CHAPTER 5

CONTROL ROOMS, ALARM AND UTILITY 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 monitoring and utility infrastructure?
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 spring semester

Contents

5 Control rooms, alarm management, and utility systems

This Chapter covers additional systems that, for various reasons, are essential to the reliable and safe operation of process plants. These systems include:

- **The control room:** Even with a high degree of automatic control, human interaction is still needed for regular operation, emergencies, and maintenance planning and execution. This chapter first focuses on the central control room and on considerations when designing one.
- **The alarm system:** An alarm system provides operators with information when an unexpected event occurs. This chapter outlines requirements for designing the alarm system and provides examples of how alarm information is presented to the operator.
- **Utility systems:** Utility systems are various kinds of support systems. Our focus is on electrical, pneumatic (pressurized air), and hydraulic power systems. A reliable power supply is essential. This chapter will explain the principles of power generation and distribution at an industrial plant. We will learn that a safe power supply can mean some equipment stays powered while others are disconnected. How earthing systems protect against current passage while providing reliable shielding and a zero reference is also explained. Some equipment relies on power supplies other than electricity, such as hydraulics and pneumatics (instrument air). Therefore, the distribution systems for hydraulic and pneumatic power are also explained.

5.1 Abbreviations

CAP	Critical action panel
DCS	Distributed control system
DMZ	Demilitarized zone
ESD	Emergency shutdown system
EWS	Engineering workstation
Ex	Explosion (proof)
F&G	Fire & Gas
FW	Firewall
HMI	Human-machine interface
HP	High pressure
HPU	Hydraulic power unit
IE	Instrumentation earth(ing)
IMS	Information management system
IS	Intrinsically safe earth(ing)
LP	Low pressure
IT	Information technology
PE	Protective earth(ing)
PCS	Process control system
PLC	Programmable electronic controller
PSD	Process shutdown system
OT	Operational Technology
SIS	Safety instrumented system

5.2 Control rooms and human-machine interface

Large and complex plants require a centralized control room (CCR) to monitor and interact with processes during regular operation, start-up, shutdown, and maintenance. Traditionally, the CCR was located on the facility site; however, it is now common to place it at a remote location, depending on staffing levels and other operational considerations. A local control room may still complement a remotely located CCR if local mobilization is needed.

Depending on the facility's overall state, it is not always safe to shut down immediately in the event of a process upset. A situation may escalate into a more severe one if an interruption occurs at the wrong time. Sometimes, backup systems are needed when parts of the system fail or are degraded. During an ESD, which will disconnect the facility's main power, the control room will maintain power to critical systems and panels via the emergency generator or the uninterruptible power supply (UPS). However, the status of field devices that lose power supply during an ESD will not be available.

The control room has dedicated personnel, known as control room operators. These operators work closely with field operators who are often outdoors during the process. The visual observations, smells, and sounds that field operators notice have prevented many accidents. Therefore, an unmanned plant must have sensors and cameras to replace the field operators' senses.

5.2.1 Layout and displays

An example of a control room layout is shown in Fig. 1. Human-machine interfaces that address human factors are key to the design of control rooms.

Human factors is the scientific discipline concerned with understanding the interaction between humans and systems. It covers, but is not limited to, aspects such as ergonomics, the physical environment (including noise and light), human behavior and capabilities, stress factors, skills, work organization, and motivation.

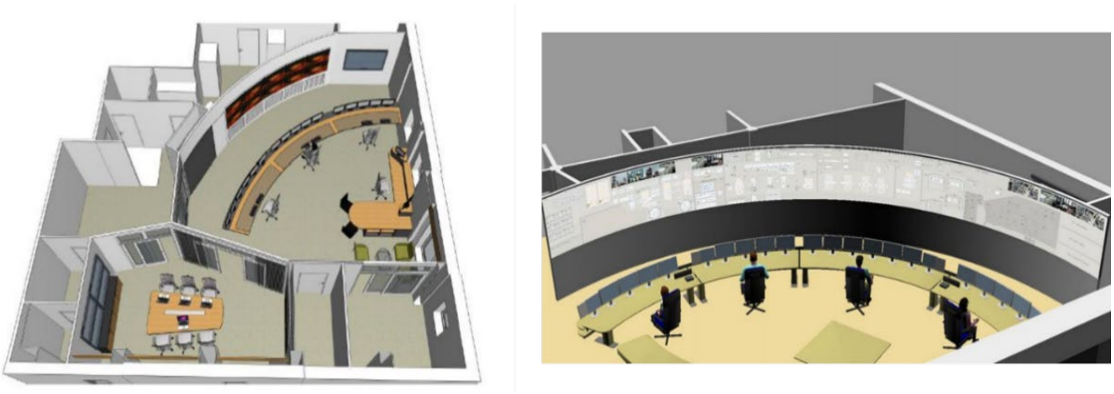


Fig. 1. Layout example of a control room

A control room presents information on large wall-mounted screens (or displays), operator stations (OS), which are PCs with screens, and, in some industries, a critical action panel (CAP). The number of operators in the control room varies with the automation level and plant size. Still, there will generally be at least two to three operators present.

These operators are complemented by process operators in the field, who will either be permanently stationed at the facility or, for unmanned facilities, mobilized during scheduled maintenance activities requiring the presence of technical personnel.

Modern control rooms typically have one or more adjacent rooms for meetings and remote access (video and internet), in which an operator from the control room must be present to minimize disturbances caused by these activities. For example, a job safety analysis (JSA) must be conducted before dismantling a valve, and the meeting must involve a control room operator. In an emergency, the operator can quickly move back to the control room to assist the other operators. The adjacent rooms are also helpful for troubleshooting, providing remote assistance, and facilitating discussions on optimization.

Examples of information available on monitors and screens in a control room are:

- Overview images of the main process with live status and measurements

- Shutdown logic, often shown as a cause & effect table (C&E)
- Power generation and distribution status
- F&G detectors
- Overview per deck/area (camera and physical location of equipment)

The control room operators also have access to personnel on board or at the facility via systems such as public address (or announcement) (PA) and walkie-talkies.

5.2.2 Example of past and new control rooms

The control room at 2/4 T processing platform used to be the heart of the Ekofisk field center in the North Sea, as the platform received oil and gas from 10 other facilities in the area, processed it, and sent it to England and Germany. The 2/4 T itself, shown in the upper right corner of Fig. 2, started up for the first time in 1974. The oil business was then more conservative, and the chosen design solutions for the control room, shown to the left, were well-proven concepts from the 1960s.

Fig. 2. Control rooms at Ekofisk field center – the old and new one

For example, the 2/4 T control room had instrument air tubes routed from the field devices into the panels, with air-based controllers mounted on the left side, as shown in the picture. Adjusting the controller's parameters was then performed manually. SIS systems were also primarily implemented using electrical circuits rather than programming, except for some fire and gas detection systems. With several panels and systems located throughout the room, a fast-moving operator was required to respond when something unexpected occurred and alarms began to sound.

Fig. 3 Control room in Trondheim for Ivar Aasen (Teknisk Ukeblad & AkerBP)

In 1997/98, the control room at 2/4 T was transferred to the new platform named 2/4 J (shown also to the upper right in Fig. 2. The new control room, shown to the lower right Fig. 2 became a more modern type (as of early 2000), featuring operator screens and wall-mounted displays.

A picture of a land-based modern control room from the 2020s is the Ivar Aasen remote control room, shown in Fig. 3. This control room was operated from AkerBP's offices in Trondheim's city center until 2024, when it was decided to move control back to the offshore facility.

Modern land-based control rooms often resemble those found in modern offshore control rooms. The control room at Elkem in Bremanger, a land-based facility for metal processing of silicon and the post-production into Silgrain, is one such example shown in Fig. 4. According to Teknisk Ukeblad, Elkem drew inspiration and gained experience from its visits to Equinor's facilities at Kårstø and Borregård. Initially, the facility had around 10 smaller distributed control rooms, each controlling a specific part of the process. With the new control room, the article highlights the following features:

- Improved alarm management: An annual rate of 5000 alarms per day has been reduced to less than 140, with improved prioritization and filtering of alarms that need attention.
- Silent working environment: The previous control rooms were small and noisy. Now, working and collaborating efficiently among personnel in the control room is easier, without unnecessary interruptions.
- Improved visualization of the entire process: A 20-meter-wide screen stretching over the entire room has been installed. Here, the central control systems are illustrated in the lower part, while video surveillance cameras are shown at the top. For the graphics, gray and white color palettes represent normal (expected) equipment and status, while intense colors indicate alarms and conditions requiring attention.

Fig. 4. Illustration of the new control room at Elkem Bremanger (Teknisk Ukeblad)

5.2.3 Regulatory requirements for control rooms and design

The Norwegian Labor Inspection Authority (No: Arbeidstilsynet) has a general regulation for the design of control rooms, which reads:

> *«Kontrollrom skal utformes og plasseres slik at driftssikkerheten for systemet og sikkerheten for arbeidstakerne er best mulig med hensyn til fare for ulykker. Det skal særlig tas hensyn til fare for brann, eksplosjoner og utslipp av helsefarlige stoffer og biologisk materiale.»*

These requirements stipulate that the control rooms be located at a safe distance from areas that could be affected by foreseeable dangerous incidents or accidents. Finding a suitable location is more manageable for land-based facilities than for offshore ones. The offshore solution is to locate the control room behind a physical fire-resistant wall, dimensioned to withstand specific loads from explosions and heat radiation.

Process facilities following Norwegian Ocean Industry Authority (HAVTIL) regulations, i.e., facilities that directly receive oil and gas from offshore installations via pipelines (such as Kårstø, Aukra, and parts of Melkøya), must comply with the following requirements:

> **§ 21 Human-machine interface and information presentation**

> *Monitor-based equipment and other technical equipment for monitoring, controlling, and running machines, installations, or production processes, shall be designed so as to reduce the risk of mistakes that can be significant to safety.*
>
> *Information transmitters and operating devices shall be designed, placed, and grouped to allow for simple and quick receipt of necessary information and implementation of necessary actions. The presented information shall be correct and easily understandable.*
>
> *Information systems shall be designed for both normal and critical situations.*
>
> *The control room shall be placed, designed, and outfitted so that safety and working environment are prudent and the risk of mistakes of significance for safety is reduced.*

The clause has a guideline (accessed via the clause) that points to relevant standards for the design of screens and user interfaces:

> *During design as mentioned in the first subsection, an analysis of the human-machine interface, including necessary task and function analyses, should be carried out. For such analyses, Part 2 of the NS-EN 614 standard should be used.*

The NS-EN ISO 11064 standard should be used for design of the central control room. For the design of alarm systems, refer to Section 33a.

