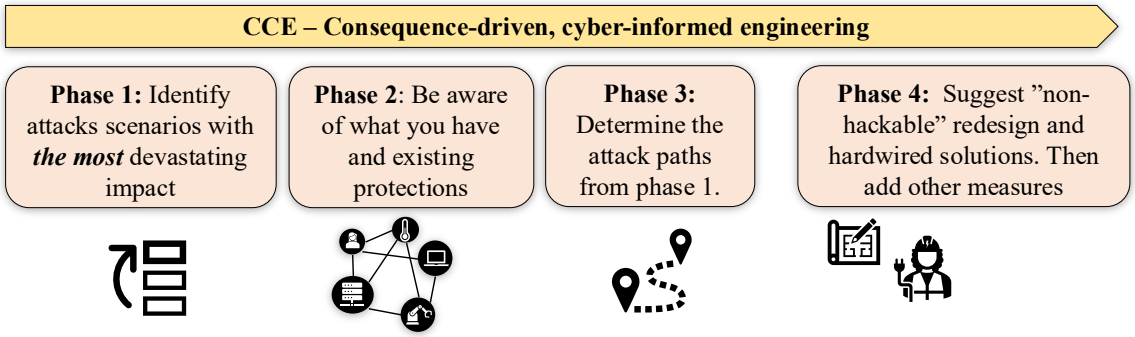


Fig. 39. CCE method (adopted from ind.gov/cce)

The four steps involved are:

- **Phase 1 - Consequence Prioritization:** This step involves identifying the attack scenarios with the most severe consequences, named high consequence events (HCE). The starting point would be to identify the processes that, when manipulated, could cause harm. A scoring method is applied to select those HCE with the highest damage potential.
- **Phase 2—System-of-Systems Analysis:** This phase is about collecting, organizing, and describing the systems that could be involved in the HCE events, their status for how they are being protected today**,** and their potential vulnerabilities. Three block diagrams and system hierarchies are suggested to support the analysis.
- **Phase 3—Consequence-Based Targeting:** This phase tries to determine how the attacker may plan the HCE attacks and what tactics and techniques they might use. The entries, paths, and systems targeted throughout the network should be illustrated in a Purdue-like diagram. CCE applies a variant of the ICS cyber kill chain for visualization.
- **Phase 4—Mitigations and Protections:** This phase involves identifying and deploying measures that can remove or disrupt the HCE attack. Priority should be placed on eliminating or reducing the ability to perform the attack through re-engineering and the use of non-hackable solutions before considering additional cybersecurity measures.

Examples of re-engineering and non-hackable solutions are:

- Replace a pump with a too-high capacity to prevent delivering pressure or composition above what the system downstream can tolerate.
- If the safe state of an energized-to-trip valve is well defined, replace it with a de-energized-to-trip valve.
- Add, for some selected safety functions, a fully hardwired way to isolate or activate power to the equipment so that it enters its fail-safe state. Such solutions are sometimes referred to as non-hackable, as they typically involve only simple electromechanical devices, such as switches, relays, and circuit breakers.
- Install local and, if possible, electromechanical instruments for manual readings of parameters such as level, temperature, and pressure.

Fig. 40 uses a system control diagram (SCD) to illustrate how a non-hackable command-and-actuation system can be added as an alternative route to close the shutdown valve XV-1500 if the emergency

shutdown system (ESD) and the process shutdown (PSD) systems have been manipulated. The ESD and PSD system is assumed to be configured using function blocks defined in IEC PAS 63131 (2017): Two latching blocks (LB), one single binary block (SB), one digital input monitoring block (MB), two Single binary control of pneumatic/hydraulic equipment/valve blocks (SBV), and an OR (O) function (shown inside a circle). One may, for example, assume that the LB output has been manipulated to prevent it from triggering an action.

