CHAPTER 1
INTRODUCTORY TOPICS

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 an industrial control system?
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

1 Introduction to instrumentation systems and safety

This is the first of 12 chapters in a course compendium for TTK 4175 Instrumentation Systems and Safety, developed specifically for students in bachelor's and master's programs in Engineering Cybernetics at the Norwegian University of Science and Technology (NTNU). However, the course compendium aims to achieve wider outreach.

This first chapter introduces a few of the fundamentals of instrumentation systems, emphasizing their role in industrial automation and safety. It outlines key concepts, including the instrument loop, controller types (e.g., PLCs and DCSs), and the reasons why safety instrumented systems (SISs) must be independent of controllers used for regular (normal) operation. The chapter also explores how instrumentation integrates with systems engineering and sustainability goals. The engineering and operational lifecycle is briefly introduced, including verification, validation, and stakeholder involvement. Furthermore, it provides an overview of relevant regulations, EU directives, and standards, with a focus on Norwegian and European contexts. Practical guidance on CE marking, harmonized standards, and sector-specific frameworks is also included.

1.1 Abbreviations

ANSI	American National Standards Institute
CE	Conformité Européenne
DCS	Distributed control system
DMZ	Demilitarized zone
CE	Conformité Européene
CEN	Comité européen de normalisation
CENELEC	Comité européen de normalisation en électronique et en électrotechnique
DIN	Deutsches Institut für Normung
EN	European Norm
ESD	Emergency shutdown system
ETSI	European Telecommunications Standards Institute
F&G	Fire & Gas
FW	Firewall
HMI	Human-machine interface
IEC	International Electrotechnical Commission
IMS	Information management system
ISA	International Society of Automation (I
ISO	International Organization for Standardization
IT	Information technology
PCS	Process control system
PLC	Programmable logic controller
PSD	Process shutdown system
OT	Operational Technology
RTU	Remote termination unit
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirements specification

1.2 What is an instrumentation system?

An instrumentation system is an integrated arrangement of sensors, actuators, control logic, communication, power supply, and operator interfaces, designed to monitor, measure, and control physical processes, enabling safe, reliable, and efficient operation in accordance with stated requirements and within defined functional and environmental limits.

Instrumentation systems are applied across all industries and at various scales, from ships and aircraft to manufacturing facilities and processing plants.

The term "control" encompasses devices necessary to interact with the controlled process or system and typically includes programmable controllers, hardwired logic using relays and contactors, and actuated devices such as electrically, pneumatically, and hydraulically operated valves. Control may extend beyond normal operations, such as responding to hazardous events during abnormal situations. To distinguish between the two, we often differentiate between a *process* (or regular) control system, which manages normal operation, and a safety-instrumented system (SIS), which manages abnormal situations. The term “safety” is included in the course title to emphasize the additional focus on how SIS systems are built and managed, with consideration of the requirements and restrictions imposed by regulations and standards.

The more specific topics covered in the course are:

- Industrial communication and network architectures, explaining how the systems interact with each other and the environment
- Control room layout and alarm system design, to enable humans with the necessary oversight and ability to intervene
- Technical documentation, explaining how the systems are built, installed, and operated
- Industry 4.0 data exchange platforms, like OPC UA, to explain principles for how data from the factory floor level is shared with systems outside the factory networks
- Risk analysis, focusing on identifying hazards and risks that need to be managed in system design and through safety measures
- Key attributes of safety-instrumented systems, our focused type of safety measure, and how they differ from (closed-loop) control systems
- Functional safety, focusing on the requirements placed on design processes, architecture, and reliability assessments of safety-instrumented systems
- Fire and gas detection, a specific type of safety-instrumented system involving various fire and gas detection technologies
- Machinery safety, placing requirements on how machines are designed to avoid harm to people
- Cybersecurity, addressing how instrumentation systems can be attacked and how such attacks can lead to loss of safety
- Explosion-proof design, explaining design principles for electrical equipment placed in areas with an explosive atmosphere

Most examples and practices are anchored in the process industry. Several examples are drawn from the petroleum sector, as many of its design and operating practices have been shared openly. However, the concepts, methods, and theories are transferable to other industries, e.g., nuclear power facilities, hydrogen generation facilities, carbon capture, railway, maritime, and manufacturing.

The course aims to balance broad outreach so students can understand how topics relate to one another with deep dives into selected topics so students can learn specific methods, skills, or abilities to participate in and lead activities as automation engineers.

The rest of this chapter provides further insight into the scope and focus of the course before moving on to introductory concepts in instrumentation systems and to how regulations, EU directives, and standards govern their design and operation.

1.3 Relationship to systems engineering and sustainability

This course is part of the systems engineering discipline. According to the International Council on Systems Engineering (INCOSE), systems engineering is “a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods.” In essence, systems engineering applied to instrumentation systems covers:

- Establishing requirements: What requirements are applicable, and how are they anchored, such as in e.g., standards and analyses?

- Development of system architecture and choice of applicable solutions: What technologies are involved, what impacts the choice of solutions, and what phases are involved?
- Managing systems during the operational phase: What is the role of performance monitoring, diagnostics, and maintenance?

In all these areas, verification and validation are essential: verification ensures that the stated requirements are met, while validation assesses whether the requirements are correctly identified and sufficiently complete.

Systems engineering embraces a multidisciplinary approach, which is essential throughout all phases of designing and operating an instrumentation system. For example, it involves coordination across fields such as electrical engineering, automation, information and communication technology (ICT), mechanical engineering, process engineering, technical safety, and cybersecurity. Moreover, successful implementation requires collaboration between professionals with practical, hands-on experience, such as technicians and control room operators, and those responsible for planning and oversight, typically engineers.

Sustainability and sustainability goals are high on the agendas of society and companies. The 17 UN Sustainable Development Goals target many areas, ranging from climate action to creating a better society. The European Commission has introduced an EU taxonomy for sustainable activities anchored in the EU taxonomy regulation published in 2020. This regulation specifies how European economic activities must document their contribution to the six environmental objectives, as explained in more detail at https://ec.europa.eu/sustainable-finance-taxonomy/.

Some suggestions on how this course contributes to sustainability include:

- Many industries essential for society, including renewable energy production, involve activities and processes that have the potential for accidents if the risks are not adequately managed. The risks may involve natural hazards, foreseeable human error, or intentional acts by malicious individuals.
- Instrumentation systems are essential in detecting process upsets and interacting with the events before they can develop into accidents.
- The way we secure instrumentation systems against external threats is essential to maintain the instrumentation systems' effectiveness.

In this way, automation engineers may also contribute to the safe and secure design and operation of industries.

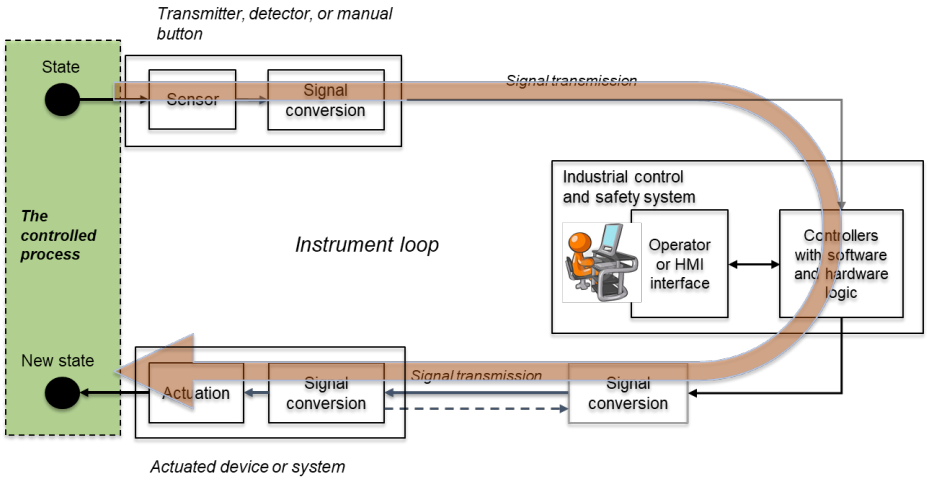

Fig. 1. Instrumentation loop (high level)

1.4 Instrument loop

An instrumentation loop (Norwegian: instrumentsløyfe), is dedicated to a specific function, begins with one or more sensing devices (such as transmitters or detectors) that convert physical phenomena into measurable signals, includes the transfer of these signals and control commands through communication paths, and ends with the corresponding actuated devices that influence the controlled process, as shown in Fig. 1.

Devices are called field devices because they are installed directly in the operational environment ("in the field"), close to the physical process they monitor or control, rather than in a centralized control room. Their location enables direct interaction with process conditions such as temperature, pressure, or flow.

Sensing devices can also be referred to as input elements, sensors, transmitters, and detectors, depending on the context. Regardless of the term, we recognize that such devices consist of a sensor that interacts with the physical environment and a transmitter that converts the signal to the format required for communication.

Fig. 2 identifies additional equipment within the instrument loop, for example:

- Junction boxes: These field (outdoor) enclosures provide housing for intermediate connection points for cables and wires. A cable may consist of multiple wires, some for signaling and others for power supply and earthing. Inside the junction box are terminal blocks where individual wires are fastened on one side and cross-connected with wires on the other. Fig. 2 illustrates how technical drawings can mark how many wires enter and exit a junction box. The transmitter signal is sent through a two-wire cable, then transferred to two new cables: one with 12 wires and another with 36 wires.
- Cabinets: These are indoor enclosures equipped with terminal blocks to connect incoming cables, controllers, and power supplies. They are generally much larger than junction boxes and do not require the same dust- and waterproof enclosures as outdoor junction boxes. Fans are typically needed to ventilate the heat generated inside the cabinets.

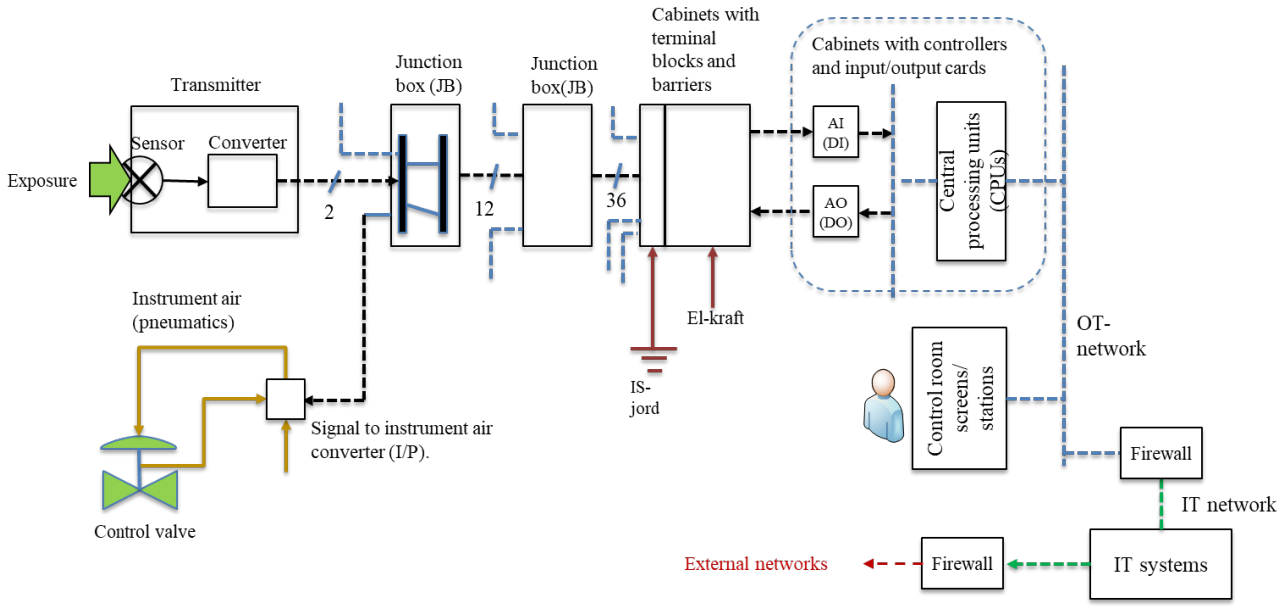

Fig. 2. Instrumentation loop (a more detailed level)

Fig. 2 identifies that all devices in the instrument loop, including the control room, connect to the operational technology (OT) network. The OT network is separated from the information technology (IT) network using one or more firewalls. Direct remote access to the OT network is usually not permitted, but it may be granted via the IT network after authentication and authorization.