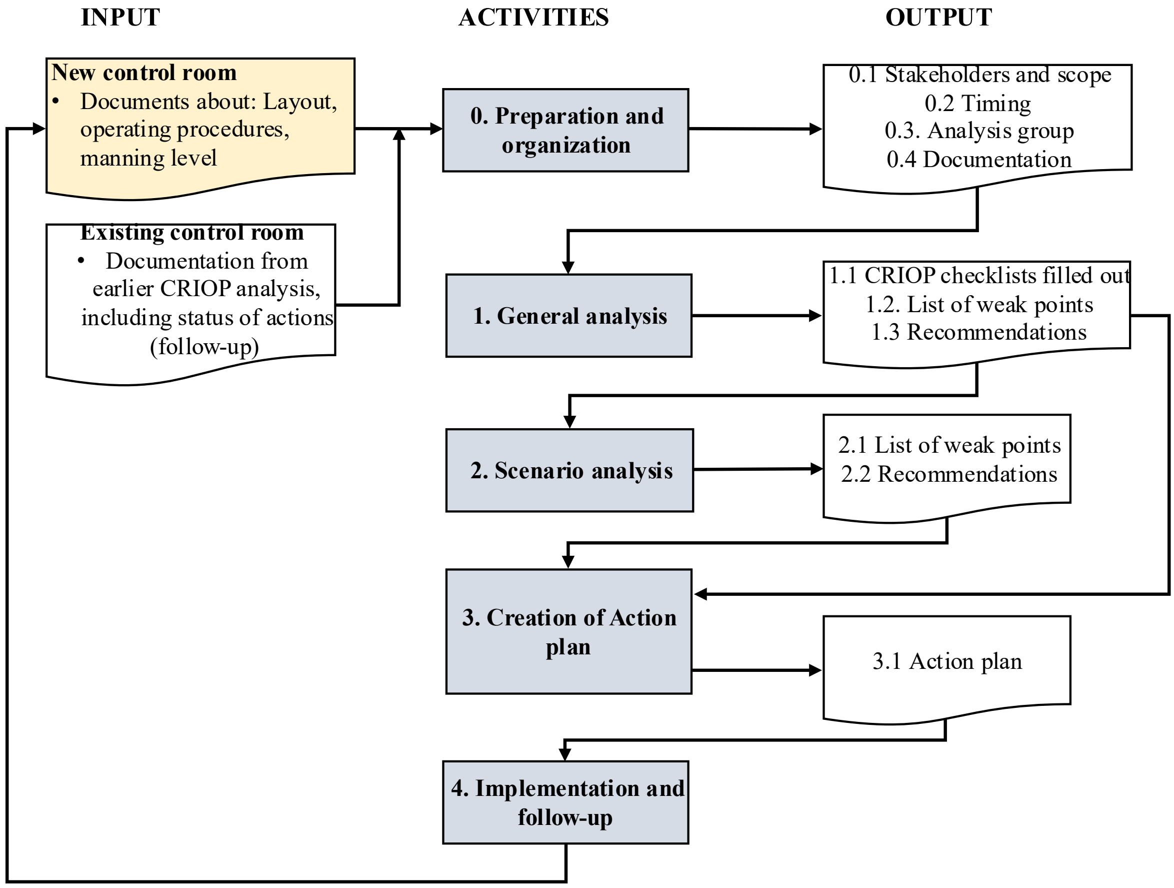


Fig. 5. CRIOP methodology (main report)

The referenced ISO standard has not been updated since 2000. Still, the industry has developed a structured guide for control room design, known as the CRIOP methodology, originally developed by SINTEF for the oil and gas sector. The methodology has a webpage with a more detailed explanation in the CRIOP report (SINTEF, 2011). Today, application areas extend beyond the oil and gas sector to the layout and organization of train cabins, ship bridges, and, more recently, control centers for autonomous ships.

The CRIOP methodology consists of the following steps, as shown below and in Fig. 5:

1. **Preparation and organization**, including identifying who will be involved (defined as the analysis group), determining when to conduct workshops/meetings with the identified individuals, and preparing documents that describe the current version of the control room design, proposed manning level, roles, and operational procedures.
2. **The general analysis** focuses on the factors that affect the control room's ability to manage general abnormal situations rather than those specific to any scenario. The analysis group gathers in a workshop to discuss and report on questions using predefined CRIOP checklists. Checklists are organized according to:
    - Layout of control room (screens, desks, distances, location)
    - Working environment (noise, light, heat, and ventilation)
    - Control and safety systems (layout, symbols, sound, status, and colors for process and alarms on screen)
    - Job organization
    - Procedures (operation, testing, start-up, emergency handling)
    - Training and competence needed
    - Remote operation (if applicable)
3. **The Scenario analysis** focuses on identifying specific scenarios that may occur during various abnormal operations and emergencies. Here, the scenarios are detailed using, for example, sequentially timed event plotting (STEP) diagrams, which illustrate the tasks that actors need to perform, their timing, and their interactions. Checklists address various human factors related to the scenarios. The scenario analysis may be more comprehensive than the general analysis.
4. **The development of an action plan** that incorporates all the weak points identified in the general and scenario analyses. Weak points are typically listed in a table along with recommended actions, the responsible person, and target data for resolution.
5. **Implementation of results and follow-up**, which involves the tasks and persons responsible for monitoring the action plan and ensuring its availability for future CRIOP analyses.

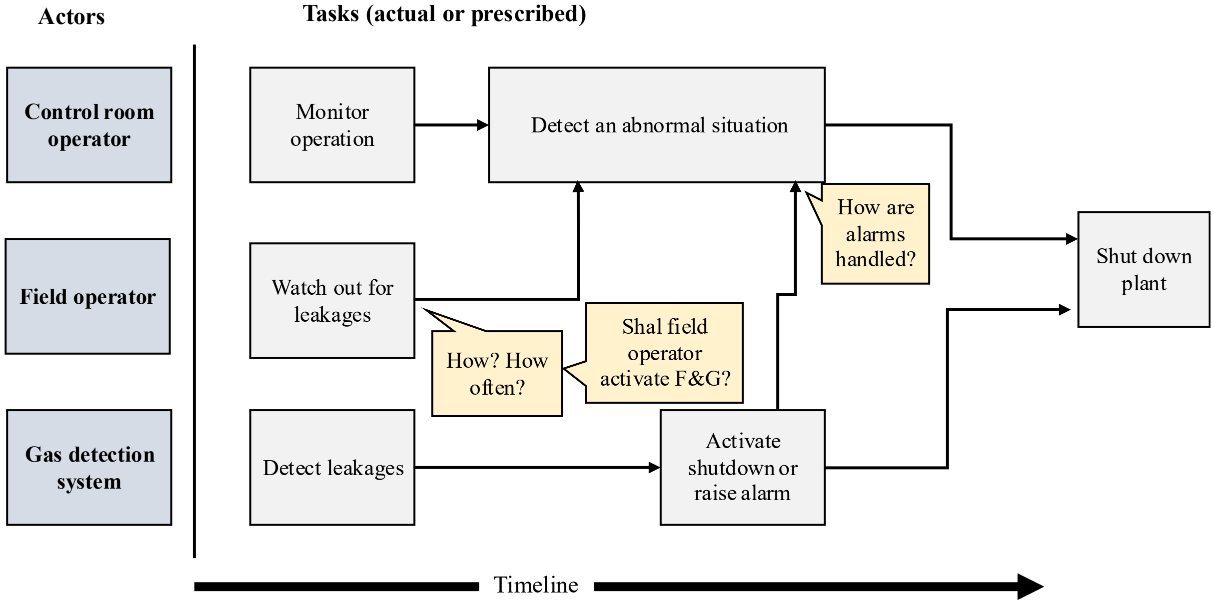


Fig. 6. STEP diagram

The CRIOP methodology has developed several checklists to structure the discussions and report the results. This example shows that the questions address specific regulations, standards, and best practices. The references must be updated to reflect the industry or application being analyzed, without affecting the general questions about best practices and topics to consider.

Scenario analyses are conducted for particularly challenging operational situations. Here, one or more Sequential Timed Event Plotting (STEP) diagrams, along with checklists, are used to address issues related to each identified event. Fig. 6 illustrates the main principles of a STEP diagram, identifying the actors, tasks, and their relationships. We note that actors may be humans or technical systems, and tasks may be either automatic or manual. By discussing the tasks and coordination one by one, it is possible to identify issues that are unclear, not covered by procedures, or not supported by the technical systems.

5.2.4 Operator screen layout

Information essential to display to operators is:

- Process and plant layout and real-time status, with distinguishable symbols for normal and abnormal states, for example, using symbols and colors
- Setpoints
- The possibility of accessing historical trends for any parameter
- List of alarms, including alarm priorities

Not all information can be displayed simultaneously, and a hierarchy of pictures is typically designed: The main (first) screen picture provides an overview of the process's overall status and key alarms. In contrast, underlying screen pictures offer more detailed information when accessed.

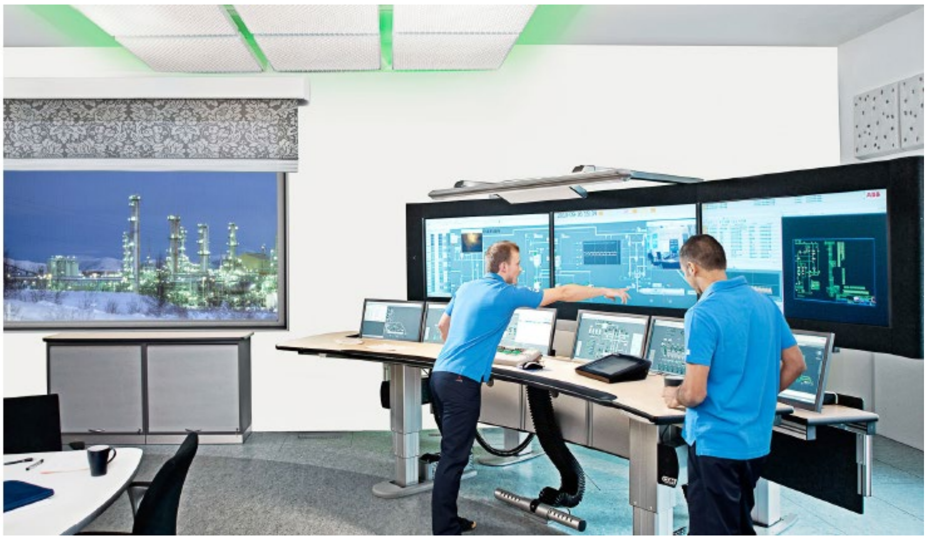


Fig. 7. Screen layout examples from ABB manual "Ability™ System 800xA Alarm Management"

Large wall-mounted screens are essential supplements to the operator screens. Operators can view the same picture from different locations within the room. Some large screens are dedicated to always showing the overall process layout and status, while other displays show the status of alarms and safety-instrumented systems.

An operator screen layout example is shown in Fig. 7. Some examples of principles and trade-offs when designing operator screens are:

1. Ability to provide good situational awareness—both during everyday situations and when the situation drifts from normal operation to emergency.
2. Place the most essential information foremost/on the main screen to ensure it is accessible without scrolling
3. Clear – easy to tell the difference between normal conditions and deviations

4. Careful choice of alarm visual presentation using lights, flashes, and color to avoid confusion while helping to attract the operators' attention
5. Alarm filtration is included to prevent operator overload during an alarm avalanche, a situation in which hundreds of alarms are triggered simultaneously.
6. Ability to access trend curves from historical data with the necessary resolution and the possibility to show several parameters in the same plot.

Designing a control room environment is not only about choosing the technical solutions and screen layouts, but also requires human factors competence to address factors like:

- Stress level and the ability of operators to manage simultaneous tasks
- Use of training, for example, with simulators, to obtain necessary competence and experience with operating scenarios
- Amount of information and form of presentation (e.g., quantity and how intuitive it is)
- Working environment (psychosocial, noise, lighting, etc.)
- Ergonomic solutions, i.e., workplace facilitation that ensures that operators are not exposed to illness and strain injuries, about the design of the workplace itself (distance from the screen, height of desks, chairs, distance to the wall-mounted screen, and visibility/readability).

5.2.5 Critical Action Panel (CAP)

The operator stations and displays rely on computerized technologies, often Windows-based products. The Norwegian Ocean Industry Authority (HAVTIL) requires that control rooms monitor status and activate the most critical functions from an independent panel that is more robust than general IT computer systems. Paragraph §33 in the facilities regulation states that:

> *It shall be possible to manually activate functions from the manned control centre that bring the facility to a safe condition independently of the parts of the system that can be programmed.*

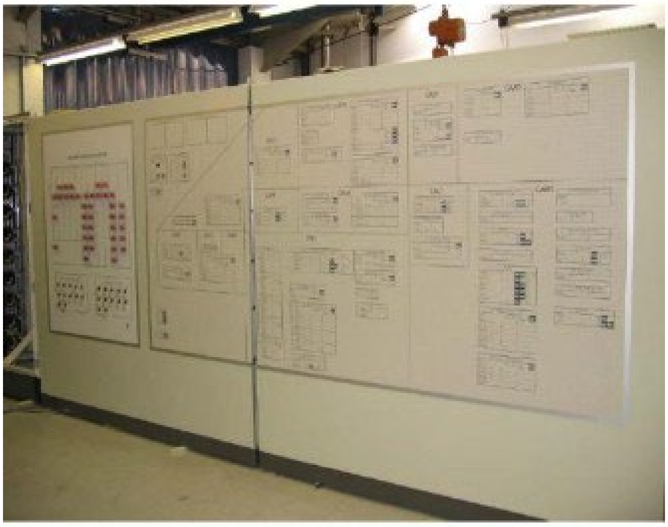


Fig. 8. Example of CAP panels

This panel, named the critical action panel (CAP), shall be a backup to the other operator screens and displays, and may include:

- Lamps that provide critical systems and equipment status about fire and gas detectors, fire extinguishing systems, emergency generators, and the position of key valves.
- Push buttons for activating ESD, starting fire pumps and emergency power, disconnecting power supplies, and (for floating facilities), activating ballasting valves, as well as operating watertight doors.