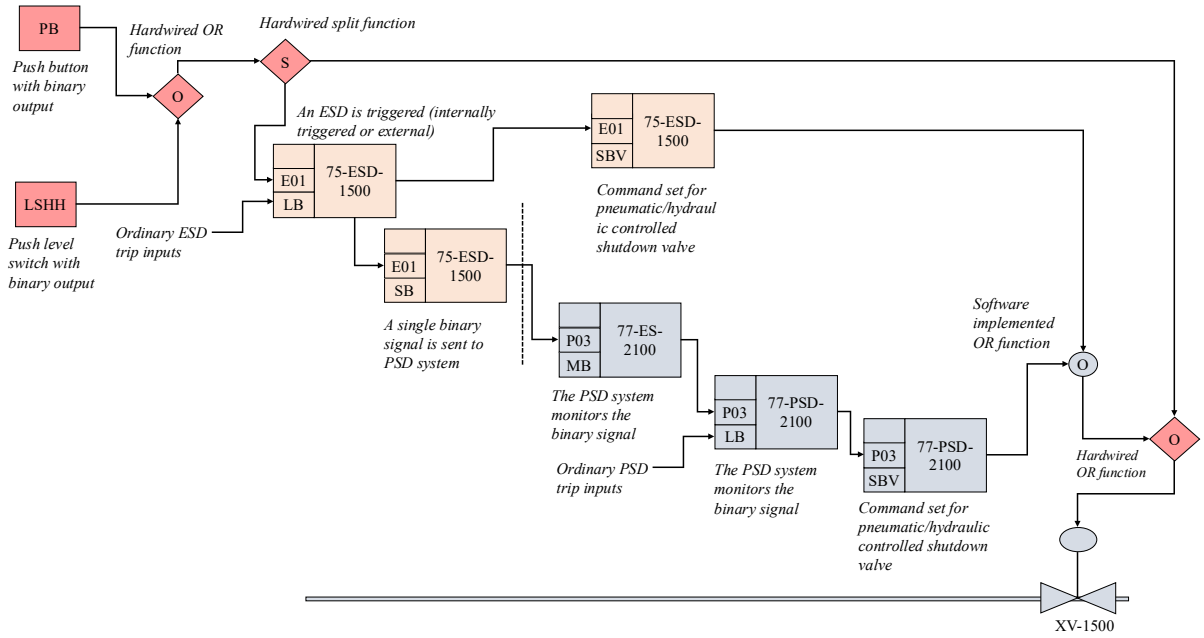


Fig. 40. Introducing non-hackable solution to active shutdown valve

The red symbols illustrate the hardwired (non-hackable) logic: We assume that the push button (PB) and the electromechanical level switch with a fixed setpoint (LSHH) are energized during regular operation, and that power is removed if either is active. Relays and contactors are used to realize the split (S) and OR (O) functions. Here, the diamond symbols indicate that these simple logical functions are implemented in hardware rather than in software (circles). The split function routes the off signal to the ESD logic controller as a backup. However, a manipulated ESD or PSD system cannot prevent the alternative hardwired path from closing the valve.

Also, circuit breakers, which are essential for many safety functions, have built-in software that can be manipulated. Care must therefore be taken to choose as simple (software-independent) circuit breakers as possible.

11.8.6.2 CCE applied to two synthetic facilities

The U.S. Department of Energy has published two reports where the application of CCE has been illustrated:

- Stinky Cheese Company (https://www.osti.gov/biblio/1696803)
- Baltavia Substation Power Outage (https://www.osti.gov/biblio/1645032)

11.9 Overview of organizations

Several organizations monitor cybersecurity at the national and global levels. We will introduce some of these below.

11.9.1 CERTs and publishers of vulnerability alerts

The term CERT stands for computer emergency response team. It is a type of center that assists in monitoring and handling more significant cybersecurity attacks against critical infrastructures. CERTs may publish alerts to companies that are not publicly available, and companies must notify the authorities and involve the relevant CERT if they are subject to attacks. In addition to CERTs, various organizations monitor vulnerabilities, analyze them, and share this information publicly.

In Norway:

- Nasjonalt Cybersikkerhetssenter (NCSC). Norwegian National Centre, which is also an arena for national and international cooperation on cybersecurity management. It hosts the NorCert—Norwegian Computer Emergency Response Team, which handles and coordinates severe cyber-attacks against critical infrastructure and information.
- KraftCERT provides a Cyber response environment for the power and petroleum sectors, but it also supports the process industry, water and wastewater sector, and energy recovery.
- NORMA-Cyber Center that provides services to Norwegian ship owners and other players in the maritime industry.