1.5 Industrial controller types – PLC and DCS

Industrial controllers specialize in real-time operation in exposed industrial environments. There are two categories of controllers:

- Industrial programmable logic controllers (PLCs): These were initially made to operate standalone systems.

- Distributed control systems (DCS): These are specially built to operate and synchronize controllers distributed over an entire facility. The term "distributed" refers to a combination of central and remote (distributed) controller nodes, enabling greater, more scalable control capacity than PLCs.

PLCs' functionality and capacity have increased over the years, and the distinction between DCSs and PLCs is less evident.

For example, ABB refers to the AC 500 as its PLC product family, targeting industries such as water, tunnels, building infrastructure, machinery, handling, marine, food, and beverage. The AC 800xA is their DCS product family, covering many of the same industries and electrical control and monitoring systems. Siemens refers to SIMATIC PCS 7 as its DCS family, while its PLC product family includes SIMATIC S7 (large-scale systems) and LOGO (compact controllers).

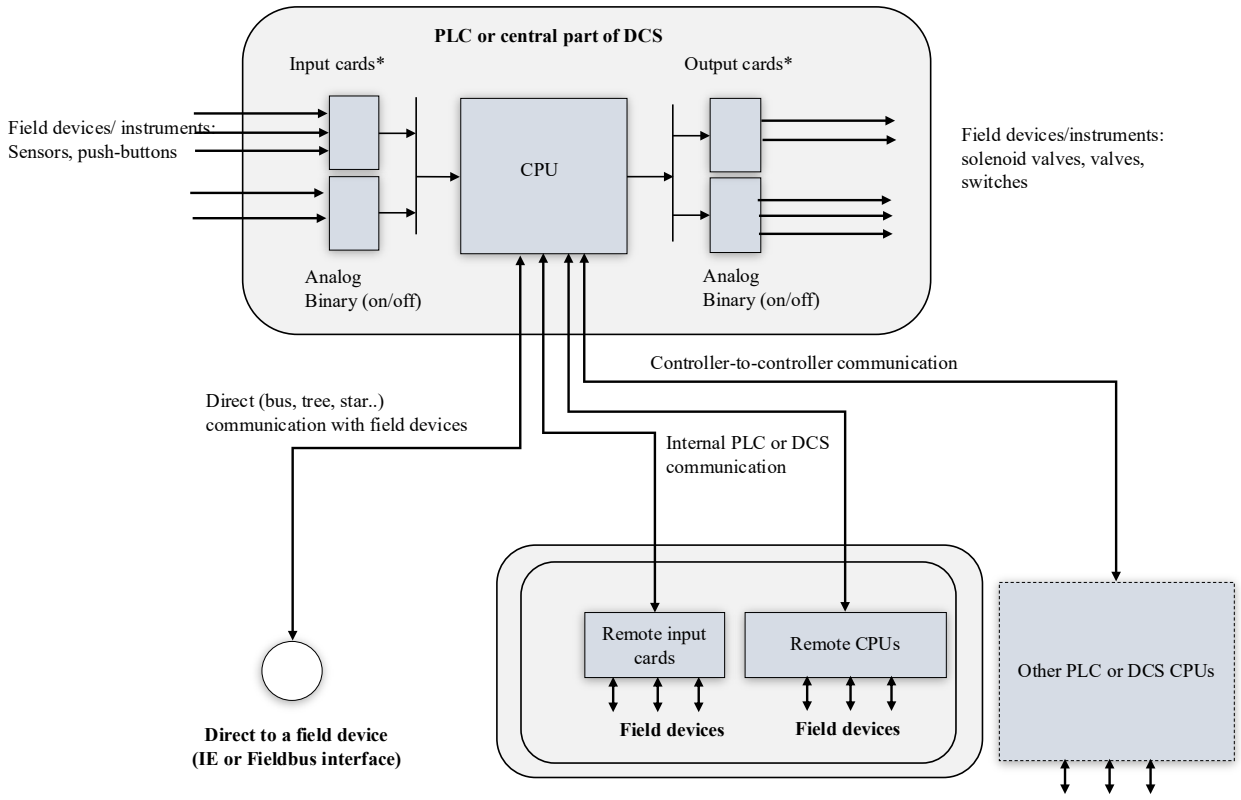

Fig. 3. Principle layout of a CPU and input/output cards

Fig. 3 illustrates the main components of a PLC and a DCS: input and output cards and one or more central processing units (CPU) connected via an internal bus that may be proprietary and with interfaces to other devices and systems using standardized communication, such as Fieldbus, Industrial Ethernet, or analog current and binary (on/off) voltage signals.

The CPU and I/O cards are often mounted in a rack inside a cabinet, along with the power supply and other modules. In the rack, the components are mounted side by side, as illustrated in Fig. 4. The electrical connection board to which the units are connected is often called the backplane.

When DCS and PLCs are integrated to form larger control and safety systems, they are sometimes referred to as:

- Safety and automation system (SAS), industrial control and safety system (ICSS), or just industrial control system (ICS): This term is primarily used for the control and safety systems for individual

facilities, with local and sometimes also remote control rooms, covering Purdue levels 0-2. SAS is a commonly used term in Norway's offshore oil and gas industry, whereas ICS and ICSS are more commonly used outside Norway and in several international standards.

- Supervisory control and data acquisition (SCADA) system. The term SCADA is used with at least two different meanings:
  - Referring to the supervisory level (Purdue level 1-3) that connects several PLCs and DCSs across a wide area, or across multiple facilities. The core components are then operator stations, other human-machine interface (HMI) systems, remote terminal units (RTUs), and servers (for access to real-time data, historical data, trends, events, and the like). RTUs may be regarded as remote CPUs specialized in interfacing with DCSs and PLCs.
  - Referring to all systems needed for the operation of larger and wide-area facilities, covering Purdue levels 0-2/3.

  In Norway, the term is often used for land-based process plants and for electrical power distribution facilities, but is less common for offshore oil and gas facilities.

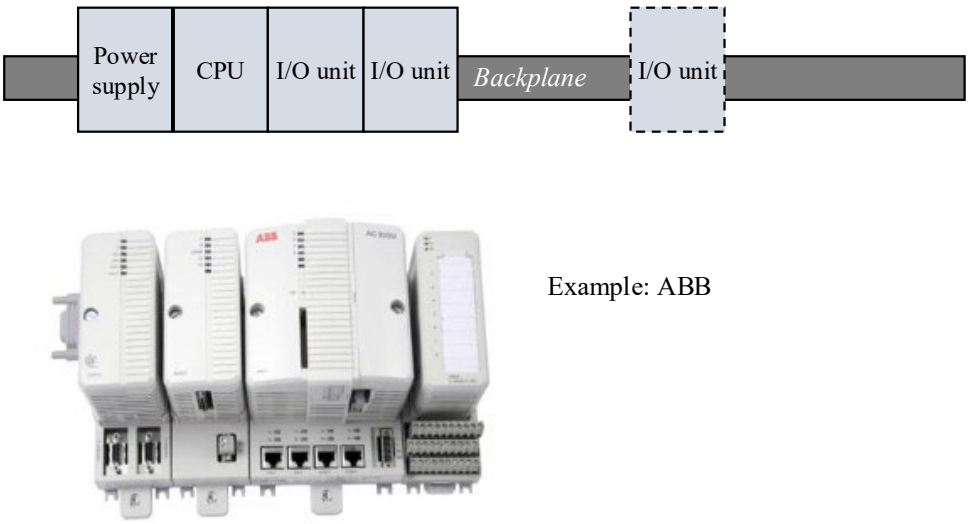

Fig. 4. Principle layout mounting of PLC and DCS in a cabinet

1.6 What is a safety-instrumented system (SIS)?

Safety, as defined by the IEC glossary, is freedom from risk that is not tolerable. Intolerable risk can concern unacceptable harm to people, the environment, or assets of high importance to society. Instrumentation systems dedicated to detecting and responding to abnormal events, such as process upsets not managed by the process control system (PCS), fires, and gas leaks, are called safety-instrumented systems (SIS).

A facility often has several SISs to organize safety functions according to their overall purpose. For example, most process facilities have SIS systems named process shutdown system (PSD) that stops parts of the process in response to a process upset, emergency shutdown system (ESD) that take a more global set of actions beyond shutting down, such as depressurizing confined volumes of gases and removal of ignition sources, and a fire and gas (F&G) system that, besides detecting, also activates extinguishing systems.

A SIS differs from many of the characteristics of a typical process control system. With a basis in Fig. 5, examples include:

- Most SIS systems perform their tasks rarely, while PCS operates continuously. Unlike PCS systems, most SIS systems are dormant (passive) during normal operation but are always ready to act “on demand.” During normal operation, SIS systems usually only monitor and do not perform any actions if they are of the type “on demand” (act only when needed). The term “demand” refers to the specific abnormal events that the SIS shall respond to, and “on demand” may be interpreted as “act when needed.” Examples of SIS functions include:

- Stopping the flow of liquids and gases into a tank if the tank pressure or level exceeds what is normal or allowed.
- Disconnecting and isolating power supplies to all electrical equipment in the event of a fire or gas leakage to remove ignition sources.
    - Starting fire pumps and other extinguishing equipment if fire or smoke is detected.
- SIS systems must be able to perform their tasks regardless of the status of the control systems: A failure of the PCS system can be one of the reasons why a SIS needs to act. Therefore, the SIS must be independent of the PCS system, meaning it should not be affected by any failure in the PCS's hardware or software. Independence of systems can be implemented by physical separation, logical/software separation, or functional separation.

- SIS systems are subject to stricter regulations than PCS**:** SIS systems protect against accidents, and the failure of one or more SIS systems can lead to higher risks to people, the environment, and other vital assets. Compared to PCS systems, SIS systems are subject to more regulations and international standards that impose requirements and restrict their design freedom.
- SIS systems must be independent of other systems: SIS systems must be independent of PCS, so that a fault in the PCS does not impact the ability of SIS to respond. In addition, each SIS must be sufficiently independent of the others. PSD, ESD, and F&G each play a role and are needed at various stages of an accident's development. For example, a process upset not managed by the PSD system will require the ESD system to shut down the entire plant. If the process upset develops into a gas release, the F&G system must detect the situation, notify the ESD system, and initiate necessary extinguishing systems. A failure of the PSD system (or any other) must not adversely affect the others, and likewise for ESD and F&G.

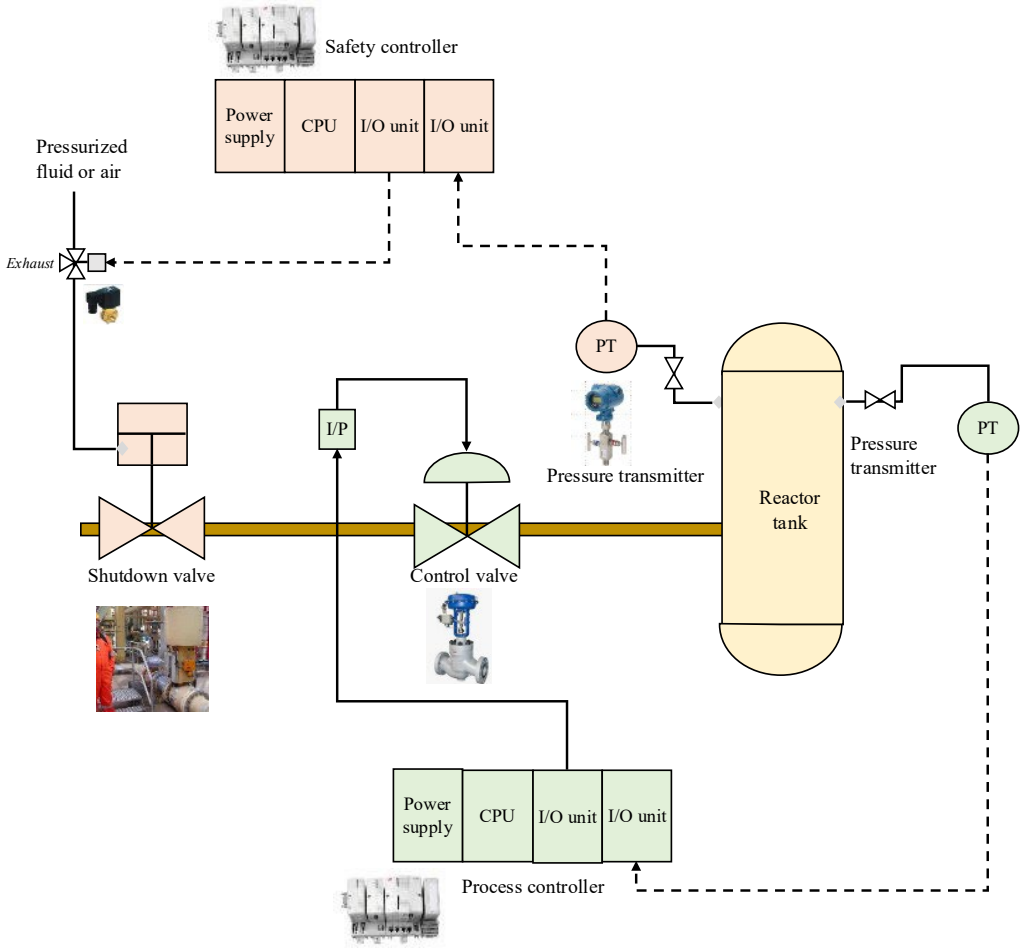

Fig. 5. Illustration of PCS vs SIS (relative sizes of devices not drawn correctly)

In summary, we may consider the following differences between PCS and SIS:

SIS	PCS
• Activated upon demand, either seldom, often, or continuously • Function is not "closed loop" control, but represents an action that is completed when the system enters the safe state • The consequence of SIS failure can be an accident • SIS systems must be independent from other systems, both PCS and other SISs. • Both devices and complete systems are subject to additional safety-related requirements in standards and regulations	• Continuous closed-loop control or activated as needed under normal operating conditions • Control failures can cause abruption of the process • Relies on safety systems to take over when there is a loss of control

Consequently, we may simplify the ideal independence of SIS and PCS as illustrated in Fig. 6.