Fig. 8 shows an example of a CAP panel. In this CAP, the zones for pushbuttons are separated from the status information, but the design varies by facility.

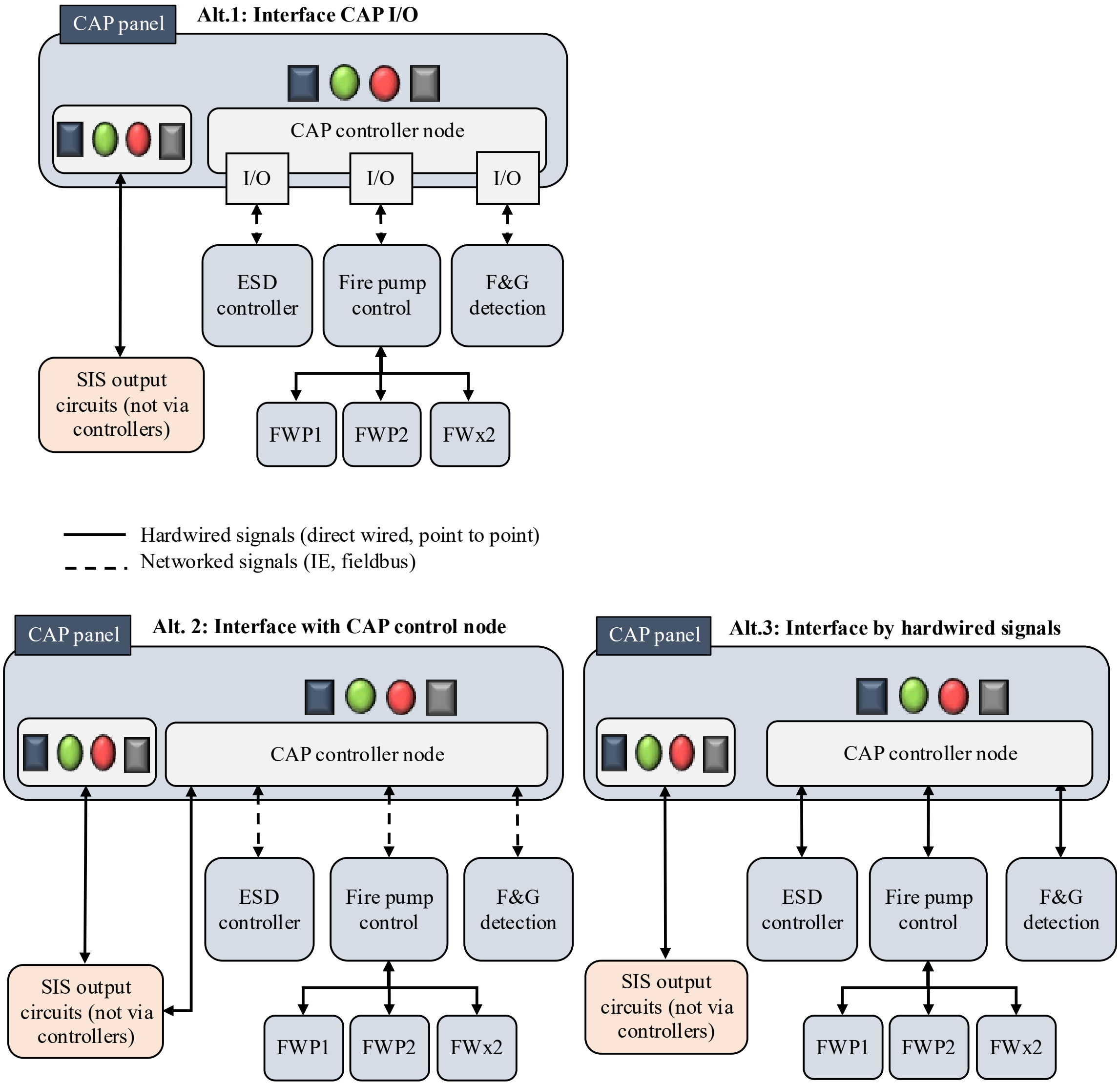


Fig. 9. CAP panel implementation alternatives per NORSOK I-002

Requirements about the design of the CAP are found in the following Norwegian guidelines: NORSOK I-002 (2021), NORSOK S-001 (2021), and Offshore Norway GL 070 (2026). NORSOK I-002 describes three alternatives for CAP panel design and interfaces, as shown in Fig. 9. The principles are as follows:

- Some statuses and functions, like emergency shutdown (ESD) and fire and gas (F&G) systems, are based on direct exchange with the SIS controllers. Signals can be exchanged over a separate, secure bus (if the CCR is located remotely) or via individual wires (one signal at a time).
- Some functions may also interact directly in the electrical circuit that provides power to the final elements, independently of the SIS controllers. These signals are always hardwired.

Each signal to and from the CAP is routed separately to the relevant I/O card or input/output signaling circuit. This method of routing signals separately is called hardwired signaling.

The other listed SAS independent functions concern primary power isolation (and reset):

- Individual time-delayed isolation of primary (main) power supply (A and B sides of the main switchboard)

- Reset the countdown timer for isolation of primary power supply ("regret")

For remotely located facilities, NORSOK I-002 (2021) requires that CAP functions be sent via a separate and secure datalink.

5.3 Alarms and alarm management

The operator stations incorporate an alarm management system. The system presents alarms, prioritizes them, and provides operator decision support. An alarm is a message that notifies operators when an issue requires their attention. Alarms often indicate an unexpected, undesired, or unauthorized state of a system or device. The origin of the alarms is faults and abnormal events, including equipment failure, detected by any of the systems (PCS, PSD, ESD, F&G, and other systems) onboard the facility and relevant to the operation.

The European Norm EN IEC 62682 (2022) and EEMUA 191 (2013) are examples of standards used to design alarm management systems within the process industries. We will address some issues within the scope of these standards. The following will refer to the alarm management system as just the alarm system.

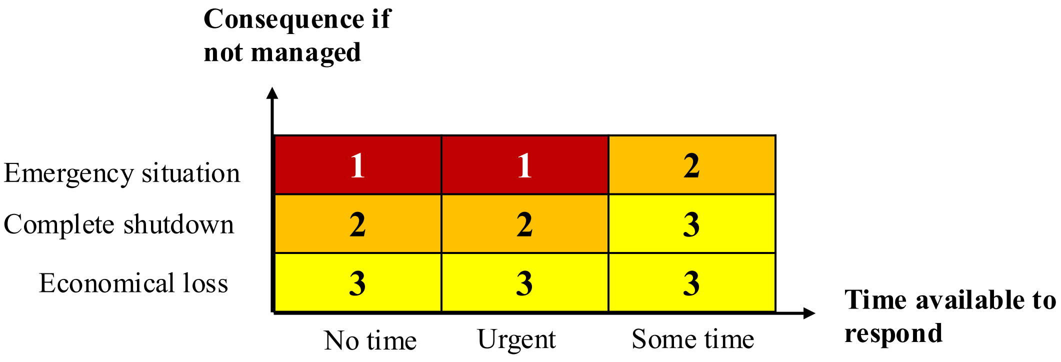
5.3.1 Primary and secondary functions

The **primary function** of the alarm system is to notify operators of abnormal process conditions and equipment malfunctions and to provide support for their responses. The alarm systems receive inputs from the PCS and the SIS, and the alarm can relate to an unexpected state of the measurement, output state of the controllers, or state of actuated devices. Which alarms to include is often determined by a hazard and risk assessment, combined with an overall alarm philosophy or set of principles.

For alarms to be effective, they must:

- Be relevant for supporting operators' tasks
- Sufficient to explain the starting point and sequence of events that led to the alarm
- Be explanatory so that it provides guidance on how the situation can be managed

An event can trigger multiple alarms, known as an alarm flood, which means the alarm rate increases rapidly. Algorithms are built into the system to identify the most critical alarms to resolve. Such algorithms are called alarm filtering.



	No time	Urgent	Some time
Emergency situation	1	1	2
Complete shutdown	2	2	3
Economical loss	3	3	3

Fig. 10. Deciding on alarm criticality

Marking alarms by criticality (e.g., from 1, the highest, to 3, the lowest) helps operators prioritize the most important ones. For example, an alarm indicating a malfunction from a single device in a safety-instrumented system, such as a gas detector, is less critical during normal operation than when the process is out of control. The criticality of an alarm determines how quickly the cause must be corrected or addressed. An example of how the criticality is determined is shown in Fig. 10. Two factors are applied here: one is the consequence, which indicates severity, and the other is the time, which indicates how much time the operators have available to act. As expected, the combination of having little or no time during an emergency results in the highest criticality (1).

Analysis of the process safety time per hazardous scenario is often used to determine how quickly the operator must respond to an alarm.

Process safety time refers to the period between a process upset or another event that could lead to a hazardous situation. Any intervention must occur within this time to be effective.

The activities to be carried out within the process safety time are illustrated in Fig. 11.

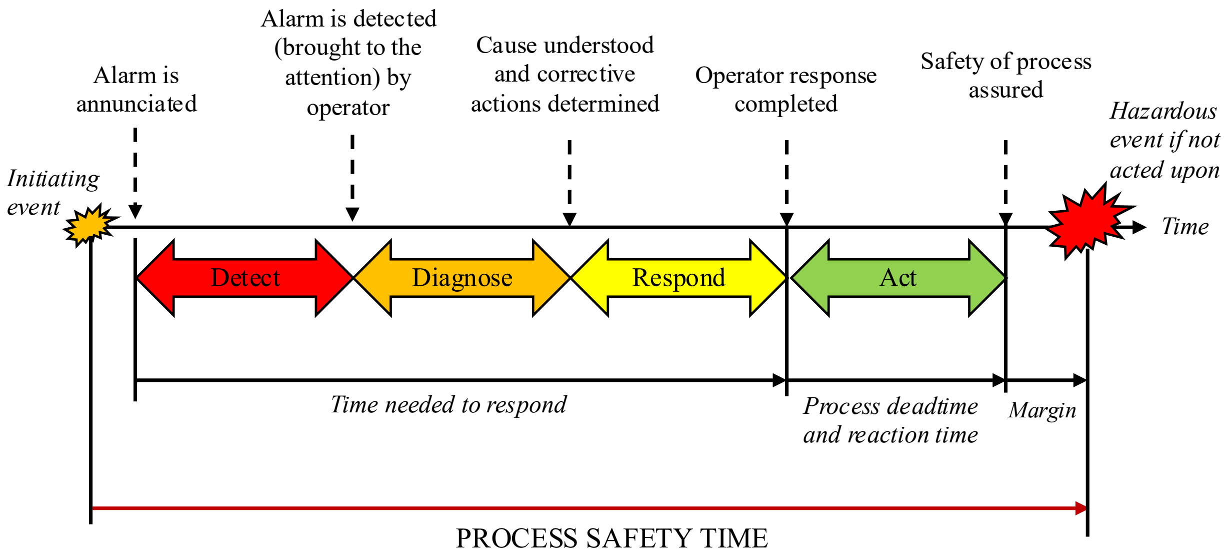


Fig. 11. Process safety time versus time available to respond

As shown in the same illustration, the overall response regarding where safety is achieved relies on the following steps:

- The alarm is detected by a source system and brought forward to the alarm system for annunciation.
- The operator becomes aware of the alarm. If multiple alarms are announced simultaneously, the operator may need extra time to respond.
- The operator can diagnose the situation to understand the cause of the alarm and decide on a corrective action, considering other relevant information. This task can be quite complex if a situation is about to escalate or has already escalated. If the situation is stressful or unfamiliar, it can also take more time to determine the best course of action.
- To execute the actions, such as pushing a button to shut down the plant, starting firewater pumps or any other extinguishing systems, or moving into the process area to operate a manual valve. As we understand, the response time may vary depending on the situation.
- The effects of the operator response may take some time; for example, to achieve a state where the pressure is reduced, the leakage stops, or the heated tanks cool down.