Outside Norway (but also used by Norwegian industry):

- Dragos – a US company focusing on monitoring threat actors, cyberattacks, and attempts of OT systems, and performing deep analyses of actual cyberattacks. Companies may also use Dragos software tools for inventory monitoring and vulnerability assessment. Dragos publish reports on the threat landscape and statistics about cyberattacks each year.
- CISA - Cybersecurity and Infrastructure Security Agency. The CISA is a US government agency and the national coordinator for critical infrastructure security and resilience. Their ICS-CERT service publishes cybersecurity advisories and alerts related to common vendors and manufacturers of ICS and OT devices and systems.
- US-CERT: US cyber incident response team. Organized under the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA).
- ICS-CERT: US resource center and site for assistance and evaluation of cybersecurity threats and events related to cybersecurity. Organized under US-CERT.

Several organizations publish information about vulnerabilities, for example:

- The CISA ICS-CERT service (already mentioned)
- MITRE, keeping updated the following webpages:
    - CVE – Common Vulnerability and Exposures: A publicly available list (and website) managed that provides unique identifiers for all types of publicly disclosed cybersecurity vulnerabilities. CVE does not store detailed technical information or resolution status; such details are typically expanded in the NIST National Vulnerability Database (NVD). Most CISA alerts reference CVE IDs when available, but they are not automatically stored in CVE. Vendors, researchers, and organizations request or assign CVE IDs through the CVE Program as part of coordinated vulnerability disclosure.
    - CWE – Common Weakness Enumeration: A public list (and website) that categorizes types of software and hardware weaknesses that can lead to vulnerabilities. While CVE identifies specific, real-world vulnerabilities, CWE provides the classification framework for the underlying root-cause weaknesses. CVE records often reference applicable CWE categories to indicate the type of weakness involved.
- The US National Vulnerability Database (NVD):
    - A public database maintained by NIST that provides detailed information (such as CVSS scoring, impact data, and product mappings) for publicly disclosed

vulnerabilities based on entries in the MITRE CVE list. Here, CVSS stands for Common Vulnerability Scoring System, and is a scoring system published and maintained by the non-profit Forum of Incident Response and Security Teams (FIRST), available at FIRST.org. NVD imports all public CVE records, enriches them with additional metadata, and publishes them, although updates may occur with a delay rather than full real-time synchronization.

- Shodan:
  - A webpage operated by a private US-based cybersecurity/internet-intelligence company. It has a search engine for detecting internet-connected devices, which can be useful for checking if there are systems and devices not intended to be publicly reachable.

Some manufacturers also publish the their own vulnerabilities from their company webpages, for example as done by ABB.

Fig. 41 illustrates (in a simplified way) the relationships among CISA-CERT alerts, CVEs, CWEs, and NVD. All vulnerabilities entered as CVEs are also listed in the NVD, though sometimes with a delay. Compared to CVE, NVD adds some additional scores, ratings, and features for advanced search. Both databases are sponsored by the US Department of Homeland Security (DHS) and CICA.

The alerts published by CERT-ICS from CISA are given a reference ICSA-xx(year)-xxx-xx (sequence number). For each alert, the applicable CVEs involved for the specific device are referenced.