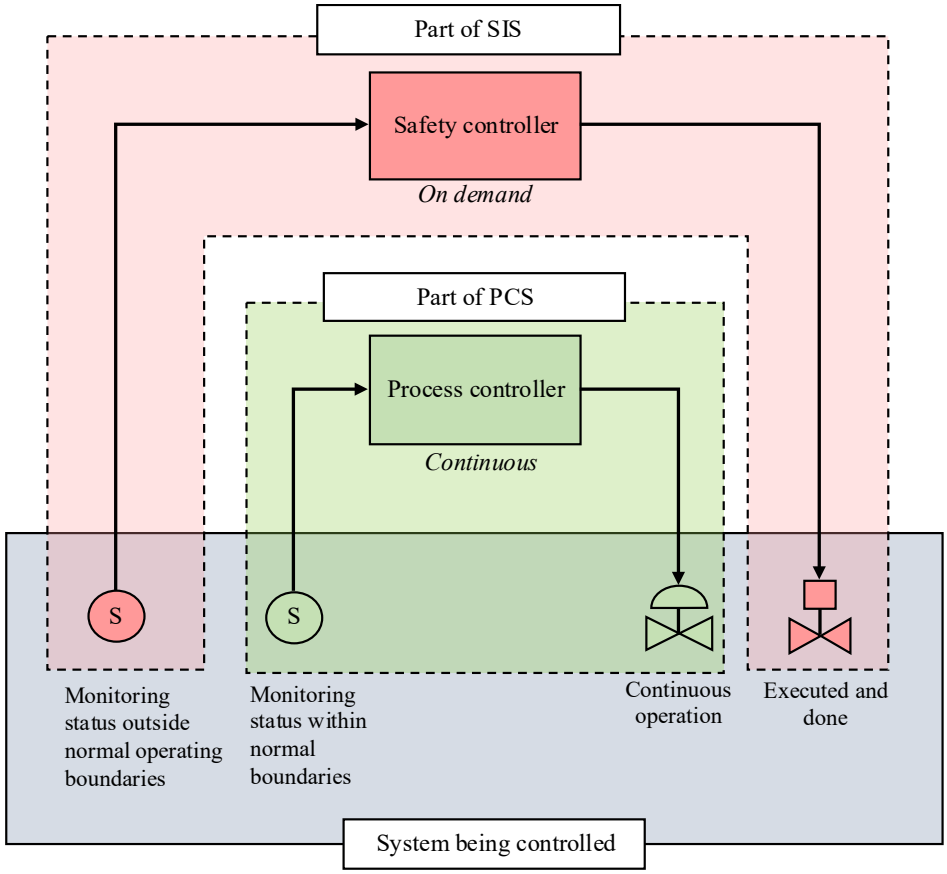

Fig. 6. Alternative visualization of ideal independence between PCS versus SIS

1.7 Overall network architecture

The overall network architecture of an industrial facility is divided into layers according to the Purdue Reference Model or the ISA 95 model. The typical layers are shown in Fig. 7, starting with level 0, which includes devices that interact with the process or system being operated. Professor Theodore J. Williams from Purdue University introduced the name "Purdue" as part of his work with members of a university-industry collaboration. Between

1990 and 1992, they published a layered architecture of networks that share data from the factory floor up to the enterprise or business level.

Years later, Working Group 95 in the International Society of Automation (ISA) developed a new standard, ANSI/ISA-95.00.01-2010, titled "Enterprise-Control System Integration - Part 1: Models and Terminology," building upon the principles of the Purdue model. The ISA standard was later republished as an IEC standard under the name IEC 62264-1 (2013), but the name ISA 95 model has persisted.

Network layers are often grouped into two sections: OT and IT. OT is an abbreviation for Operational Technologies and encompasses all networks and connected devices used to operate and monitor the plant.

> *Operational Technology (OT): Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events [Gartner Glossary]*

Information Technology (IT) encompasses all computers, servers, and networks within the asset owner's office environment. The term is widely used among cybersecurity professionals to distinguish systems involved in plant operation from office networks.

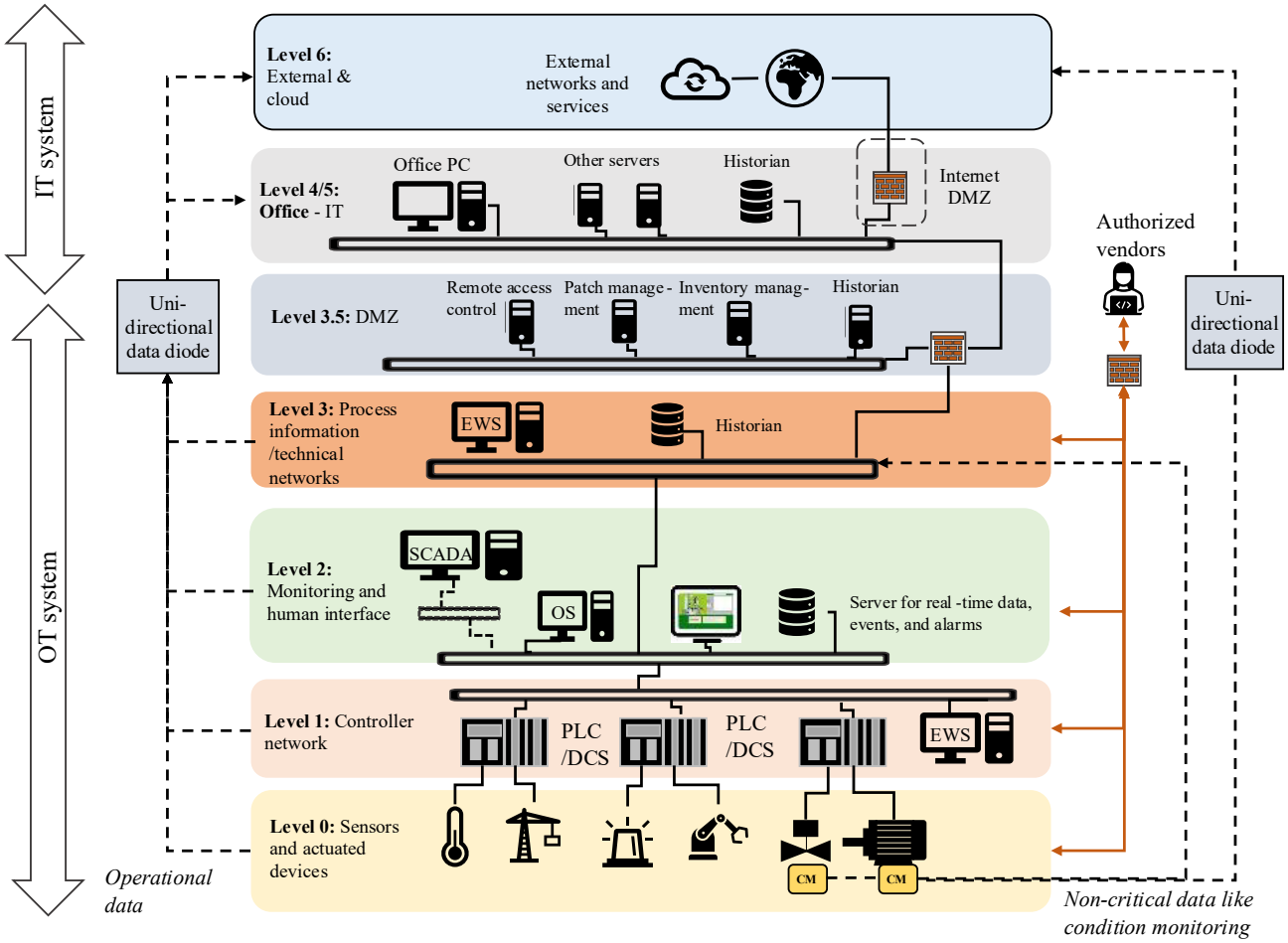

Fig. 7. Purdue (or ISA-95) reference architecture

Before the 1990s, OT networks were often physically separated from IT networks, primarily because the technologies involved could not communicate. However, with the emergence of the internet and the use of more commercial-off-the-shelf (COTS) components in control rooms, servers, network components, and information

management systems, it became possible to connect them, sometimes without awareness. The enterprise/business side also expected greater access to operational data to support decision-making and monitoring. This led to new services, such as remote access support for OT upgrades and problem-solving. Instead of preventing IT and OT from connecting, the focus shifted to securing and authorizing these connections and subjecting them to strict rules and procedures.

The layers explained in more detail are:

OT network levels:

- Layer 0: Includes the sensors and actuators with network and signaling installed within the controlled process.
- Level 1: Controllers, I/O cards, network devices, servers, and cabling. May include engineering workstations (EWS) for accessing controllers, but they could also be in level 3. Controllers with I/O cards can be DCSs, PLCs, or a combination of both.
- Level 2: Operator interfaces such as operator stations, wall displays, panels, servers, network devices, and cabling. The network at level 2 can extend to supervisory control and data acquisition (SCADA) systems that encompass multiple systems or facilities.
- Level 3: Network for process information gathering, optimization, and technical support. Examples of systems include an information management system (IMS) that collects information from systems at levels 0-2 control systems, other servers for data storage and exchange, and a domain name server (DNS) that tracks IP addresses within the OT system. EWSs may also be installed at this level. Condition-monitoring data, not involved in the direct operation of the process or systems, is often linked directly to level 3 to avoid overloading the networks at levels 0-2 that support real-time and time-critical operations.
- Level 3.5: This level is the network and equipment where IT connects to the OT system. The network is named a demilitarized zone (DMZ). NIST glossary (Accessed 2025) defines DMZ as:

  > *DMZ: A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted.*

  All network traffic between OT and IT systems must pass through the DMZ. A general rule is that no network traffic can go directly between OT and IT; it must be routed through a server in the DMZ. One or more firewalls control the data traffic to and from the zone. The DMZ includes various systems for controlling access to the OT system and managing security upgrades (patch management).

Some literature refers to layers 0-2 networks as the process control network, while levels 3 and 4 are called the process information network. An instrumentation system covers levels 0-2, while level 3 consists of supporting systems, such as data aggregation and storage servers.

IT network levels:

- Level 4: Office network at a specific facility
- Level 5: Overarching office network interfacing several facilities
- Level 6: External networks and clouds external to the company but with valid entry points

The networks are not always organized this systematically, and some prefer not to. However, the model remains useful for identifying the core functions. One specific challenge of the Purdue reference architecture is that it (originally) suggests that all data must traverse layers between systems that exchange data. Therefore, as shown in Fig. 7, the network topology needs to accommodate more efficient, large-scale data exchange between the lower levels, IT, and the cloud. For example, some applications on the OT side rely on calculations and analyses made in cloud applications. This is not ideal, but part of a megatrend that the OT network may have to accommodate without compromising safety and security.