All these steps will add up to an overall response time that must be lower than the process safety time to be effective.

Operator training is often done in simulators. The simulators have the same user interface (operator screens) as the actual control room, but a large-scale simulator model replaces the connected process. Simulator training enables operators to manage rare but potentially severe events.

The **secondary function** of the alarm system is to provide access to past alarms, enabling us to better understand what happened and why. Event logs must enumerate the alarms and display them in the sequence in which they occurred. The purpose of the event log is often to determine what initiated the alarm.

The alarm system is not the only system the operator must monitor and track to detect abnormal events. The overall trend in process variables and access to video recordings used for surveillance is also important.

5.3.2 Alarm-related terminologies

Alarm systems apply several concepts that are defined in EN IEC 62682 (2022), including the following selections:

What type of alarm:

- **Key alarms** that are directly safety-related (e.g., fire/gas alarms) and critical process alarms (e.g., high level in flare liquid separators). Other high-priority process alarms, such as key alarms, may also be appropriate.
- **Basic alarms** are generated by detecting deviations in individual measurements from the process or specific equipment components.
- **Aggregated alarms** are generated by combining the states of several basic alarms so that the condition of a process part is described more precisely than basic alarms can describe.
- **Model-based alarms** are generated based on online simulations of mathematical models of defined process elements.

Information characterizing the alarm:

- **Alarm message:** Text string displayed with the alarm indication that provides additional information to the operator (for example, on the action to be taken)
- **Alarm annunciation:** The Function of the alarm system is to call the operator's attention to an alarm. This can be done by sound, light, flashing, or other means.
- **Alarm prioritization:** The process of assigning a level of operational importance to an alarm
- **Alarm priority:** The relative importance assigned to an alarm within the alarm system to indicate the urgency of the response, e.g., the seriousness of consequences and the allowed response time.
- **Alarm rate:** Number of annunciated alarms in a specific time interval
- **Alarm setpoint:** Threshold value of a variable or discrete state that triggers the alarm indication. In a piping and process diagram (P&ID), alarm setpoints are sometimes indicated as LAL (level alarm low), LAH (level alarm high), PAH (pressure alarm high), and similar terms.
- **Allowable response time:** The maximum time between the alarm's announcement and when the operator takes corrective action to avoid the consequence. This time limit must be below the process safety time.
- **Alarm flood:** A Condition during which the alarm rate is greater than the operator can effectively manage. For example, more than 10 alarms per 10 minutes.

Alarm system design involves alarm rationalization, a process that reviews potential alarms using principles of alarm philosophy, selects alarms for design, and documents the rationale for each alarm.

Alarm systems typically implement the following functions:

Alarm filtering: An algorithm built into the control system that selects which alarms to display and not. Some filtering is permanent, meaning certain alarms are never shown, while other filtering is conditional, applied only in specific abnormal situations to prevent the operator from becoming overloaded. The latter is referred to as designed suppression.

> Alarm filtration has always been a challenging task. Have the rules been properly designed so that no alarms important to the situation are ever shared with the operator? Filtering algorithms, therefore, require careful planning and, after deployment, also reevaluation.

Alarm acknowledgment: Operator confirms having seen the alarm and is ready to handle it. After acknowledgment, the operator decides whether to act on the alarm or to prioritize other alarms first. In some cases, acknowledged but still unresolved alarms may, after some time, trigger a plant shutdown.

Alarm suppression, sometimes referred to as design suppression: An automatic suppression that prevents alarms from being announced to the operator, even if active, based on the state of the system.

- The suppression is based on a filtering algorithm activated upon an alarm situation, and it automatically decides (i.e., filters) which alarms to exclude from the operator screen, prioritizing the least important alarms given the operating conditions and plant state.
- The aim is to reduce overloading and confusion for operators under various operating scenarios, including emergencies.
- The suppressed alarm is sometimes, depending on the configuration, suspended after some time.
- Examples of alarms being suppressed:
  - During facility's start-up: Suppression of alarms that report levels, pressures, and temperatures being outside the low or high limits for a short period of time. Alarms from equipment on standby can also be suppressed.
  - During normal operation: Suppression of alarms from systems that are temporarily stopped.
  - In an emergency: Suppression of alarms that are secondary to the primary alarms. Primary alarms are those necessary to understand what triggered the hazardous scenario and what is most urgent to address to avoid escalation; secondary alarms can wait to be attended to.

Shelved suppression (alarm shelving): A manual type of suppression by the operator so that the alarm is silenced or removed from the main alarm list for a temporary time, before it reappears.

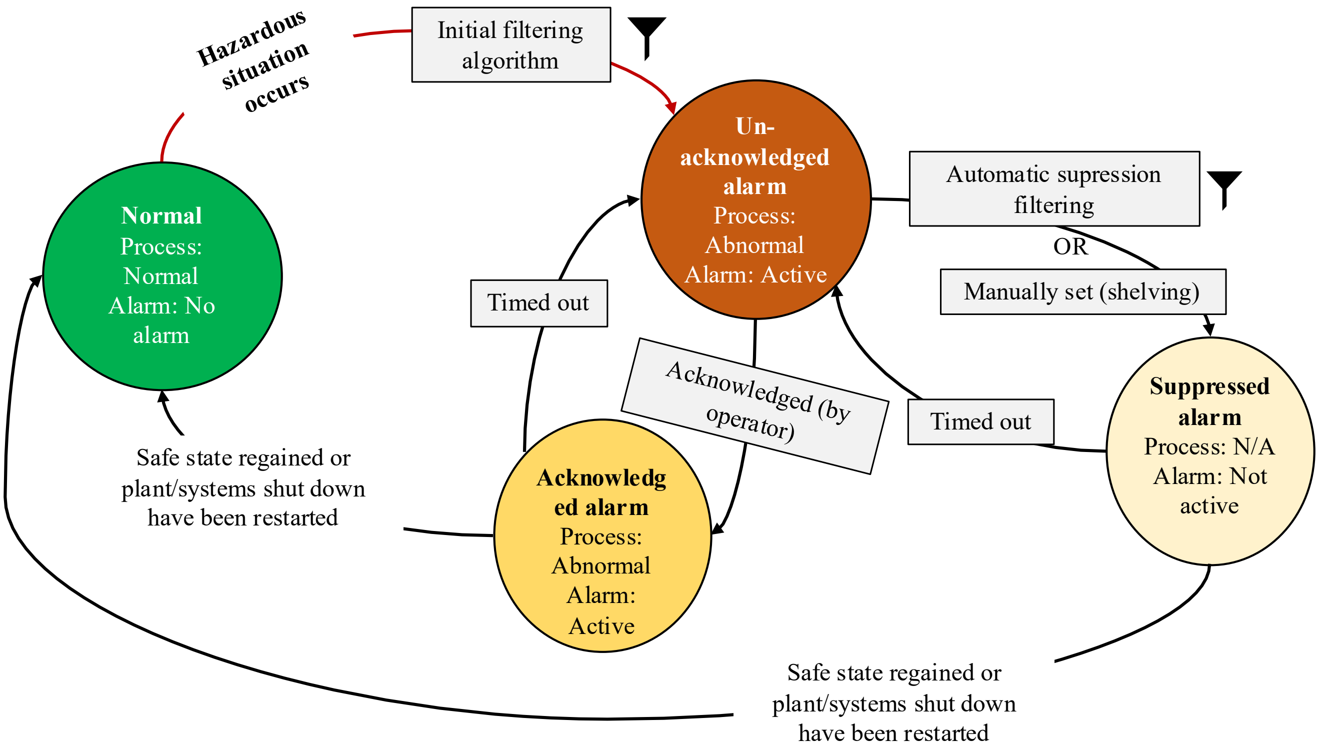


Fig. 12. States of the alarm system (simplified version of illustration in EN 62862)

The states of an alarm system can look something like Fig. 12, inspired by EN IEC 62682 (2022):

1. **Normal (no alarm) state:** The process is in a regular, non-hazardous state, with no active alarms or an acknowledged active alarm.
2. **Unacknowledged:** This is the state in which the alarm has been raised but not yet acknowledged by the operator.
3. **Acknowledged:** The situation is abnormal, but the operator has acknowledged the alarm and is trying to resolve it.

4. **Suppressed:** The alarm is still active, but an algorithm or the operator decides that the alarm is not critical in the present operating situation and removes it from the main alarm list or display.

Alarm filtering (shown with a funnel symbol in Fig. 12) uses an algorithm to select the most relevant alarms based on the situation. A potential pitfall is filtering out alarms that should have been brought to attention; therefore, filtering algorithms require careful planning and reevaluation.

5.3.3 Example of regulatory requirements

The Norwegian Ocean Industry Authority's regulations for onshore facilities provide an example of alarm system requirements. The technical and operational regulation §33 reads:

> *Onshore facilities shall have control and monitoring systems which, using associated alarms, warn the operator of incidents, nonconformities or faults that are significant for safety. The alarms shall be issued such that they can be perceived and responded to within the time required for safe use of equipment, plants, and processes.*

The guideline to the clause provides examples of how the alarm systems should be designed:

> *Alarms should be defined and designed such that*
>
> 1. *the alarms that are presented are relevant, easy to register and understand, and clearly show where any nonconformities and hazardous situations have arisen,*
> 2. *the alarms are coded, categorized, and assigned priority based on the safety significance of the alarms and how quickly measures must be taken to avoid undesirable consequences,*
> 3. *the alarm systems allow for suppressing and reducing alarms, so as to avoid mental stress for control room personnel during interruptions in operations and accident incidents.*
>
> *With regard to the design of the alarm systems, standards EN 62682 and EEMUA 191 should be used. The performance requirements of EEMUA 191 Chapter 6 and EN 62682 Chapter 16.5 should be adapted to the specific facility.*

Examples of requirements in EEMUA 191 are (i) that all alarms should notify (make themselves known), inform, and guide the operator, (ii) all alarms should be helpful and relevant to the operator, and (iii) each alarm should have a specified/described follow-up. Valuable and relevant alarms are those that pertain to the situation at hand. Follow-up procedures outline the actions operators should take in the event of an alarm. For example, to investigate the cause of the alarm and initiate equipment shutdown as needed.

5.3.4 Alarm philosophy

An alarm system should result from a thorough, structured process that incorporates site-specific considerations and complies with relevant regulations. The first step in such a process is often to create an alarm philosophy document. The alarm philosophy should explain the basic principles and justifications of the chosen alarm system and is not (as the name indicates) some philosophical activity. The alarm philosophy is developed by the asset owner and shared with the control system supplier, which implements the solutions. The alarm philosophy should describe:

- The functions of the alarm system
- Principles of annunciation and logging
- The operator's role: How the operator’s responsibility to intervene changes with the process state, and what support the operator needs in the different process states
- How the system should be designed to take human limitations into account
- The use of alarm priorities: The purpose of prioritization, how priorities are defined in the system, and the justifications for these definitions.
- Practice for acknowledging the alarms, i.e., under what situations this can be done
- Standards to be used
- Principles of the generation of alarms
- Principles of structuring alarms

- Presentation of alarms (visual, light, symbols, etc.)