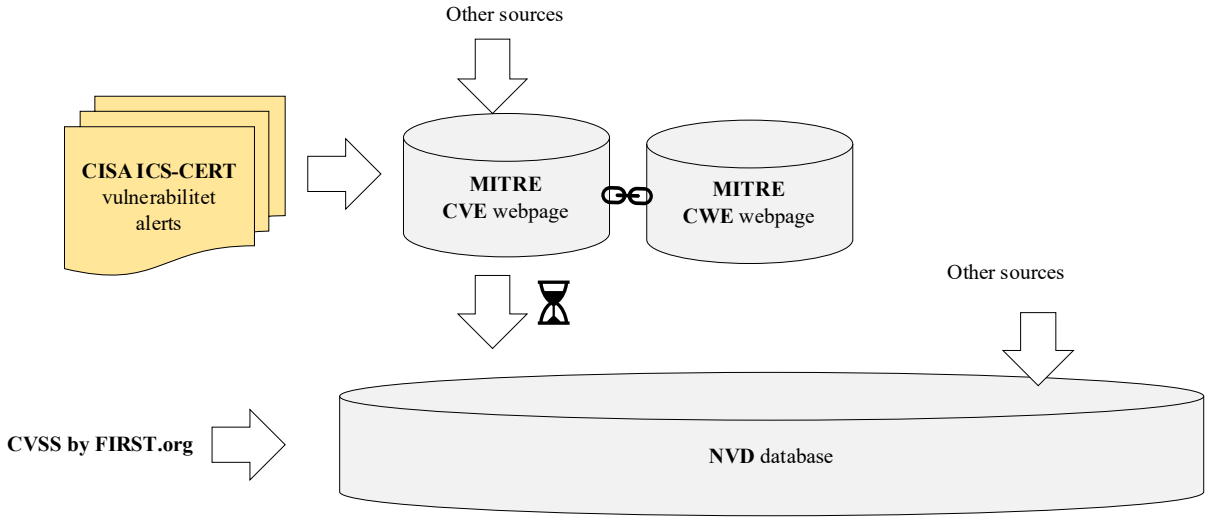


Fig. 41. Relationships between organizations publishing vulnerabilities

11.9.2 Yearly updates on OT cybersecurity threats and attacks

Each year, Dragos publishes a status report titled "ICT/OT cybersecurity Year in review" on attack groups and malware targeting industrial control systems. Dragos is a US-based industrial (OT/ICS/IIoT) cybersecurity company recognized globally. The company publishes many relevant reports, including analyses of actual attacks, and provides services to various industrial companies to monitor the threat landscape and attacks.

In 2022, Dragos drew attention to a new malware called PIPEDREAM, developed by the hacker group CHERNOVITE. It is referred to as malware with advanced capabilities, modularized to take different steps in the attack. Dragos has found that PIPEDREAM can execute 38 percent of known ICS attack techniques and 83 percent of known ICS attack tactics listed in the MITRE ATT&CK matrix. The report continues to state that PIPEDREAM can manipulate a wide variety of industrial control programmable logic controllers (PLCs), industrial software, and can utilize and exploit commonly used industrial

communication standards, such as CODESYS, Modbus, and Open Platform Communications Unified Architecture (OPC UA). So far, Dragos or others have (as of December 2025), to the best of the author's knowledge, as the author read, no known cyberattack using this malware.

11.10 Bibliography

Assante, M. J., & Lee, R. M. (2021). *The Industrial Control System Cyber Kill Chain*. SANS Institute.

Bhunia, S., & Tehranipoor, M. M. (2017). *The Hardware Trojan War: Attacks, Myths, and Defenses*. Springer Cham. https://doi.org/https://link.springer.com/book/10.1007/978-3-319-68511-3

Bochman, A. A., & Freeman, S. (2021). *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE). 1st edition*. CRC Press.

DNV RP G108. (2017). *Cyber security in the oil and gas industry based on IEC 62443*. Det Norske Veritas. https://doi.org/https://www.dnv.com/cybersecurity/recommended-practices/dnv-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

DoE. (2021). *CyOTE Case study: Oldsmar water treatment facility (prepared by Idaho National Laboratory)*. U.S. Department of Energy. https://doi.org/https://inl.gov/wp-content/uploads/2022/04/Oldsmar-CyOTE-Case-Study_508_FINAL.pdf

Dragos. (2017a). *CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations*. https://doi.org/https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

Dragos. (2017b). *TRISIS Malware. Analysis of Safety System Targeted Malware*. https://doi.org/https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

Dragos. (2019). *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. https://doi.org/https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

Dragos. (2020). *Spyware stealer locker wiper: LockerGoga revisited*. Dragos. https://doi.org/https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/

Dragos. (2022). *Analyzing a New Water Watering Hole*. https://www.dragos.com/resource/analyzing-a-new-water-watering-hole/. Retrieved 05.10 from

EU Cyberscurity Act (CSA). (2019). *EU Cybersecurity Act (CSA): Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*. European Commission.

EU Cybersecurity Resilience Act (CRA). (2024). *EU Cybersecurity Resilience Act (CRA): Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)*. European Commission.

EU Directive 2016/1148 (NIS 2 Directive). (2022). *On measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Official Journal of the European Union (OJEU).

Gellner, J. R., & St. Michel, C. P. (2020). *CCE Case Study: Baltavia Substation Power Outage (An Idaho National Laboraty report)*. US Department of Energy & Office of Scientific and Technical Information. https://doi.org/10.2172/1645032.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Haver, M. H. (2022). *Cyber security in industrial control systems: Lessons learnt from past attacks. Specialization project thesis at the Department of Engineering Cybernetics.* NTNU.