- The OT network has alternative data exchange paths that need to be secured from any level on the OT side and “upwards”. It is vital that all of these are identified and properly managed, and that no such paths have been “accidentally” or willingly added.

- For monitoring purposes, the data exchange should ideally be guaranteed to be unidirectional, sometimes achieved with a unidirectional data diode.
- Bi-directional data exchange requires a higher level of security, with authentication, authorization, and encryption.

Yet, many plants require that certain tasks, such as reconfiguration of field devices and updating PLC or DCS application programs, be carried out locally at the plant with written permission, similar to a work permit that applies to all kinds of work at a facility. Instead of the layered approach, the topology can, at least for parts of the network, resemble a star topology, connecting several zones to a common gateway or firewall.

The layered network architecture is applied in several international standards, e.g., IEC 62264-1 (2013) on Enterprise-control system integration, IEC 62890 (2020) on Industrial-process measurement, control, and automation - Life-cycle management for systems and components, and IEC 62443, which focuses on OT systems' cybersecurity requirements, adopts the Purdue model's principal layout. It is this latter standard that has introduced level 3.5 (DMZ). Variants are also found in recognized guidelines, such as NORSOK I-002 (2021), NIST Guide on OT Cybersecurity SP 800-82 (2023) and DNV RP G108 (2017). It also reflects the general automation pyramid shown in Fig. 8, a conceptual, simplified model of the hierarchies of systems and technologies, in which the width of each layer is proportional to the volume of data handled at that level. Level three is sometimes referred to here as the manufacturing execution system (MES), which focuses on optimizing and coordinating operations occurring at the lower levels of the automation pyramid. Level four refers to enterprise resource planning conducted offline, separate from production, for business processes and enterprise-wide planning.

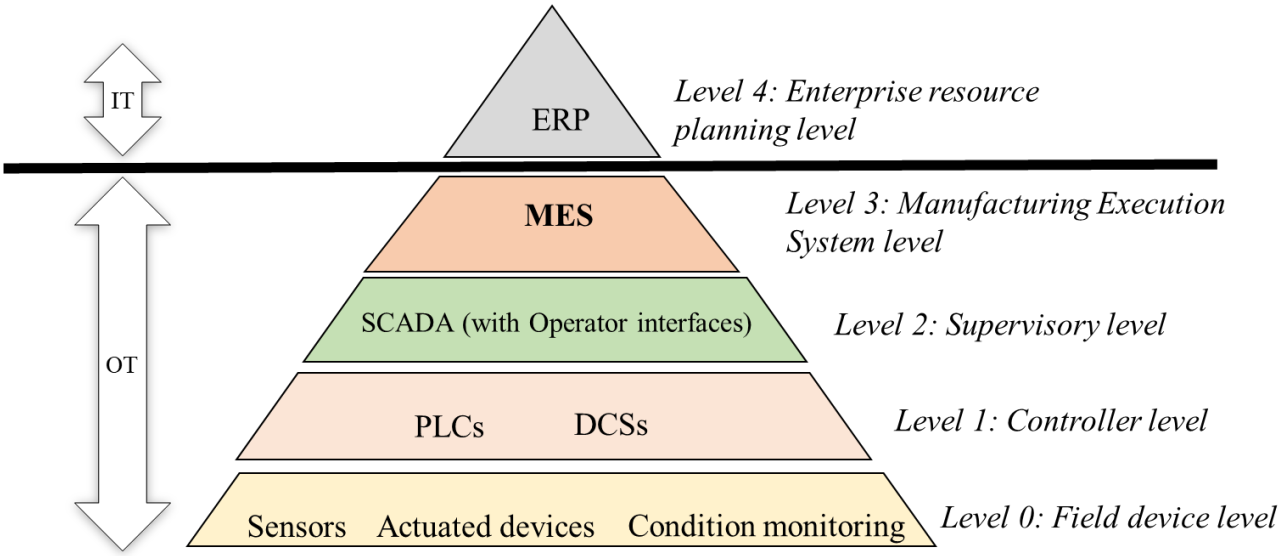

Fig. 8. Automation pyramid

Joint industry initiatives, such as Industry 4.0, aim to enable a more standardized, seamless exchange of data and formats independent of manufacturers' hardware and software platforms. For example, protocols and information models that seamlessly transport, organize, and populate data from the field to the cloud.

Nevertheless, many facilities will have a mixture of old and new equipment. Even new facilities put into operation today may have equipment that is 3-4 years old, depending on when it was ordered. Facilities that are 15-20 years old today, which is not a significant age, may have equipment that has not been replaced since then. Planning and replacing equipment are often resource-intensive (and therefore costly) and may require unacceptable production downtime. For example, replacing a control system at a process facility may cost several hundred million Norwegian Kroner if the plant is large and complex.

An illustration of a typical facility network architecture is shown in Fig. 9 (excluding level 0). Some explanations have been added to address the difficulty in reading the details. At the bottom, we find all level 1

controllers, including ESD, F&G, PSD, PCS, subsea PCS, and compressor/generator/HVAC controllers. These are connected to a redundant ring network using Industrial Ethernet. The PCS system connects several remote cabinets with remote I/O cards (this detail is intricate to read) using Profibus or Modbus. We also observe that the F&G controller connects to a fire panel (or central) with its loop, where fire and gas detectors are connected.

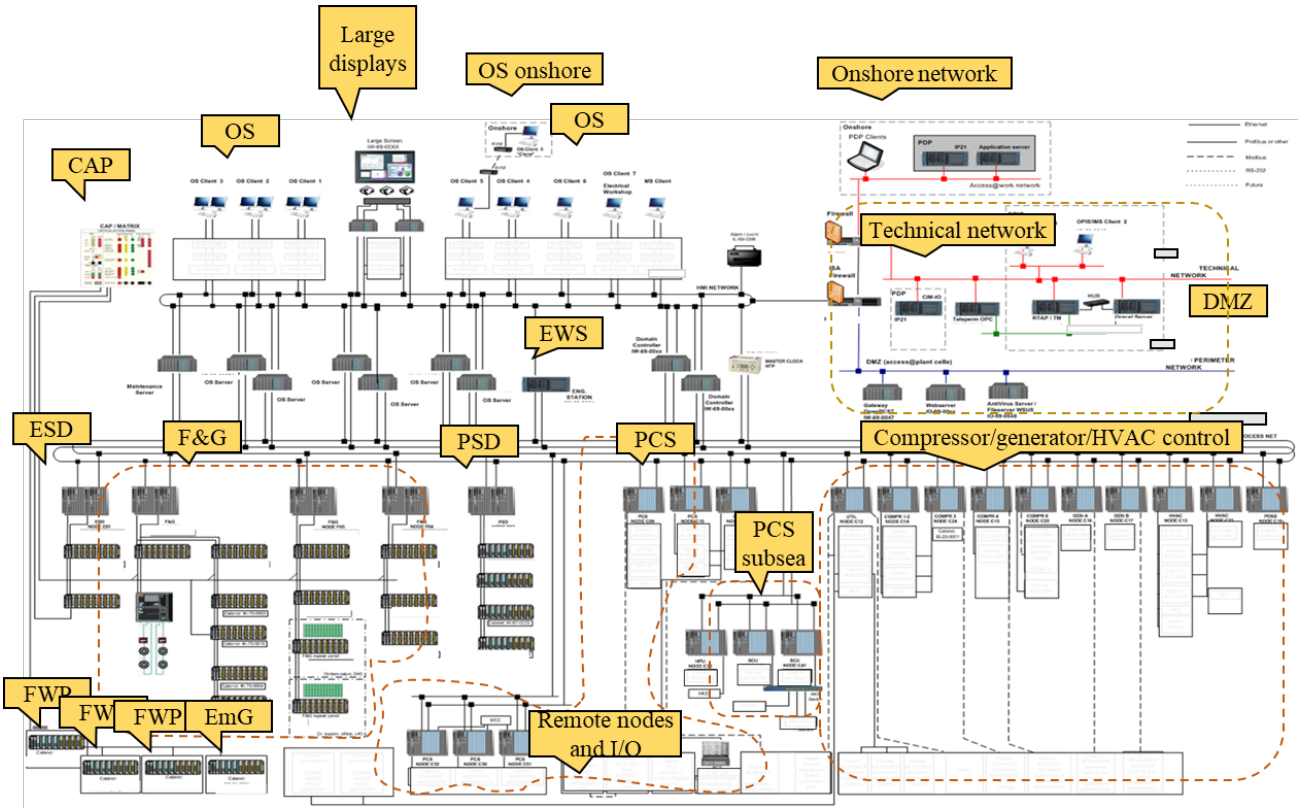

Fig. 9. Network architecture of an oil and gas facility (used with permissions from Siemens)

At the top left, we find layer 2 with the operator stations for monitoring and control. A single-ring network connects several operator stations (OS), which are operator (PC) screens for monitoring and interaction, via Ethernet.

Servers aggregate monitoring data and events, which operator stations (as clients) can access. All real-time communication relies on Industrial Ethernet routed over the same network cables. Layer 2 also includes the Critical Action Panel (CAP), installed in the control room. The CAP is wired directly to input cards for controllers at level 1; however, it is not detailed whether the signals are digital protocols, on/off signals, or a combination.

An Engineering Workstation (EWS) has been placed between network layers 1 and 2, rather than having separate EWSs at these levels. One explanation is that this architecture is a few years old and was designed before newer network segmentation practices aimed at improving cybersecurity were established. Level 3.5, the DMZ, is marked on the right (middle) and placed behind a firewall that controls traffic between the IT system (office networks) and the OT system via Ethernet. A technical network (usually level 3.0) is also placed behind a firewall. The network appears to be on the IT side, as expected. One explanation is that the architecture reflects the fact that less data had to be transported between the OT and IT sides.

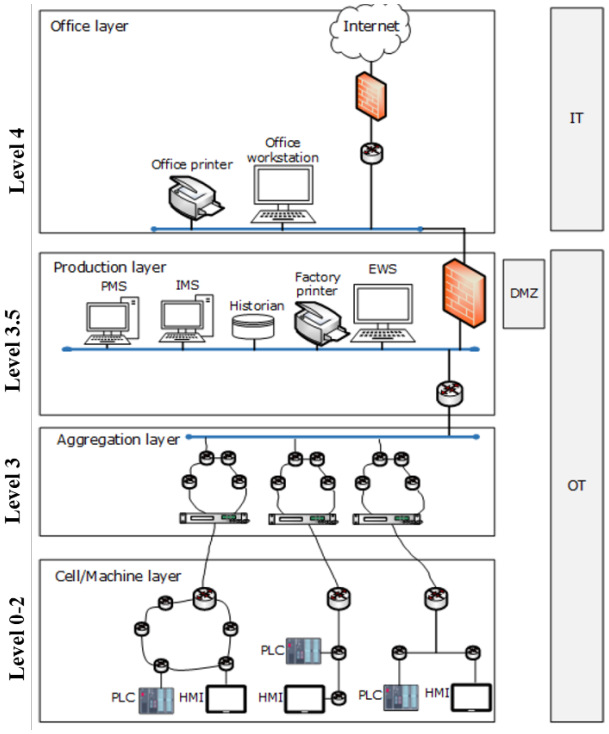

Fig. 10. Network architecture of a manufacturing plant (master thesis by Endresen (2022))

Fig. 10 shows a principal network architecture for a manufacturing plant, as suggested by Endresen (2022). Here, we observe that levels 0-2 are organized by production lines (or "manufacturing cells"). Systems at level 3 aggregate and coordinate between data exchange for levels below and above. Level 3 also shares data with levels above via the DMZ.

1.8 Engineering and operating an instrumentation system

Engineering, as a discipline, covers the design, construction, and installation of systems; the preparation of specifications and design documents; and the execution of equipment ordering, manufacturing, system integration and installation, verification, and validation. The operation covers the phases when the system is in operation, including maintenance and management of changes/rebuilds. The various tasks are organized according to the facility lifecycle described below.

1.8.1 A facility's life cycle

The tasks listed above can be allocated into a model of the plant's life cycle, as shown in Fig. 11The lifecycle is not limited to instrumentation systems but also covers other systems, such as power, process equipment, piping, ventilation, structures, and buildings.