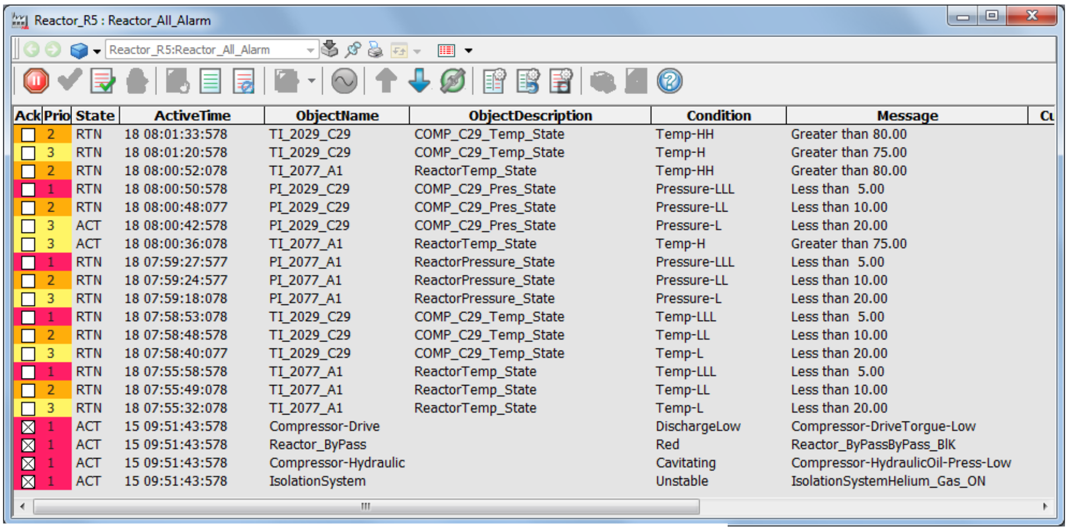
Working with the alarm philosophy can be challenging, but experience from existing control rooms on what is functioning well and what is not can be used as input. The involvement of experienced operators is crucial for understanding the needs and requirements of technical solutions, as well as their possibilities and limitations.

5.3.5 Presentation of alarms on the screen

Alarms may be presented on the screens as:

- **Overview alarm lists:** A list of alarms, typically the key alarms, displayed in permanently available overview images on operator screens and displays.
- **Detailed alarm lists:** Alarm lists can be accessed in the underlying screen pictures for more detailed investigation.

Some alarms are grouped rather than presented individually. In this case, an extra click on the detailed alarm images will give more information. Fig. 13 shows an example of an alarm list on the ABB Ability™ System 800xA Alarm Management webpage.



Ack	Prio	State	ActiveTime	ObjectName	ObjectDescription	Condition	Message	Cu
☐	2	RTN	18 08:01:33:578	TI_2029_C29	COMP_C29_Temp_State	Temp-HH	Greater than 80.00	
☐	3	RTN	18 08:01:20:578	TI_2029_C29	COMP_C29_Temp_State	Temp-H	Greater than 75.00	
☐	2	RTN	18 08:00:52:078	TI_2077_A1	ReactorTemp_State	Temp-HH	Greater than 80.00	
☐	1	RTN	18 08:00:50:578	PI_2029_C29	COMP_C29_Pres_State	Pressure-LLL	Less than 5.00	
☐	2	RTN	18 08:00:48:077	PI_2029_C29	COMP_C29_Pres_State	Pressure-LL	Less than 10.00	
☐	3	ACT	18 08:00:42:578	PI_2029_C29	COMP_C29_Pres_State	Pressure-L	Less than 20.00	
☐	3	ACT	18 08:00:36:078	TI_2077_A1	ReactorTemp_State	Temp-H	Greater than 75.00	
☐	1	RTN	18 07:59:27:577	PI_2077_A1	ReactorPressure_State	Pressure-LLL	Less than 5.00	
☐	2	RTN	18 07:59:24:577	PI_2077_A1	ReactorPressure_State	Pressure-LL	Less than 10.00	
☐	3	RTN	18 07:59:18:078	PI_2077_A1	ReactorPressure_State	Pressure-L	Less than 20.00	
☐	1	RTN	18 07:58:53:078	TI_2029_C29	COMP_C29_Temp_State	Temp-LLL	Less than 5.00	
☐	2	RTN	18 07:58:48:578	TI_2029_C29	COMP_C29_Temp_State	Temp-LL	Less than 10.00	
☐	3	RTN	18 07:58:40:077	TI_2029_C29	COMP_C29_Temp_State	Temp-L	Less than 20.00	
☐	1	RTN	18 07:55:58:578	TI_2077_A1	ReactorTemp_State	Temp-LLL	Less than 5.00	
☐	2	RTN	18 07:55:49:078	TI_2077_A1	ReactorTemp_State	Temp-LL	Less than 10.00	
☐	3	RTN	18 07:55:32:078	TI_2077_A1	ReactorTemp_State	Temp-L	Less than 20.00	
☒	1	ACT	15 09:51:43:578	Compressor-Drive		DischargeLow	Compressor-DriveTorgue-Low	
☒	1	ACT	15 09:51:43:578	Reactor_ByPass		Red	Reactor_ByPassByPass_BlK	
☒	1	ACT	15 09:51:43:578	Compressor-Hydraulic		Cavitating	Compressor-HydraulicOil-Press-Low	
☒	1	ACT	15 09:51:43:578	IsolationSystem		Unstable	IsolationSystemHelium_Gas_ON	

Fig. 13. Alarm list (ABB)

For each alarm, we notice the following information:

- If the alarm has been acknowledged ("Ack")
- Priority of the alarm (1, 2, or 3) supported by color codes
- State of the alarm here as return to normal (RTN) and active (ACT)
- Active time means how long the alarm has been active. We notice here that many alarms came at the same time
- The object name and description identify where the alarm comes from. For example, TI2029 may indicate that this is a temperature (T) alarm indicator (I) associated with a transmitter with tag number 2029, installed for what we assume is the compressor unit number C29. We may notice that the same transmitter can provide multiple alarms with varying priorities.
- Condition identifying why the alarm was raised. For example, the first alarm from TI 2029 was raised at the setpoint "High" (H), while the second alarm was a "High-High" (HH) condition. H indicates a setpoint where the safety-instrumented system raises an alarm without action. At the same time, HH is a setpoint that involves an action, such as a shutdown (in this case, limited to the compressor). From the sequence of the two alarms, we understand that the temperature has been rising quickly.
- The message provides supporting information. For TI 2029, we note that setpoints are provided for H and HH.

The alarm system typically provides more information about the alarms, such as whether they have been raised repeatedly, shelved, or suppressed. The operators do not have time to study such information during an emergency. However, at regular intervals, they should review such information as a "health check" of the alarm system and its ability to provide necessary support.

5.3.6 Alarm system performance

Alarm system performance is a metric that measures how effectively an alarm system functions in relation to its intended purpose and requirements. One commonly used metric is the alarm rate, defined as the number of alarms raised per unit time. The measured alarm rate can be compared to a maximum allowed alarm rate, for example, expressed in the following way:

Average alarm rate	Consequence
More than 1 alarm per minute	Clearly unacceptable
One alarm every two minutes	Too demanding (for operators) to manage
One alarm every 5 minutes	Manageable
Less than one alarm every 10 minutes	Clearly acceptable

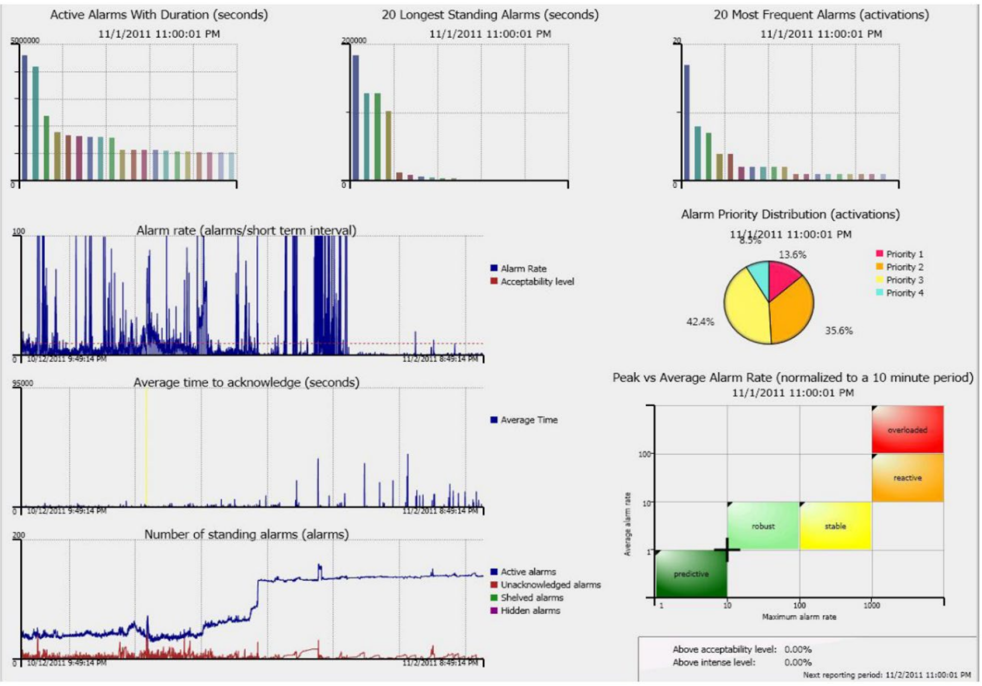


Fig. 14. Alarm performance indicators (ABB)

Other examples of metrics for alarm performance are shown in Fig. 14, such as:

- Which alarms are active right now and for how long they have been active: The operators should investigate if there are critical alarms among these and why they have not been managed sooner.
- The 20 alarms that have been active for the longest time: Operators are further assisted in identifying those alarms where the lack of resolution is of great concern.
- The 20 most frequent alarms: Operators receive assistance in identifying which system parts are responsible for the most alarms and under what operating conditions.
- Alarm rate (frequency of alarms per unit of time).
- Distribution of alarms according to priority: Besides the distribution of alarm priorities, the operators can identify how they can resolve the situation before the safety-instrumented system takes over (on HH or LL setpoints, which would generally be priority 1)
- Average time to acknowledge the alarms.

- The alarm rate, i.e., the number of alarms present per unit of time, for active, non-acknowledged, dismissed (shelved) alarms. The alarm rates can be compared with the maximum rates allowed, taking into account the operators' ability to manage them within the available time.
- Hidden alarms, that is, alarms that are filtered out for several reasons, such as shelving and suppression. This list should be reviewed to determine whether such filtering functions are working as expected and whether the criteria in the alarm specification are met.
- Matrix that indicates the average number of alarms with low, medium, and high (unmanageable, if high) alarm rates.

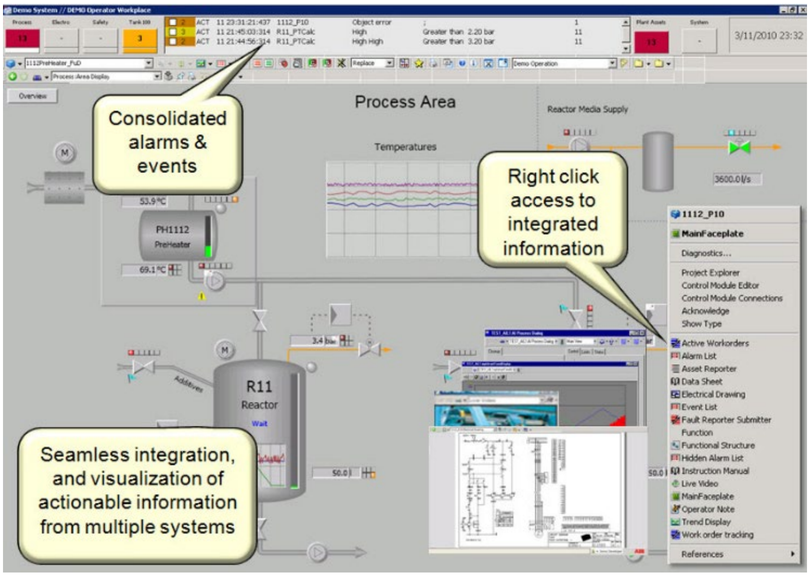


Fig. 15. Alarm presentation to operators (ABB)

It may seem questionable to allow “standing” (active) alarms, i.e., alarms that have not been acknowledged or resolved. However, some of these alarms can arise from equipment that is out of service (typically L and LL alarms), as well as alarms associated with the start-up or ongoing modification work of equipment and process sections. Acknowledging means confirming that the alarm has been set and that the operators have understood its implications and causes. If an alarm is irrelevant, the operators can decide to shelve it (put it aside). The alarm system may also suppress the alarm based on its algorithms. The alarm may recur if the situation is not managed correctly.