Houmb, S. H., Iversen, F., Ewalds, R., & Færaas, E. (2023). Intelligent Risk-Based Cybersecurity Protection for Industrial Systems Control—A Feasibility Study (SPE 217430). *2023 Society of Petroleums Engineers (SPE) journal*.

IEC 62443. (2009–2025). *Security for industrial automation and control systems. Multiple parts, each published separately.* International Electrotechnical Commission.

IEC 62443-3-1. (2009). *Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control system*. International Electrotechnical Commission.

IEC 62443-3-2. (2020). *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*. International Electrotechnical Commission.
IEC 62443-3-3. (2013). *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels (corr. 2014)*. International Electrotechnical Commission.
IEC 62443-4-2. (2019). *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*. International Electrotechnical Commission.
IEC glossary portal. (Accessed 2025). *IEC Products & Services Portal - glossary*. International Electrotechnical commission. Retrieved 15.05.24 from https://products.iec.ch/home
IEC PAS 63131. (2017). *System control diagram*. International Electrotechnical Commission.
IEC PAS 63325. (2020). *Lifecycle requirements for functional safety and security for IACS*. International Electrotechnical Commmission.
IEC TR 63069. (2019). *Industrial-process measurement, control and automation - Framework for functional safety and security*. International Electrotechnical Commmission.
IEC TS 62443-1-1. (2009). *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*. International Electrotechnical Commission.
INL. (2020). *Consequence-driven Cyber-informed Engineering (Phases 1- 4)*. Idaho National Laboratory.
ISA TR 84.00.09. (2017). *Cybersecurity Related to the Functional Safety Lifecycle*. International Society for Automation.
Iyengar, A., & Ghosh, S. (2017). Hardware Trojans and Piracy of PCBs. . In S. Bhunia & M. Tehranipoor (Eds.), *The Hardware Trojan War: Attacks, Myths, and Defenses*. Springer Cham. https://doi.org/https://doi.org/10.1007/978-3-319-68511-3_6
Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Forrester.
Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348
Mandiant webpage. (2022). *TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping*. Retrieved 05.10 from
matrix, M. d. (Accessed 2024). *https://d3fend.mitre.org/*.
MITRE attack matrix for ICS. (Accessed 2024). *https://attack.mitre.org/matrices/ics/*.
NIST Cybersecurity Framework 2.0. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute for Standards and Technology. https://doi.org/https://www.nist.gov/cyberframework/framework
NIST glossary. (Accessed 2025). *https://csrc.nist.gov/glossary*. National Institute of Standards and Technology, division Computer Security Resource Center (CSRC). Retrieved 15.05.24 from https://csrc.nist.gov/glossary
NIST Guide on OT Cybersecurity SP 800-82. (2023). *SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security*. National Institute of Standards and Technologies. https://doi.org/https://doi.org/10.6028/NIST.SP.800-82r3
NOU. (2015). *NOU2015: 13 Digitale sårbarheter - sikkert samfunn*. https://doi.org/https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/
NSM. (2020). *NSM Grunnprinsipper for IKT-sikkerhet. Versjon 2.0.* Nasjonal Sikkerhetsmyndighet.
Offshore Norway (ON) guideline 104. (2026). *Recommended guidelines on cyber security baseline requirements for Operational Technology systems*. Offshore Norge.
Reason, J. (1990). *Human error*. Cambridge University Press.
The Langner Group. (2013). *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. https://doi.org/https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
Vartdal, L. (2025). *Development of an OT Simulation Platform for Executing Cyber Attack and Implementing Intrusion Detection Strategies (master thesis)*. NTNU (https://hdl.handle.net/11250/5369349). https://doi.org/https://hdl.handle.net/11250/5369349

Wetzels, J., & Krotofil, M. (2019). *A Diet of Poisoned Fruit: Designing Implant and OT payloads for ICS Embedded Devices*. Secura.

Øien, K., Jaatun, M. G., Thieme, C., Grøtan, T. O., Gnanasekaran, V., & Lundteigen, M. A. (2025). *Guidance on integrated safety and cybersecurity barrier management (Report 2025:01073)*. SINTEF.