The following describes the phases:

The **feasibility study:** This is the first phase, where cost estimates are prepared for different construction alternatives for the facility. Considerations may include the facility's location, size, capacity, and other factors. Feasibility studies may also be relevant for existing facilities when a major rebuild or expansion is needed.

Pre-study: This phase and the feasibility study are not always distinct. Essentially, one details the project's framework conditions, costs, schedule, and solutions, often considering one or two of the most feasible alternatives. Decisions need to be made about operating and management philosophy (such as staffing levels and levels of automation), facility size and capacity, types of processing systems, the need for local storage of processing fluids, and more.

Preliminary design: This phase details the selected concept to a level sufficient to support a credible cost estimate for investment decisions. Some of the more extensive equipment with long delivery times is being ordered.

Detailed design: This phase follows investment approval and entails preparing all documentation, including technical drawings, placing orders, cost follow-up, and coordination/planning for everything that must be in place before construction and installation can start.

Construction and installation: This phase is a work-intensive period that involves coordinating and executing work across multiple sites, as well as receiving, installing, and commissioning equipment and systems. Some suppliers deliver larger systems with interfaces, while others provide stand-alone components. Modules are often completed as much as possible before being moved to the facility.

Commissioning: This phase involves checking the installed system (piecewise) against the specifications and other design documents, often on a system-by-system and signal-by-signal basis. Commissioning is usually distributed over time and locations, for example, in the premises of a specific delivery by a manufacturer, and when systems have been installed at their destination and integrated with other systems.

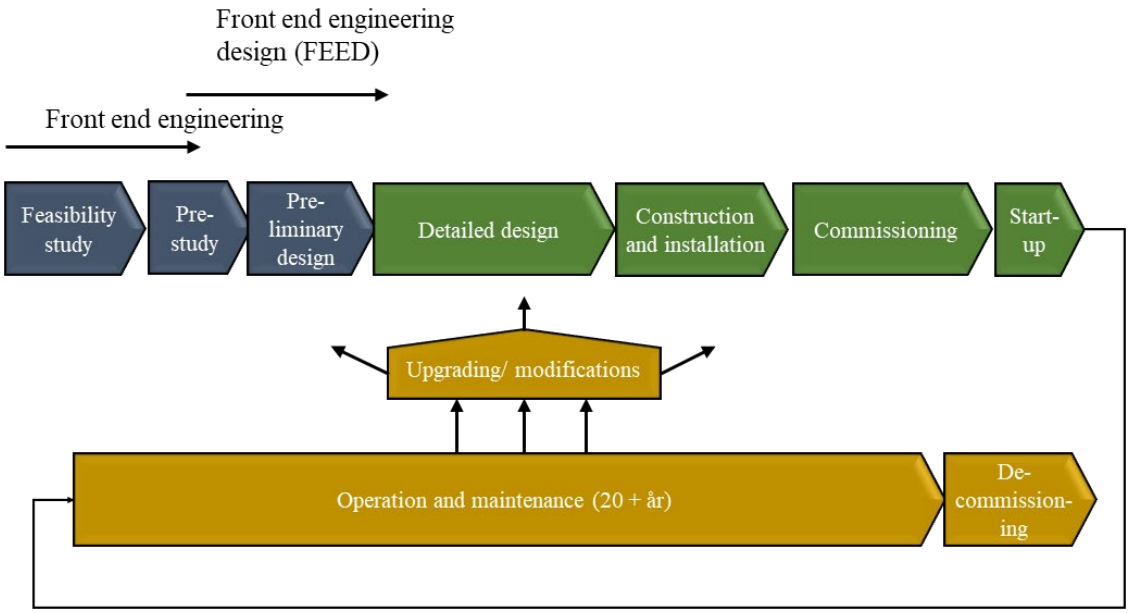

Fig. 11. Lifecycle phases of a facility

Formal activities to demonstrate the system's compliance with standards, specifications, and installation instructions are conducted before and after the commissioning phase, depending on the specific project, and include Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), and Site Integration Testing (SIT). The three types of tests are often identified as key milestones in the overall project execution plan. FAT is a complete system inspection and testing conducted at the manufacturer's premises for a specific system delivery, usually witnessed by the customer. SAT and SAT are similar witnessed inspection and testing of the system after having been installed at its destination, but where the focus is to validate that the installed system can operate in the environment it is installed in and that it works together with other systems, as explained in IEC 62381 (2024).

Start-up: This stage marks the transition from engineering to the operational phase, including the transfer of documentation and operation and maintenance procedures.

Operational and maintenance phase: This phase covers the facility's entire operational lifetime, typically 15-20 years for individual systems and 30+ years for the facility. Maintenance, testing, and condition monitoring

ensure operational availability and safety. More extensive modifications are treated as new projects, starting with, for example, a feasibility study.

Upgrading or modification: This phase is triggered when systems fail or reach the end of their life, or when process operating conditions change, or when the process must increase or reduce its capacity. Systems may also become obsolete, leaving spare parts unavailable. Changes in how the process is operated may also trigger replacement or rebuilding.

Decommissioning: The final phase of a system's life. It involves shutting down, disconnecting, and dismantling the equipment and can involve many health, safety, and environmental challenges. Storage and after-handling of equipment can also be significant tasks in decommissioning.

Most projects involving the engineering of instrumentation systems are large and complex, often with budgets in the tens or hundreds of millions (NOK). The coordination and timing of these tasks are critical. For example, the ordering of equipment must be timed so that the construction is not delayed, documents must be prepared early enough to support verification, validation, and design processes, the resource must be available to carry out testing, and all systems to be interfaced, such as mechanical systems, electrical power supply, earthing systems, and process equipment, must be available. The costs and complexity of engineering and replacing an instrumentation system require a 20-25-year life expectancy. Manufacturers must commit to delivering certain products over the long term, but equipment obsolescence means some products must be purchased for stock. A typical lifetime for instrumentation systems is 15-20 years, even though some equipment is upgraded or replaced.

1.8.2 Testing, verification, and validation

Testing, verification, and validation are also carried out within many of the other lifecycle phases, beyond the phase named "Testing and validation".

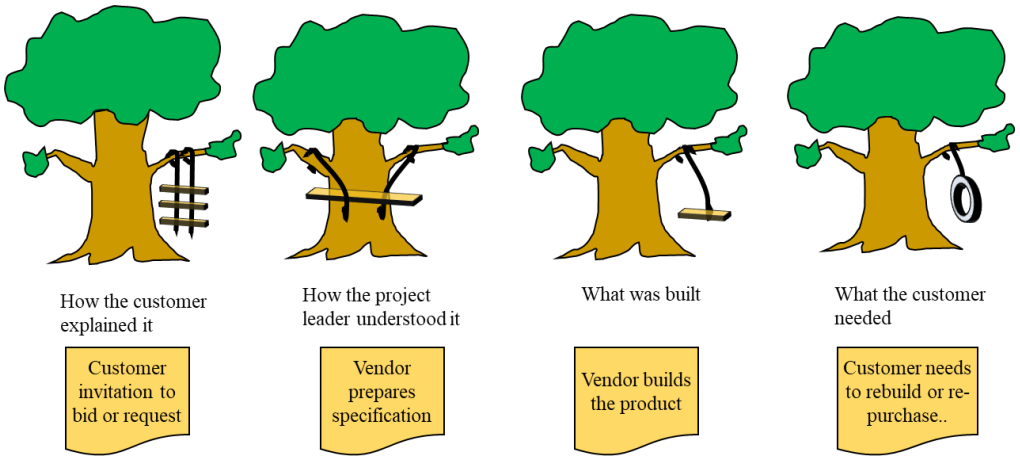

Fig. 12. Possible consequences of insufficient verification and validation

- **Verification** is about demonstrating that the specifications are met at all stages. Some describe these tasks as determining whether the system is correct.
- **Validation** complements verification, focusing on how the system will behave and whether the behavior is as intended. Some explain this task by determining if you have the right system. Verification can confirm that the specification was met. At the same time, validation can reveal that the specification is incomplete or even incorrect, leading to incomplete systems or systems that behave in undesired ways.
- **Testing** is an umbrella term for tasks used to determine whether a system's characteristics or functions are met. There are many types of testing, as identified by, e.g., IEC glossary portal (Accessed 2025), which mentions several types of testing, including unit testing, regression testing, black-box testing, white-box testing, acceptance testing, in-service testing, and dynamic testing. Testing may be part of verification and validation, as well as of the integration of built systems and commissioning.

Fig. 12 illustrates why validation is so important, even with good routines for verification and testing:

- The customer needs a new product and invites vendors to come with an offer. The invitation-to-bid description could be vague or high-level, leaving room for misinterpretation.
- The selected vendor prepares a specification based on how they interpreted the request, builds the product, and presents it to the customer.
- The customer is surprised that they have gotten something different from what they intended.
- The customer is dissatisfied; the vendor loses a happy customer, and the customer must invest more money to get the product they need.

Verification and validation could prevent the situation above, for example:

- The vendor actively involves the customer in understanding the customer's needs and reviews the specification to avoid misinterpretations.
- The vendor clarifies more details as the design matures before manufacturing starts.
- The customer is more proactive towards the vendor and asks for audits and reviews of the specification and design documents.

1.8.3 V-model or waterfall model

An alternative lifecycle model is the waterfall or "V-model" (both names are used). This model organizes a similar set of phases, as shown in Fig. 11 into the legs of a V: the phases leading up to implementation are on the left leg, while the phases covering integration and testing are on the right leg. The V-model identifies verification activities across the left and right legs, focusing on ensuring that each phase delivers according to its specifications.

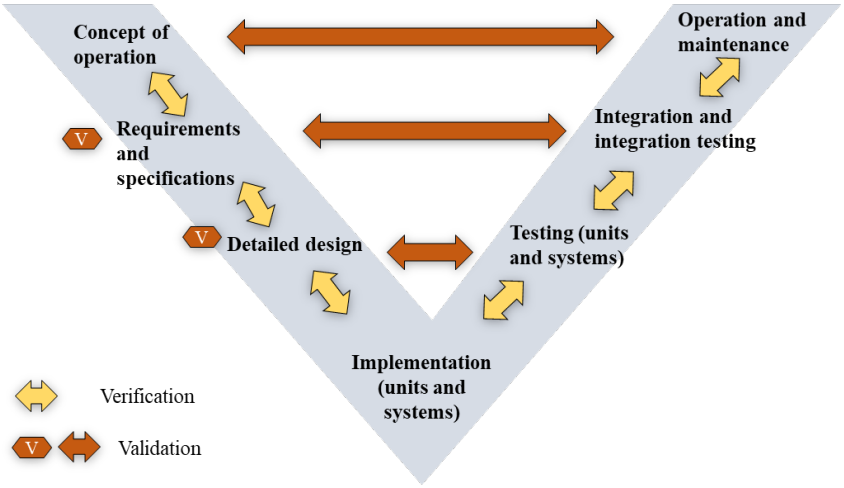

Fig. 13. The V-model (or waterfall model)

Validation activities, on the other hand, check if what is produced (right side) conforms to what is needed (left side). To prevent high costs from being incurred on building the wrong products, it is recommended to incorporate validation activities, such as documentation reviews with relevant stakeholders, during the specification and detailed design phases, when many critical decisions are made.

There are many variants of the V-model, both for larger engineering projects and for software, hardware, and software-hardware development and integration. Therefore, the naming of the phrases may vary, even if the principles on the left and right remain the same.

1.8.4 Specific engineering tasks

Fig. 14 has an overview of several engineering tasks when planning and building an instrumentation system in a flowchart-like illustration. Not shown are activities related to preparing procedures for operation, maintenance, and testing in operation.

The process indirectly identifies the need for close cooperation with several disciplines. For example:

- The choice of measurement principle and scale for sensors must be made in collaboration with the process engineers, who know in depth what needs to be measured, the measurement range, the requirements for accuracy, and the location of the equipment.
- Choice of setpoints for alarms and shutdown, in collaboration with technical safety and process engineering disciplines, based on their simulations.
- The choice of fire and gas detection relies on collaboration with the technical safety discipline, which will have information about the location of leakage points, the type of gases, dispersion during leakage, and the need for detection coverage in an area.
- The mechanical discipline needs to give input about the type of valves, whether they are open or closed during regular operation, and response time requirements.
- The electrical discipline needs to be involved in planning power supplies, earthing systems, cabinet mounting and content, and cabling.