Alarms are also presented on the operator screen. One (not too recent) example is shown in Fig. 15. Key information about the alarms is presented at the top, while more in-depth insights can be obtained by clicking further into the alarm menus.

5.4 Utility (or auxiliary) systems

Utility and auxiliary systems are indirectly needed to support safety and control systems. Examples include power generation, hydraulic power systems, instrument air (or pneumatic) systems, water distribution systems, heating, ventilation, and air conditioning (HVAC) systems, telecom systems, and systems that provide chemicals, such as pipeline and vessel cleaning. For simplicity, we will use the term utility system from now on. The focus of this chapter is the following utility systems:

- **Electrical power and earthing systems:**
  Used to generate and distribute power and includes various systems for protection against damage to these systems. Earthing systems are essential for ensuring the safety of people and preventing electromagnetic interference between power distribution and signaling systems, as well as between electronic or programmable devices.

- **Instrument air (or pneumatic) system:**
  Used primarily to operate valves. Air is also completely safe in potentially explosive environments.
- **Hydraulic power system, also called hydraulic power units (HPU):**
  Used for operating larger valves that require much power. Effective when valves are to be kept in position using an enclosed volume.

5.4.1 Power generation and distribution

Electrical power distribution is one of the essential systems in a process plant.

Besides all consumers related to the process operations, the distribution system feed housing facilities, equipment rooms, and control rooms need electrical power. An industrial facility may have a power supply as follows:

- Local power generation at the plant with its power generators
- Power cable from external distribution networks

Land-based facilities typically receive power from an external electrical distribution system, except in remote, isolated areas. Offshore facilities have traditionally generated power, but as more platforms are electrified, local generators are being replaced by cables from the mainland.

What is described above is often referred to as the main power supply, meaning the one the facility relies on during regular operation. However, the primary power generation *may* fail, and the facility must have backup options. Losing power to critical equipment could lead to a loss of control and the inability to understand what is happening in a critical situation.

Just as hospitals and other essential services in society require backup power, industrial facilities do as well. The backup power consists of an emergency power system powered by fuel-powered generators and battery banks (UPS – Uninterruptible Power Supply). The emergency power is dimensioned to serve only the most critical consumers and will not be sufficient to maintain regular operation. UPS is dimensioned to maintain essential safety functions, including an overview of where fire and gas detectors have raised an alarm, the status of firewater pumps, and the status of satellite communication and telecom systems. Emergency lighting often has built-in batteries to provide light in areas for a set period. Equipment like firewater pumps often has its own fuel-powered generators, as its power needs are extensive in securing firewater for a given number of hours.

Power distribution at an industrial facility can vary depending on the processes involved and the extent to which power is generated locally by generators or supplied from an external public distribution network. However, all distribution networks are divided into different power levels, each of which is known as a switchboard. Transformers are installed between switchboards at different power levels. One or more switchboards can be dedicated to emergency power with a standalone backup generator.

Fig. 16 shows a simplified power generation and distribution network for an offshore oil and gas facility, presented as a one-line diagram. The power levels typical of an offshore facility are:

- Main switchboard 11 or 13.8 kV delivered by the main generators. An essential generator may also provide power at this level; however, it has a limited capacity to secure essential services during regular operation if the main generators are unavailable.
- 690 V or 440 V switchboard
- Motor control center (MCC), feeding primarily motors at 690 or 440V
- 400 V switchboard feeding various consumers and smaller motors
- 230 V switchboard feeding various consumers
- Emergency switchboard 690 or 440 V supplies battery backup systems (uninterruptible power supply or UPS) and other consumers to remain operational during an emergency.
  - An emergency power generator secures the power supply after the main generators (and the essential generator) have been shut down.

  - Only equipment essential for managing a situation after an emergency shutdown (ESD) has been triggered is fed from the emergency distribution board.
- Additional emergency switchboards at 400 V feeding various consumers to be connected during an emergency.

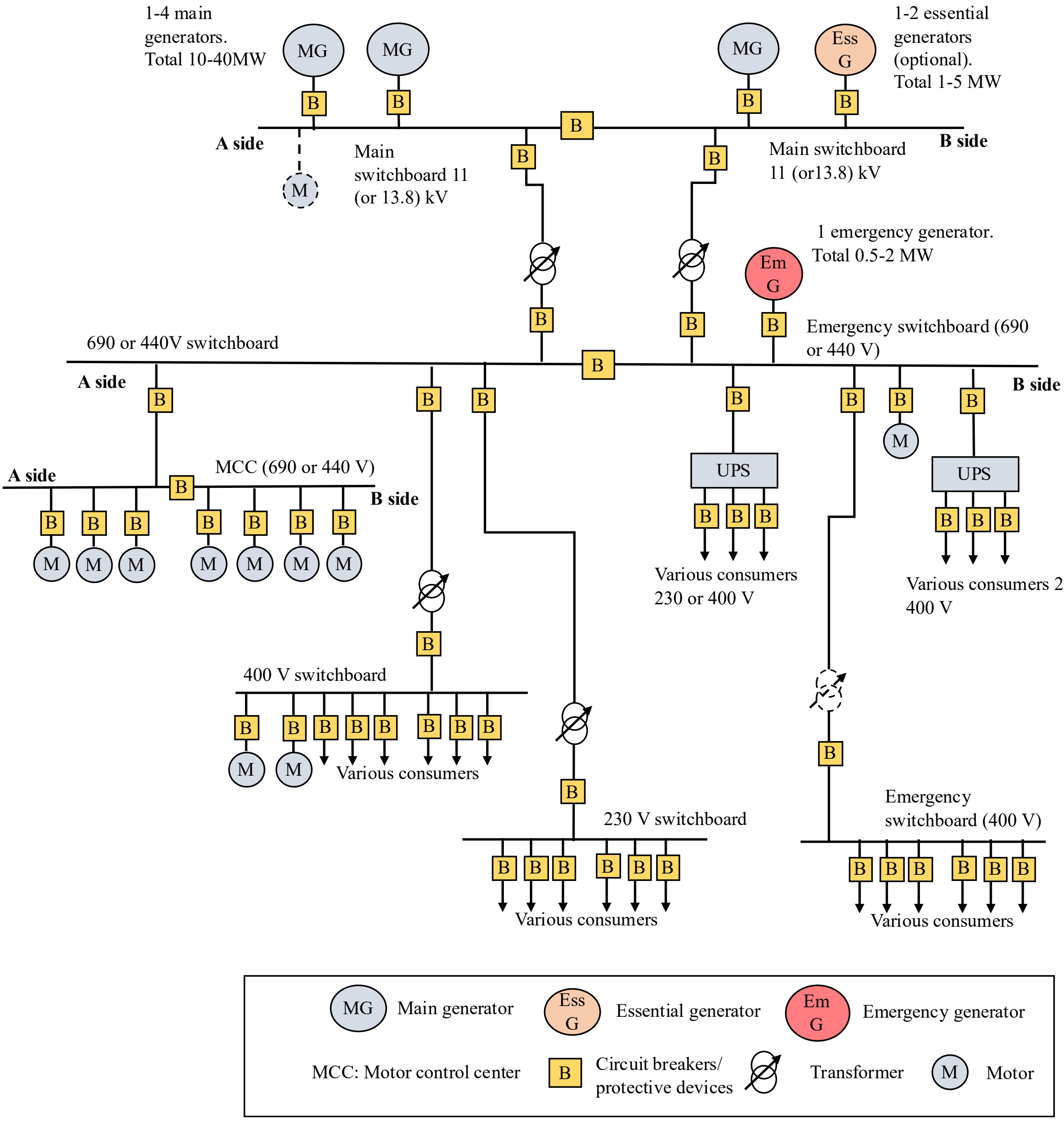


Fig. 16. Power generation and distribution offshore with local generators

Some offshore facilities have been designed or rebuilt to receive power from land. The cable intake (at the facility) can be DC power or AC power, with the AC power cable intake as shown in the power distribution in Fig. 17. At the intake, the facility has a gas-insulated switchboard (GIS) that can connect and disconnect the high-power cable without serving as an ignition source. For DC power cables, large converter halls at the receiving location are required to safely convert DC power to AC.

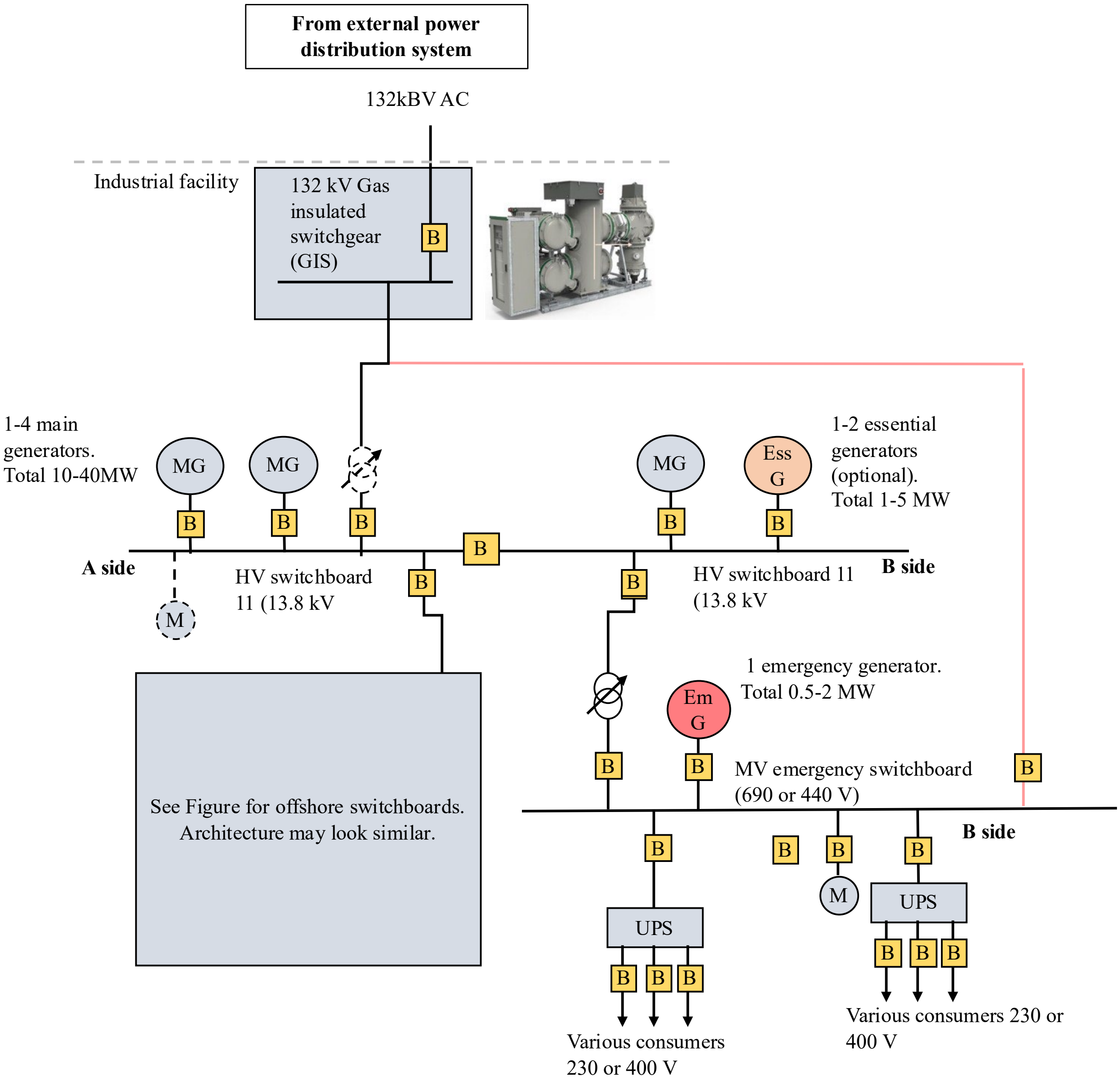


Fig. 17. Power generation and distribution offshore with power cable from land

Circuit breakers and relays are often mounted in cabinets with panels on the outside, as shown in Fig. 18. Only authorized personnel are permitted to enter these areas and open the cabinets. Protective relays are added as sensors to detect excessive currents and automatically operate the breakers to isolate faults.