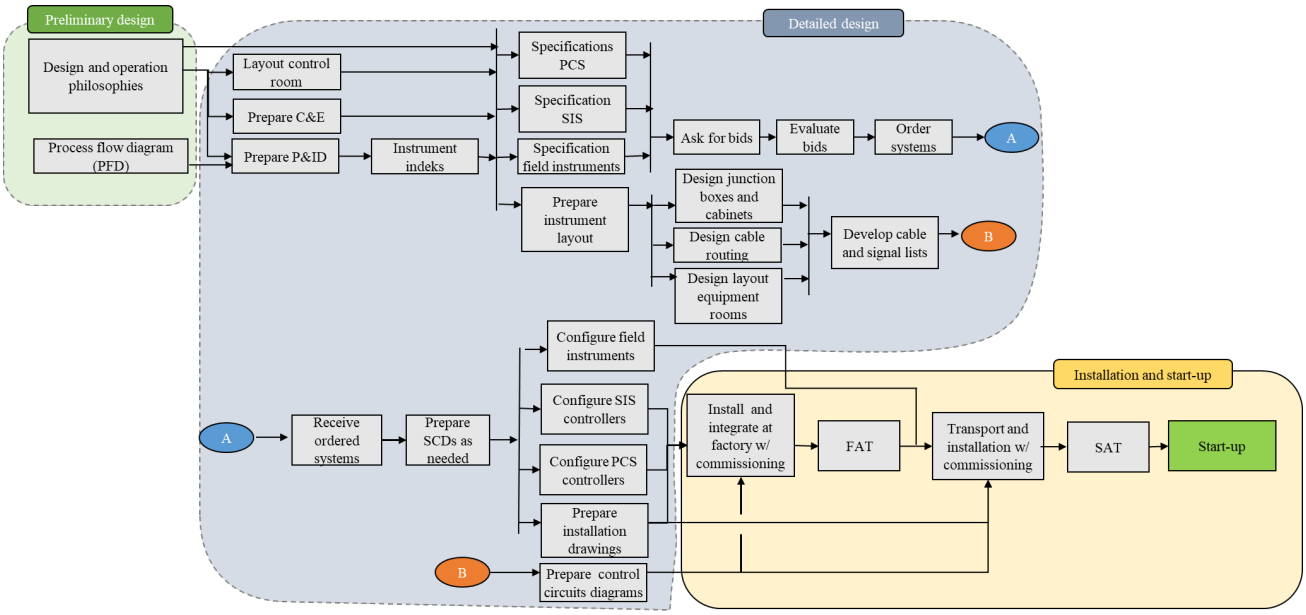

Fig. 14. Examples of engineering tasks (Adopted from T. Onshus' compendium 2019)

Many technical documents prepared for the instrumentation system start with a high-level description of the process and larger equipment, called a process flow diagram (PFD), along with the design and operational philosophies. The design and operational philosophy documents are not about philosophy; they are common names for documents that present governing principles and requirements for design solutions, operations, and maintenance. For example: Is the new plant manned or unmanned, or designed for reduced manning? Should the control room be located at the facility or a remote location? Which standards and regulations apply to the facility and its systems? Does the plant generate its own power, or does it depend on an external power supply via cables? What dimensioning loads and accidents must be considered in the design of safety systems? Which systems need to shut down in case of gas leakage? How can personnel evacuation be ensured in case of a fire?

Additional documentation includes P&IDs (piping and instrumentation diagrams), C&E (cause-and-effect) matrices, ESD shutdown hierarchies, and control room layouts. P&ID and C&E are used to prepare specifications for sensors, controllers, and actuators. The documents/drawings are entered into the system control diagram (SCD), a standardized graphical representation of program logic. All other documents and drawings relating to installation must also be prepared, including cable lists, electrical control diagrams, cable and signal drawings, and an instrument index listing all the field devices.

Later, the documents mentioned are updated to reflect the equipment purchased and supplemented with the manufacturer's own documentation. Documentation related to key requirements and installation must be kept up to date during the operational phase.

Many of the mentioned documents are explained in more detail in Chapter 3 on Technical Documentation.

1.8.5 Involved stakeholders

In the engineering process described above, there are four main stakeholders involved:

- **Asset owner:** Owner with overall responsibility. Responsible for upfront decisions, like performance requirements, design criteria, and standards to use. Participate in engineering and resolve regulatory issues with authorities as needed. It is responsible for the site acceptance test (SAT), the final test before starting up the new or modified facility.
- **System integrator (engineering company):** Engineering, procurement, and construction company. Assigned by the asset owner to design and integrate all systems across all disciplines. A primary task is to prepare all the documentation that depends on input from several disciplines, keep it updated, and prepare the necessary design and installation documentation. Is responsible for factory acceptance tests (FAT), often together with manufacturers, and takes part in the SAT.
- **Construction contractor:** Responsible for installing, commissioning, and testing all systems at their destination. Involved in FAT and SAT. An engineering company often serves as both a system integrator and a construction contractor.
- **Product supplier or manufacturer:** Responsible for delivering equipment, systems, and documentation, and supporting the system integrator and construction. Responsible for FAT relating to their delivery.

Some stakeholders may take on more than one role. For example, a system control vendor may also serve as the system integrator for the instrumentation and control part.

Examples from Norway include:

- **Asset or plant owner.** Yara, Hydro, Elkem, Equinor, AkerBP, Borregård, Tine, Nidar, and Freia.
- **Suppliers or manufacturers:** Emerson, Siemens, ABB, Honeywell, Kongsberg Maritime, and Origo Solutions.
- **System integrators or engineering companies:** Aker Solutions and Aibel. Some of these companies may also perform contracted work on systems already installed, for example, modifications.
- **Consultancy companies:** Safetec, DNV, Vysus, ORS Consulting, and Norconsult.

1.9 Regulations, EU directives, and standards

Many laws, regulations, and standards are dedicated to safeguarding health, safety, and the environment (HSE); some are relevant to instrumentation systems. Instrumentation systems comprise equipment that, if built or installed incorrectly, can cause harm. For example, incorrect installation of earthing systems can cause current passage if people touch the equipment. Lack of protection measures for machinery can lead to severe injuries and even deaths of people operating or maintaining the equipment.

1.9.1 Acts, regulations, and authorities in Norway

Acts (in Norwegian: lover) are national (in our case, Norwegian) laws that are adopted by parliament and that are issued (i.e., made valid) by one or more government bodies. Examples include:

- Act relating to the control of products and consumer services («Lov om kontroll med produkter og forbrukertjenester" [Produktkontrolloven]»)
- Act relating to the liability of products ("Lov om produktansvar [produktansvarsloven]")
- Act relating to supervision of electrical installations (Lov om tilsyn med elektriske anlegg og elektrisk utstyr [el-tilsynsloven]))

- Act relating to petroleum activities (Petroleum Act)
- Act on the protection against fire, explosion, and accidents involving hazardous substances... (Fire and Explosion Protection Act)
- Act relating to the protection against pollution and waste (the Pollution Control Act)
- Act on offshore energy production ("Lov om fornybar energiproduksjon til havs (havenergilova)")

Regulations (In Norwegian: forskrifter) are legally binding rules anchored in one or more acts. Regulations are often more specific than the more general statements in the acts. All acts and laws are available from https://lovdata.no/. Regulations related to offshore petroleum and CO2 are also available at https://www.ptil.no/en/regulations/all-acts/.

A ministry or other public body prepares the regulations. Examples of regulations of relevance to instrumentation systems for process, energy, and manufacturing industries are:

- Regulation on machinery ("Forskrift om maskiner [Maskinforskriften]")
- Regulation on low-voltage electrical installations ("Forskrift om elektriske lavspenningsanlegg")
- Regulation on electrical equipment ("Forskrift om elektrisk utstyr")
- Regulation on safety in relation to work within and operation of electrical installations ("Forskrift om sikkerhet ved arbeid i og drift av elektrisk anlegg»)
- Regulations relating to equipment and protective systems for use in areas with potentially explosive atmospheres ("Forskrift om utstyr og sikkerhetssystem til bruk i eksplosjonsfarlig område", based on EU's ATEX Equipment Directive)
- Regulation on health and safety in explosive atmospheres ("Forskrift om helse og sikkerhet i eksplosjonsfarlige atmosfærer", based on EU's ATEX User Directive)
- Regulation on pressurized equipment ("Forskrift om trykkpåkjent utstyr")
- Regulation on the design of facilities, etc., for offshore and connected onshore facilities (Managed by Havtil).
  - Offshore petroleum facilities: Authority Facilities Regulations
  - Onshore petroleum receiving facilities: Technical and operational regulations
  - CO2 transport, injection, and storage: CO2 safety regulation
  - Offshore windfarms: ("Forskrift til havenergilova (Havenergilovforskrifta)")

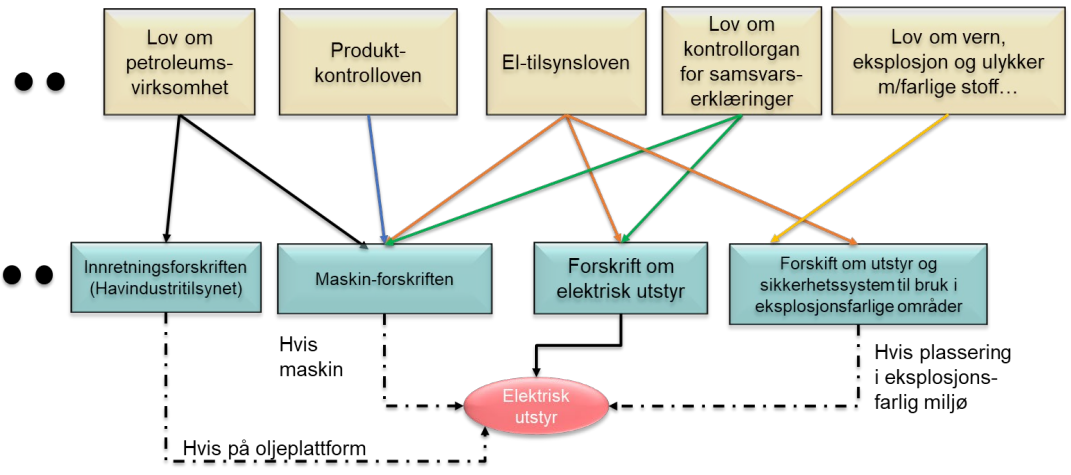

Fig. 15. Acts and laws in relation to an electrical device mounted on a machine (in Norwegian)

Examples of acts and regulations that may apply to electrical equipment, such as a sensor mounted in connection with an engine that is on an oil platform, are shown below in Fig. 15 (currently in Norwegian text only). From the illustration, we see that the design, as well as the assembly and maintenance of electrical equipment, are affected by several regulations. Some regulations apply to all electrical equipment, while others are specific to applications, e.g., a machine, an oil platform, or an area with flammable atmospheres.

The central authorities responsible for supervising and monitoring the implementation and follow-up of regulations in Norway related to the process industry and manufacturing are:

- **DSB:** Norwegian Directorate for Civil Protection (In Norwegian: Direktoratet for samfunnssikkerhet og beredskap), which is responsible for land-based industries and the public relating to:
  - Local, regional, and national preparedness
  - Emergency planning
  - Fire safety, electrical safety (land-based industries)
  - Handling and transport of hazardous substances, such as land-based process industries
  - Product and consumer safety, also covering machinery safety
- **Havtil:** Norwegian Ocean Industry Authority (In Norwegian: Havindustritilsynet), which is responsible for the industrial industries covering:
  - Oil and gas activities on the whole Norwegian continental shelf, in addition to seven connected petroleum facilities on land, and associated pipeline systems
  - Renewable energy production offshore, CO_2 transport and storage, and mineral recovery from the seabed
  - Security, including cybersecurity, for the mentioned industries listed above.

DSB regulations are a collection of national regulations, many of which are based on EU directives, and an overview is provided at https://www.dsb.no/. For example, for handling and transport of hazardous substances, they refer to the specific regulations that apply at https://www.dsb.no/lover/farlige-stoffer/farlige-stoffer/regelverk-for-farlige-stoffer/. Complementary to the overview of the regulations, DSB informs about supportive guidelines, reports, information about inspections, lessons learnt, and statistics about near misses and accidents. Most of the information is provided in Norwegian. See, for example, https://www.dsb.no/lover/farlige-stoffer/.

Havtil presents their regulations and guidelines in a similar way at https://www.havtil.no/en/regulations/all-acts/. The Norwegian version is the primary reference, but the English translation (marked as unofficial) is also available on the same pages. Also, Havtil publishes reports on inspections, audits, annual statistics about risk level at petroleum facilities "(RNNP reports"), and position papers and reports related to, e.g., safety barrier management and cybersecurity practices.

1.9.2 EU directives

EU directives are laws published by the European Commission (EC) that apply to all European countries and to members of the European Economic Area. As an EEA ("EØS") member, Norway is obliged to implement EU directives. The implementation is achieved by incorporating the rules of EU directives into National acts and regulations. This may be illustrated as shown in Fig. 15. For example, the Machinery Regulation is almost a 1:1 translation of the EU Machinery Directive. The Machinery Regulation is anchored in the Product Control Act, which implements the EU Product Safety Directive.

EU directives are available from https://eur-lex.europa.eu/ or just by "googling". Examples of directives that are central to instrumentation systems are:

- Product Safety Directive (2001/95/EC)
- Product Liability Directive (1999/34/EC)
- Machinery Directive (2006/42/EC)
- EMC Directive (2014/30/EU)
- Low Voltage Directive (2014/35/EU)
- ATEX directives about explosion protection, covering the ATEX equipment directive 2014/34/EU and the ATEX user directive 99/92/EC
- The Seveso Directive III (2012/18/EU), concerning the prevention of major accidents for land-based chemical industries
- The Offshore Directive (2013/30/EU) amending Directive 2004/35/EC concerning the safety of offshore oil and gas operations and

- Interoperability Directive (2016/797/EU) concerning interoperable European railway traffic management, including signaling systems
- Directive (EU) on information and communications technology cybersecurity certification and repealing Regulation (Cybersecurity Act) (526/2013)
- EU AI Act (and its requirements that will apply to high-risk systems)

In the adoption of such directives, it is important to be aware of the following two distinctions: minimum and maximum harmonization, which, to a large extent, place directives in one of the following categories:

- **Minimum directives** that set baseline requirements while allowing member states to introduce stricter national rules. The Seveso III Directive (2012/18/EU) and the Offshore Directive (2013/30/EU) are two such examples where member states may apply additional and stricter rules.
- **Maximum directives, also referred to as full harmonization ("new approach") directives**, contain a set of essential requirements, many of them related to health and safety, that apply to products placed on the EU market. The aim is to limit member states' ability to impose additional national product rules, ensuring products can move freely within the EU and related markets. Examples include the overarching Product Safety Directive (2001/95/EC) and the application-specific Machinery Directive (2006/42/EC). It is important to emphasize that maximum directives do not limit nations from creating their own rules and regulations concerning the *use* of products, such as machines.

Some directives also use mixed approaches, in which certain parts are fully harmonized while others allow national flexibility.

As part of the EØS agreement, Norway is required to implement EU directives. Maximum directives are implemented directly, "as is," typically as translations of the English text, since Norway cannot add any national rules or requirements. However, for minimum directives, Norway can introduce supplementary requirements. An example of this is the regulations issued by the Norwegian Directorate for Civil Protection, which are based on the principles of the Seveso Directive but adapted to align with evolving Norwegian safety best practices. The same applies to regulations issued by the Norwegian Ocean Industry (HAVTIL), which are based on, but also complement, the EU Offshore Directive. The EU interoperability directive is also a minimum directive in terms of safety and interoperability goals, while its referenced mandatory (EN) standards on technical specifications make some parts of it a maximum directive.

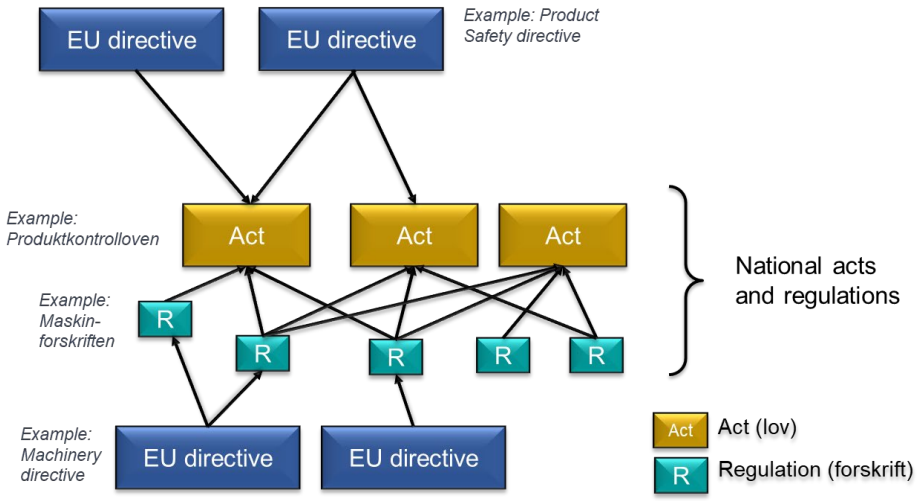

Fig. 16. EU directives vs national acts and laws

Directives developed after 1985 are referred to as **new approach** directives, reflecting a change in how directives are organized and scoped for products placed on the European market.

The new approach directives can be described as follows:

- Directives should focus on larger families of products, such as machinery, pressure equipment, and toys, rather than specific variants.
- Within these directives, the focus is on *essential* health and safety requirements, i.e., requirements that should protect people from being harmed by the handling and use of the products. The directive should formalize requirements in a way that maintains validity over time, even as technology evolves. One example of a requirement is the need to identify risk-reducing measures (technical and non-technical) through a risk assessment.
- Each directive is supplemented by *harmonized standards*, i.e., standards developed or adopted by one of the European standardization organizations CEN, CENELEC, or ETSI. The harmonized standards have more detailed requirements that ensure compliance (fulfillment) with the directive. One example of requirements detailed in a harmonized standard is how to carry out the risk assessment.
- An independent organization, a notified body, can assess how the product complies with the directive's requirements by documenting conformance with selected (and applicable) harmonized standards.
- The product developer (or owner if the owner modifies the product) fills out the declaration of conformity (In Norwegian: Samsvarserklæring).
- With the declaration of conformity, the product can be labeled with a CE marking.

The **new approach** is, in simple words, the process towards the CE marking of a product, and the new approach consists of three main pillars:

1. A directive that covers a family of products and focuses on essential requirements for safety and health
2. Related harmonized standards identified with the directive
3. Declaration of Conformity and Conformité Européenne (CE) (document)

A remark on the term "conformity" vs "compliance"
Use "compliance" to refer to products and systems meeting legal and regulatory requirements (e.g., acts and regulations), and use "conformance" to refer to meeting standards and EU directives.

The declaration of conformity is usually a 1–2-page document that lists the directives and harmonized standards the product is designed to conform with. The manufacturer must sign the document with a representative who can be personally accountable in the event of any accident or harm associated with the products. The CE marking is a label added to the product by the manufacturer to guarantee compliance with the essential safety and health requirements set out in the relevant (and listed) directives.

A remark about harmonized standards and how to find them
More information about directives and associated harmonized standards can be found by visiting the following webpage: https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en. By clicking on one of the listed Directives, it is possible to retrieve the full list of harmonized standards (e.g., Excel or PDF).

1.9.3 Norms and standards

Standards contain best practice requirements, design principles, analysis methods, and more, created by an official (national and international) body and a recognized expert group. The documents may contain requirements, design methodology, analysis methodology, etc., and achieve a status of "best practice" because, in the development of the document, you have produced something that can be agreed upon as a good way to do things. Examples of official bodies that create and publish standards are:

- IEC – International Electrotechnical Commission
- ISO – International Organization for Standardization
- CEN - Comité européen de normalisation (pan-European standardization organization)
- CENELEC - Comité Européen de Normalisation Electrotechnique
- DIN - Deutsches Institut für Normung
- ETSI – European Telecommunication Standards Institute
- ISA – International society of automation

- ANSI – American National Standards Institute
- NS - Norsk standard
- NEK - Norsk Elektroteknisk Komite

Here, we will focus on practical details regarding the coding and numbering of CEN, CENELEC, ETSI, ISO, and IEC standards.

CEN, CENELEC, and ETSI are European standardization organizations, while IEC, ISO, and ISA are global. Standards developed by one of the European organizations are called European norms and are assigned the prefix EN in the title. A standard developed by IEC, ISA, or ISA has the prefix of these three letters, respectively. When a European organization adopts an IEC standard, it will use both prefixes, e.g., EN IEC (along with the standard's number and name). Some examples:

- Standards published by IEC are marked with IEC plus a fixed digit number, for example, IEC 62061 on Safety of Machinery - Functional safety of safety-related control systems
- ISO 12100 on Safety of machinery - General principles for design - Risk assessment and risk reduction

IEC and ISO also publish three other categories of documents: technical reports (TRs), technical specifications (TS), and publicly available specifications (PAS). The web page of IEC explains the codes as follows:

- TR: A report focusing on a particular subject, including data, measurement techniques, test approaches, case studies, methodologies, and other types of information that are useful for standards developers and different audiences.
- TS: A technical specification approaches an international standard of detail and completeness but has not yet passed through all approval stages, either because consensus has not been reached or because standardization is considered premature.
- PAS: A publicly available specification published in rapidly evolving technology as a response to an urgent market need. It is designed to bring the work of industry forums and consortia into the IEC.

The TRs, TSs, and PASs are only informative and do not have the same formal status as standards. One explanation is that these three types of documents can be adopted without the same level of support (votes) from the participating countries.

CEN, CENELEC, and ETSI are organizations that publish standards that comply with EU directives. CEN, ETSI, and CENELEC standards have the prefix EN (European Norm) followed by a number, for example, EN 50325 for industrial communication systems. In topics where IEC and ISO have already published standards, CEN and CENELEC may choose to adopt these, rather than creating their own. In this way, the EU can align with an existing international practice (unless it wants to adopt a stricter approach).

When CEN or CENELEC adopts an IEC or ISO standard, the EN prefix is added. In fact, by using CENELEC as an example, there are three ways that CENELEC publishes standards, as shown in Fig. 17. The first approach is to adopt the full content of an IEC standard without any changes; in this case, “EN IEC 6XXXX” is used, noting that IEC standards always start with the digit 6. For example:

- EN IEC 62061 on Safety of machinery - Functional safety of safety-related control systems

The second approach is to adopt an IEC standard with some modifications. In this case, “IEC” is removed from the code, but the IEC standard number is kept, as evidenced by the EN followed by a number starting with the digit 6.

The third approach is for CENELEC to produce its own standard. In this case, EN is used along with numbering using a first digit different from 6, for example, digit 5, when the domain is electro-technical:

- EN 50129 on Railway applications - Communication, signaling and processing systems - Safety-related electronic systems for signaling

CENELEC, CEN, or ETSI also publish guidelines that do not have the same status as standards. Here, they may decide to adopt guidelines published by IEC or ISO (i.e., with the codes TR, TS, or PAS added to the document

code), or develop their own TR or TS. In either case, the EN prefix is replaced by CLC (for CENELEC), CEN, or ETSI in the following manner:

- CEN/TR 15640 on Sampling schemes for third-party conformity assessment of fineness in precious metal articles
- CEN ISO/TR 22100-1 on Safety of machinery — Relationship with ISO 12100 — Part 1: How ISO 12100 relates to type-B and type-C standards
- CLC IEC/TR 61508-0 on Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 0: Functional safety and IEC 61508
- CLC/TS 50459-1 on Railway applications - Communication, signaling and processing systems - European Rail Traffic Management System - Driver-Machine Interface - Part 1: General principles for the presentation of ERTMS/ETCS/GSM-R information

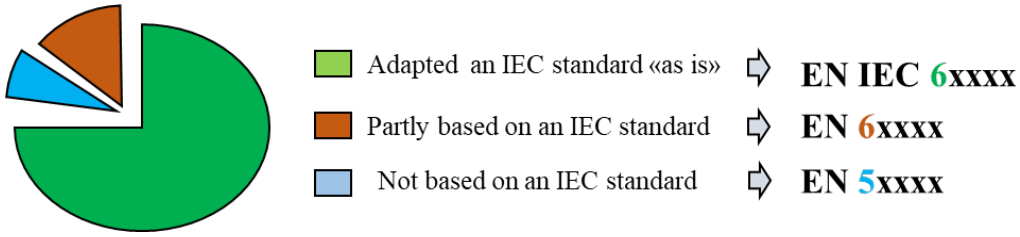

Fig. 17. CENELEC approach to publication of standards

Norsk Standard (NS) and Norsk Elektroteknisk Komite (NEK) are publishing standards for use in Norway, indicated by the prefixes NS and NEK, respectively, followed by the standard number. Sometimes NEK and NS develop their own standards, but more commonly, the organizations adopt already published IEC or ISO international standards. In this case, the NEK or NS prefix is added to the IEC or ISO number, illustrated by this example:

- Example: NEK IEC 61511-1 on Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware, and application programming requirements

NTNU provides a low-cost subscription for students to access relevant IEC, ISO, EN, NS, and NEK standards.