Fig. 18. Protective equipment

5.4.2 Routing of signal and power cables

There are several practical aspects relating to the planning and installation of cables needed for power supply and signaling:

- Junction boxes and cabinets must often be dimensioned for extra capacity for future expansions or undiscovered needs. Introducing larger cabinets or more junction boxes later can be more costly.
- Outdoor Junction boxes must have sufficient IP (ingress protection) class to prevent dust and humidity intrusion. For example, IP 66 is dust-tight and protected against powerful water jets from any direction.
- Cable trays (frames that secure cables) may require dimensioning for additional capacity. The cable route must resolve potential conflicts with other equipment and provide optimal and safe transitions through walls from one area to the next.
- Power cables routed close to signal cables may be subject to electromagnetic (EMC) noise. It is therefore necessary to maintain a sufficient distance between such cables and to connect the signal cable screens (shielding) to earth.
- Cables must enter junction boxes and cabinets correctly. For example, entry points have specific requirements for cable glands to prevent explosive atmospheres from entering the equipment, box, or panel and causing ignition.
- The choice of cable type (specifically, the sheath or outer layer) depends on the environment and exposure, as well as the type of equipment (critical or non-critical). Examples of alternative types of cables are:
  - Fire resistant
  - Fireproof
  - Oil resistant
  - Resistant to other types of liquids that can damage the cable

5.4.3 Safety rules for work with electrical systems

All electricians may work on low-voltage distribution systems. Working with high-voltage systems requires additional education and certification.

Work on electrical systems can be performed in two ways: with power connected or disconnected. The risk of harm associated with these two alternatives differs significantly. In Norway, it is mandatory that are trained in the corresponding two sets of regulations “Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg»:

- Instruks for arbeid under spenning (regulation for work with power connected)
- Instruks for arbeid på frakoblet anlegg (regulations for work without power connected

It is also mandatory to repeat such training regularly to incorporate any recent updates in the instructions and lessons learned from incidents. Many companies provide such training as a service.

5.4.4 Earthing system

The earthing system is vital for the safe operation of a plant and for the safety of its personnel. Earthing provides the following functions:

- Equalize the voltage potential between equipment or other electrically conductive equipment
- Provide potential references for electrical equipment and signals.

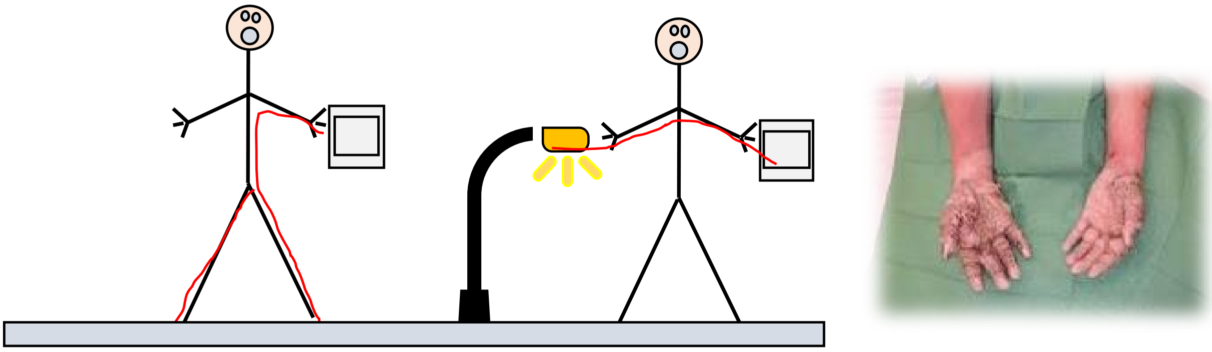


Fig. 19. Examples of current passage

Inadequate earthing can result in your body serving as a path for large currents between voltage levels, e.g., from the ground (0V). Two examples are shown to the left and in the middle of Fig. 19: One shows the current passage from a faulty device to the ground, and another shows the current passage from one faulty device to another. The consequences for the body can be severe, including internal damage and burns.

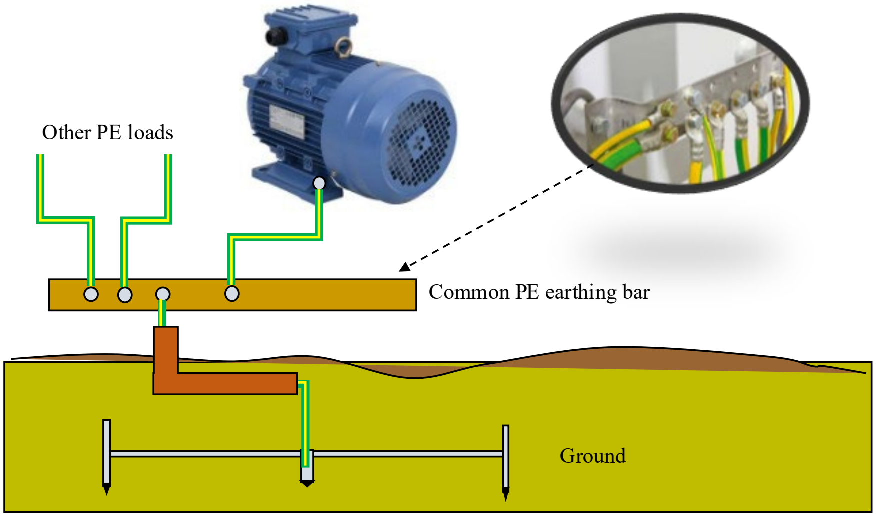


Fig. 20. Protective earth (PE)

An earthing system is split into several sub-systems according to the distinct functions and with different color coding:

- **Protective earth (PE).**
  Color: Always green/yellow.
  Function**:** The PE conductor provides a low-impedance path to earth, ensuring that any fault current is safely diverted away from equipment and personnel. It equalizes exposed conductive parts to earth potential and prevents dangerous touch voltages from developing.
- **Instrumentation earth (IE):**

Color: Green/yellow (or green/yellow conductor marked specifically as IE).
Function: The IE conductor provides a stable 0 V reference for instrumentation circuits, supports shielding against electromagnetic interference, and routes any unintended or stray currents to the main earth point without introducing noise into sensitive measurement signals.

- **Intrinsically safe (IS):**
  Color: Light blue or with a light blue label.
  Function: The IS earth establishes the 0 V reference for Ex i circuits, maintains the integrity of shielding against noise, and ensures that any excessive fault current is safely and rapidly diverted so that the circuit energy remains below ignition-capable levels in hazardous (potentially explosive) atmospheres.

Fig. 20 illustrates the main parts of the protective earth (PE) system:

- PE cables connect electrical equipment to one or more PE earth bars, each of which is connected to the main earth (hovedjord) in the ground.
- The main earth must absorb excessive currents efficiently and quickly, i.e., with high conductivity and low impedance.
- On land, the main ground is a copper cable buried in the soil. Systems without direct contact with the ground, such as ships, floating windmills, and aircraft, require alternative solutions. For example, ship hulls and aircraft bodies are defined as the main earth.

Fig. 21. PE earthing inside a cabinet

The yellow and green cables are usually easy to identify. For example, as shown in Fig. 21 for a cabinet, where a PE cable is fastened to the frame to equalize the power level with the ground.

Fig. 22 illustrates how the PE earthing system is separated from the IE and IS earthing systems.

To understand this figure, the following additional information is helpful:

- **Ex-area:** Indicates an area with a risk of explosion (due to the possibility of dust and/or explosive gases).

- **Ex i:** In an intrinsically safe design, the energy levels are kept below the energy needed to ignite an explosive atmosphere.

- **Non-Ex i**: Refers to other design principles for equipment placed in areas with explosive atmospheres, such as explosion-proof design (Ex d), ignition-proof design (Ex e), and pressurized housing/cabinets (Ex p).

We notice from Fig. 22 that the IS and IE earthing systems connect to the same main earth through their respective earth bars, independently of the PE system.

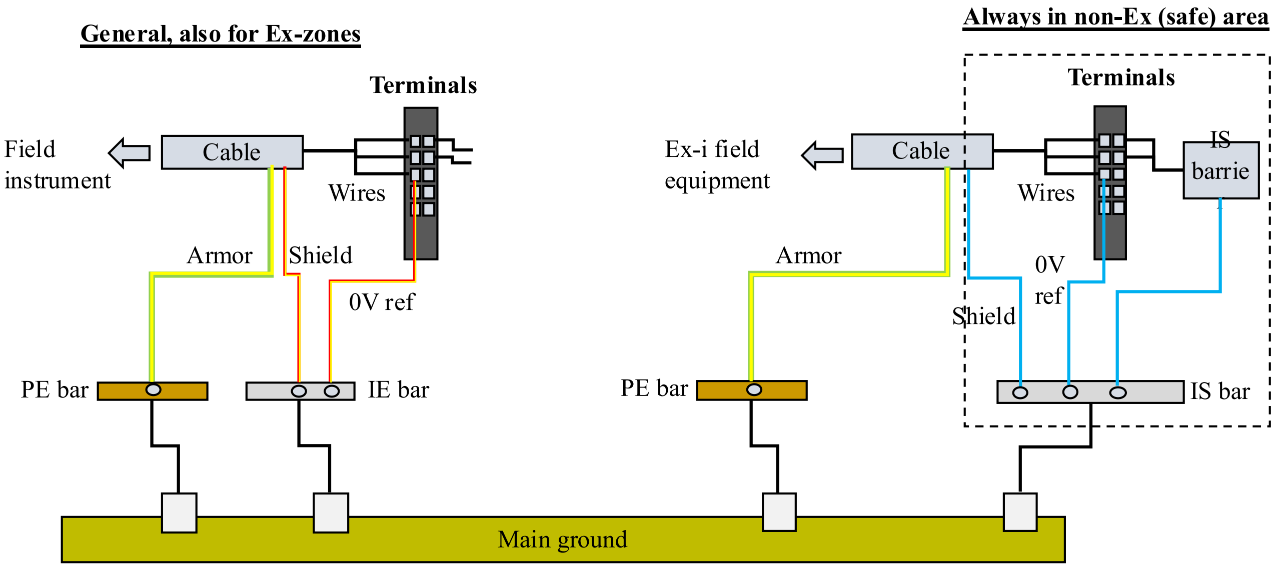


Fig. 22. Separation of PE, IE, and IS earthing

The need for separate earthing systems is illustrated with Fig. 23. The upper illustration shows how an earthing fault in equipment connected to the PE system can spread to other earthing systems if they are connected. When an earth fault in the motor causes current to circulate in the PE system, the voltage across all earthing systems rises. The result may be a new reference level (above zero), which can cause signal transmission and shielding faults. For IS circuits, an increase in voltage levels can cause excessive energy to be transferred into Ex zones, potentially igniting explosive atmospheres that may be present.

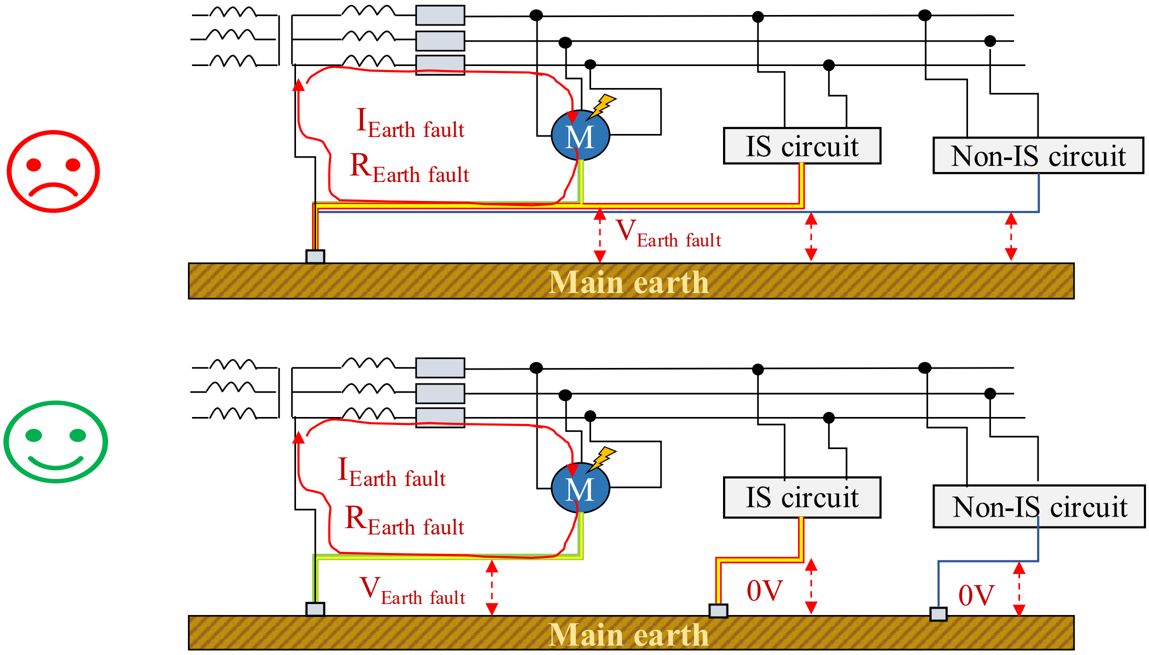


Fig. 23. Why the earthing systems should be separated (inspired by Trainor)

The lower part of Fig. 23 illustrates how the separate PE, IE, and IS earthing systems prevent a change in voltage potential in one system from affecting the others.

5.4.5 Instrument (pneumatic) air system

Instrument air is purified, dry air under pressure. It is commonly used to operate valves and, in rare cases, to carry signals from sensors. For control purposes, the electrical signal from the controller is converted into an air pressure via an analog (current-to-pressure) I/P converter mounted on the control valve. For on/off valves, often used for safety purposes, the pressurized air signal is either added to or removed from the valve by a solenoid-operated control valve.

The system that generates instrument air is sometimes called a compressed air system. Fig. 26 gives an overview of typical parts of such a system:

- Air compressor that pressurizes air taken from the environment
- Wet air receiver tank that receives the pressurized air “as is”, with humidity and some particles
- Filters that remove humidity and dirt/particles
- Dry air receiver that receives compressed air after the filter treatment
- Air distribution piping network that reaches out to the consumers, like valve actuators

According to an older version of the NORSOK P-001 standard, the normal operating pressure of an instrument air system is 8.8 bar.

The instrument distribution network may be complemented with local pressurized air accumulators that compensate for pressure drops when several consumers simultaneously demand supply. Safety valves that are not fail-safe with a spring return may require air accumulators to assist operation if instrument air production is temporarily lost. Filters are located in several places to remove humidity and oil droplets. For example, most of the air consumed during valve operation is released to the environment rather than returned to the receiving tanks.

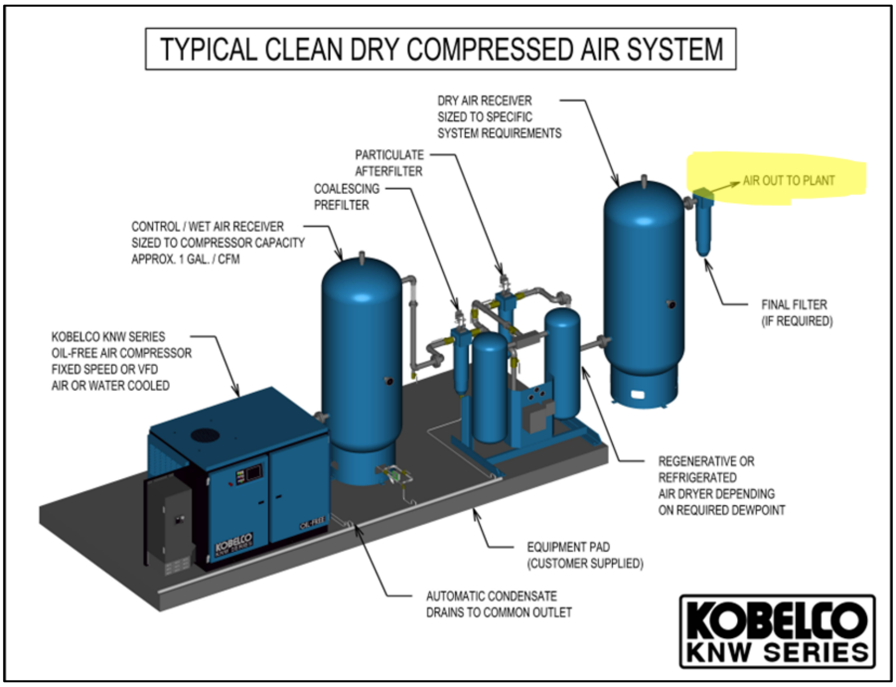


Fig. 24. Typical pneumatic utility system (Roger Machinery Company, Inc.)

Process plants used to rely heavily on instrument air for signal transfer from sensors to actuated devices and for controller implementation. Today, the use of instrument air for control is limited to assisting valve actuation for control and/or safety purposes. An advantage of pneumatic signaling is that it cannot serve as an ignition source in hazardous areas with explosive atmospheres. The downside, of course, was the number of long-reaching tubes and connections, both of which were maintenance-intensive over time and costly to replace or modify. In addition to valve operation, instrument air may be required for specific equipment, such as dryers and absorbers, and for temporary operations, such as maintenance and testing.

5.4.6 Hydraulic power unit (HPU)

The hydraulic power unit serves a purpose similar to instrument air: to provide energy via a pressurized medium. Hydraulic fluids are much less compressible than instrument air, and the power they can provide is much higher and more precise. Another difference is that hydraulic power cannot be released into the environment. Therefore, the hydraulic power consumed by valve operation is returned to the power generation system in a closed loop.

The design of the hydraulic power and distribution system will vary depending on the application and consumption needs. A simplified layout for a distribution system that involves subsea consumers is shown in Fig. 27. Here, a low-pressure and a high-pressure supply system are required. The supply (or pump) side consists of:

- The supply tank is the source for hydraulics to be pressurized by the hydraulic pumps.
- Two sets of hydraulic pumps: one set supplies the low-pressure (LP) distribution network, and another supplies the high-pressure (HP) distribution network. At an offshore facility, the high-pressure (HP) operating pressure is 340 to 790 bar (with some also mentioning 1034 bar), while the low-pressure (LP) pressure is around 200 to 340 bar.
- The pressurized hydraulic fluids are sent through some filters and into the distribution network.
- Each distribution network has a set of accumulators that are continuously refilled when hydraulics are consumed due to valve operations. The accumulators also serve as backups in case the pumps fail or are temporarily taken out of service.
- Filters to remove impurities

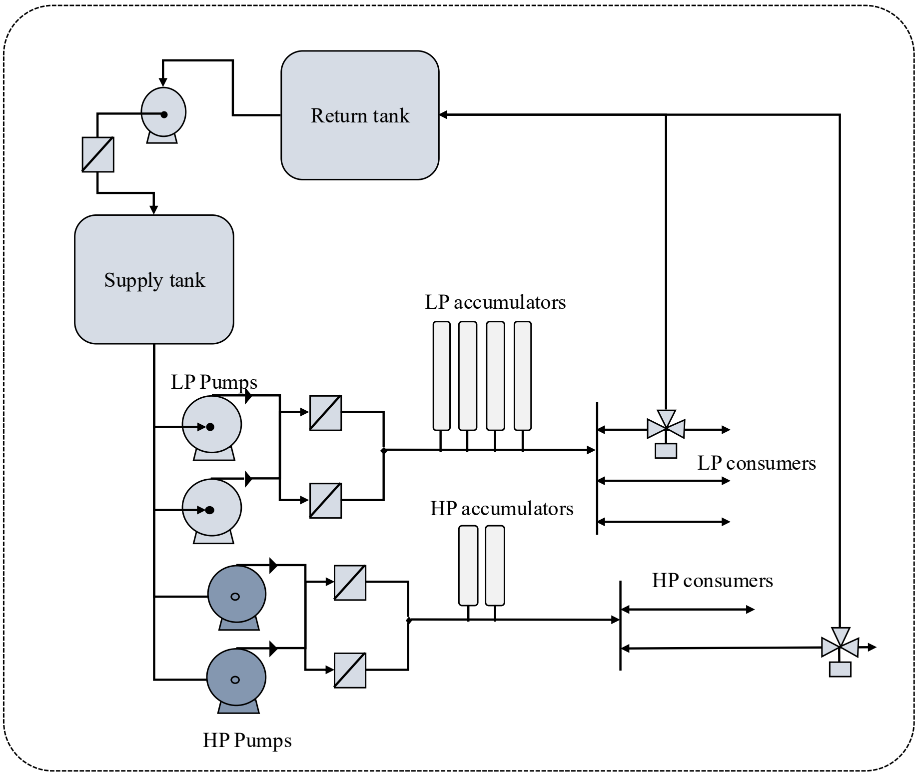


Fig. 25. Hydraulic power generation and distribution system

The return side receives hydraulic fluids from activated equipment. For example, pressurized hydraulics keep several shutdown valves open. To close the valve on command, the hydraulic volume inside the actuator is redirected to the return tank. A non-restricted return is essential for successful valve operation. A local dump valve, located near the valve actuator, may be considered for the most critical valves.

The return (tank) side consists of:

- Return tank (atmospheric pressure)
- A flashing and filling pump that refills the supply tank via filters.

Non-return valves and pressure regulators, which are distributed throughout the system, are not shown.

5.5 Bibliography

- EEMUA 191. (2013). *Alarm Systems - A Guide to Design, Management and Procurement*. Engineering Equipment and Materials Users Association
- EN IEC 62682. (2022). *Management of alarm systems for the process industries*. International Electrotechnical Commission.
- NORSOK I-002. (2021). *Industrial automation and control systems*. Standard Norge.
- NORSOK S-001. (2021). *Technical safety*. Standard Norge.
- Offshore Norway GL 070. (2026). *Application of IEC 61508 and IEC 61511 in the Norwegian Oil and Gas Industry (ed.7)*. Offshore Norge. https://doi.org/https://offshorenorge.no/retningslinjer/arkiv/helse-arbeidsmiljo-og-sikkerhet/teknisk-sikkerhet/070-guidelines-for-the-application-of-iec-61508-and-iec-61511-in-the-petroleum-activities-on-the-continental-shelf/
- SINTEF. (2011). *CRIOP: A scenario method for Crisis Intervention and Operability analysis*. SINTEF. https://doi.org/https://www.sintef.no/projectweb/criop/the-criop-handbook/