1.9.4 Product directive and CE marking

All products sold in the European market must meet the requirements of the EU Product Directive and, to confirm this, be labeled with a CE marking. The focus of the EU Product Directive is health, safety, and the environment, ensuring that products do not cause harm during use or handling. The CE marking is a declaration that the requirements of the directive are met. The CE marking includes the two letters CE plus the name of the organization that has certified the product, identified by a code (e.g., CE 0032). The CE marking cannot be added to the product unless the manufacturer has completed the declaration of conformity and prepared a user manual.

Search for example, “Emerson Rosemount transmitter 3051 declaration of conformity” on the internet to see what information is provided.

The steps towards the declaration of conformity also require specific steps and documentation that are not all shared openly:

1. Classification of the product and identification of which standards to apply to the design and use of the product.

2. Risk analysis aims to uncover hazards and incidents that may arise from using the product and determine what measures must be taken based on their severity. The risk analysis is not openly shared but must be made available to investigators if product hazards are discovered.
3. Complete the declaration of conformity and prepare user manuals with instructions that address relevant issues from the risk assessment.

1.10 Product directive applied to Machinery

The EU Machinery Directive 2006/42/EC is anchored in the EU Product Directive. In Norway, we have adopted the full content of the EU Machinery Directive into our national Machinery Regulation (In Norwegian: Maskinforskriften). The EU Machinery Directive is a maximum directive, meaning national Machinery regulations cannot add additional requirements.

Chapter 10 on machinery safety covers the practical application of the EU Machinery Directive and related harmonized standards.

1.10.1 New approach

The EU Machinery Directive implements the "new approach". This means that the Machinery Directive applies to a larger family of machine types and machine-related equipment, focusing on:

- Scope: What is defined as a machine according to the Machinery Directive
- Users: Who are the users of the directive (machine builders)
- Health and safety precautions: General principles to manage health and safety covering (among other things) risk assessment, principles for design of control systems, extra safety mechanisms like emergency stops, requirements for operating instructions, and ergonomics
- Risk-based: Specific safety measures to ensure health and safety are identified in the risk analysis of the specific type of machine in question
- Documentation and declarations:
    - Declaration of Conformity
    - CE marking

1.10.2 Harmonized standards

The EU Machinery Directive references several harmonized standards, and the standards are split into three groups:

- Type A: Basic principles and safety concepts for all types of machines. ISO 12100 (2010) on risk assessment of machines is an example of such a standard.
- Type B: Deals with safety aspects or a type of safety-related equipment that can be used for a variety of machines:
    - Type B1: Design of safety measures as part of the machine (physical: distance, noise, temperature, and design of control systems). Examples: ISO 13849 (2023) and IEC 62061 (2021).
    - Type B2: Other safety measures associated with the machine (two-handed control, interlocking, emergency stop, light curtain...). Examples: ISO 13850 (2015) and ISO 13851 (2019).
- Type C: Covers requirements covered by Type A and Type B standards applied to specific types of machines. For example, ISO 10218 for industrial robots.

More than 750 harmonized standards are available for the Machinery Directive. Most of these are C-type standards; only a few are of type A and B1/B2. If a C standard is available, applying A or B1/B2 standards is unnecessary unless a new feature is added.

1.10.3 Process towards declaration of conformity and CE marking

The manufacturer or machine builder must follow the following steps towards the declaration of conformity and CE marking:

1. Identification of relevant harmonized standards and inclusion in the machine's design and engineering.
2. Design and build the machine according to selected harmonized standards. Requirements include:

   - Perform and document a risk analysis where the specific hazards and hazardous situations related to the use and maintenance of the machine are identified.
   - Identify and design the necessary safety measures and systems.
3. Prepare technical documentation, including a user manual.
4. Acquire, as needed, a third-party certification: A notified body (i.e., an organization approved by the EU) examines the machine and documentation against the directive's requirements and the applied harmonized standards. If the requirements are met, the notified body issues an examination certificate.
5. Fill out the declaration of conformity and make the CE label available with the machine.

The declaration of conformity must contain, among other things:

- The name and address of the manufacturer and/or another person responsible.
- Machine name or designation, model, and serial number so that it can be identified
- The signature of an authorized person.
- The regulations/EU directives covered by the declaration and the harmonized standards applied.

The manufacturer must create a separate file containing all documentation related to fulfilling 1) through 5). The file must be available if requested after an accident involving the machine. For example, suppose a person is injured or dies while maintaining a machine. In that case, the investigators may check whether the risk assessment overlooked hazards and failed to prevent such an accident through design or user instructions. The investigation may result in criminal charges against the manufacturer or the machine owner. Modifications to the machine made by the machine owner or assembler that change its original functions require a new conformity declaration process. In this case, the machine owner may need to prepare and store the folder containing the associated documents.

1.10.4 What if different machines are to operate together?

A production line in a factory often consists of a set of machines that interact and synchronize, either sequentially or in parallel. For example, robots that coordinate product handling with the machines operating the conveyor belt. Instead of a single machine, we must ensure that an assembly of machines is safe. The assembly of machines may create new risks beyond the scope of the declaration of conformity for the individual machines. In such a case, the owner of the production line must follow the steps to obtain the declaration of conformity and CE marking for the assembled machines.

1.11 Sector guidelines and frameworks

Public organizations and company associations may publish guidelines and frameworks that supplement or complement international standards. Many of these receive broad recognition, sometimes at a level comparable to a global standard. For example, in Norway, the Ocean Industry Association (HAVTIL) references several NORSOK and Offshore Norway guidelines as recommendations for fulfilling regulatory requirements.

It is not possible to mention all relevant organizations that develop guidelines and standards with national or international outreach. With a basis in Fig. 18, some examples are:

- NORSOK: A Norwegian abbreviation for NORsk SOkkels Konkurranseposisjon. NORSOK is a long-standing project initiated by oil companies to publish specifications they have agreed upon. The motivation is that the costs of system design and product acquisition are reduced when each oil company has few individual preferences and requirements. The specifications are often based on one or more international standards; however, they include more detailed descriptions of the technical implementation. NORSOK specifications require a subscription to Standard Norge or purchase from the same place. Most offshore oil and gas facilities include NORSOK standards/specifications as part of contracts, also when built outside Norway.
- Offshore Norge (Offshore Norway): An employer and industry organization for companies with activities related to the Norwegian Continental Shelf. The organization's previous name was Norwegian Oil and Gas, but Offshore Norge (Offshore Norway) has expanded its scope to more offshore sectors. Their guidelines cover a wide specter of industry’s best practices. Examples include how to build and

operate SISs, conducting well risk analyses, and managing cybersecurity. All guidelines are publicly available and can be downloaded from their webpage. The authorities refer to some of these guidelines in their regulations, indicating they are considered suitable means of meeting the applicable regulatory clauses.

- The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. The organization is non-regulatory, aiming to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve our quality of life. All guidelines can be downloaded from the webpage. Many companies in the critical infrastructure and energy sector reference this framework, such as the NIST Cybersecurity Framework. More recently, IEC 62443 on cybersecurity for industrial automation and control systems has, to some extent, depending on the industry sector, taken over the position this framework held.
- The International Society for Automation (ISA) publishes many applicable standards within automation, safety, and cybersecurity. Unfortunately, there is no access via a Standard Norge subscription, so personal memberships are needed to access the standards.
- NAMUR stands for "Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie" and translates as "User Association of Automation Technology in Process Industry". It is now regarded as an international association, even though its center of gravity is still in Germany. It is today focusing a bit broader than Process industries, for example, on manufacturing and digitalization (with Industry 4.0).

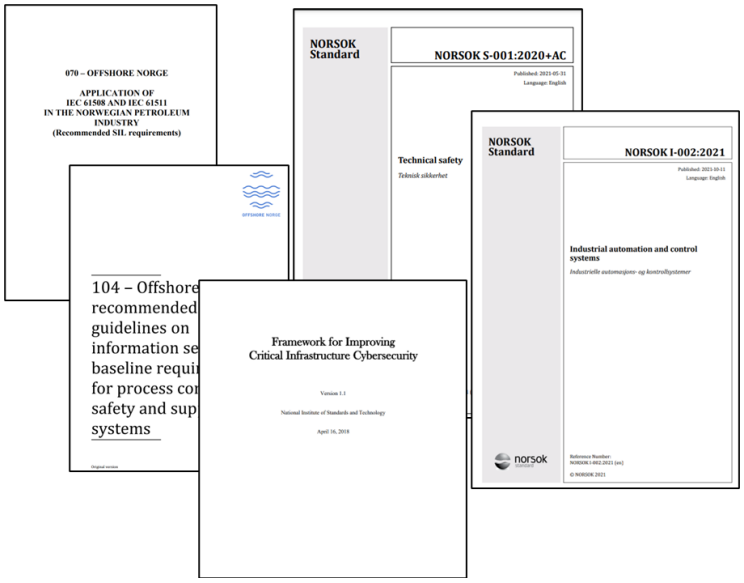

Fig. 18. Overview of some selected sector guidelines and frameworks

1.12 Where to find applicable definitions of terms

To the extent possible, the terms used in this chapter and other chapters are based on recognized glossaries, such as:

- IEC Electropedia glossary (IEC glossary) – gathering many of the terms defined in IEC standards
- IEC product and services portal (IEC glossary portal, Accessed 2025) – gathering many terms defined in IEC standards and other documents published by the organization
- ISO vocabulary (ISO vocabulary) – gathering many of the terms defined in ISO standards and related documents published by the organization
- IEEE glossary (IEEE thesaurus and taxonomy, Accessed 2025) – gathering many of the terms defined in IEEE standards

- NIST glossary (cybersecurity) (NIST glossary, Accessed 2025) – gathering many of the terms related to cybersecurity

1.13 Bibliography

References in addition to the footnotes are listed in the following:

- 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
- Endresen, S. (2022). *Cyber security handling in manufacturing plants (Master thesis)*. NTNU. https://doi.org/https://hdl.handle.net/11250/3025734
- IEC 62061. (2021). *Safety of machinery - Functional safety of safety-related control systems*. International Electrotechnical Commission.
- IEC 62264-1. (2013). *Enterprise-control system integration. Part 1: Models and terminology*. International Electrotechnical Commission.
- IEC 62381. (2024). *Automation systems in the process industry - Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)*. International Electrotechnical Commission.
- IEC 62890. (2020). *Industrial-process measurement, control and automation. Life-cycle management for systems and components*. International Electrotechnical Commission.
- IEC glossary. *IEC Electropedia: The World's Online Electrotechnical Vocabulary (webpage)*. International Electrotechnical Commission. Retrieved 15.05.24 from https://www.electropedia.org/
- IEC glossary portal. (Accessed 2025). *IEC Products & Services Portal - glossary*. International Electrotechnical commission. Retrieved 15.05.24 from https://products.iec.ch/home
- IEEE thesaurus and taxonomy. (Accessed 2025). *IEEE Thesaurus*. Institute of Electrical and Electronics Engineers https://www.ieee.org/publications/services/thesaurus-access-page.html
- ISO 12100. (2010). *Safety of machinery — General principles for design — Risk assessment and risk reduction*. International Organization for Standardization.
- ISO 13849. (2023). *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*. International Organization for Standardization.
- ISO 13850. (2015). *Safety of machinery — Emergency stop function — Principles for design*. International Organization for Standardization.
- ISO 13851. (2019). *Safety of machinery — Two-hand control devices — Principles for design and selection*. International Organization for Standardization.
- ISO vocabulary. *ISO Online browsing platform (OBP)*. International Organization for Standardization. Retrieved 15.05.24 from https://www.iso.org/obp/ui#home
- 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
- NORSOK I-002. (2021). *Industrial automation and control systems*. Standard Norge.