DNV

WHEN TRUST MATTERS

MANAGING THE RISKS OF BLACKOUT

For passenger ship owners and operators

GUIDANCE PAPER

Content

Editorial

Most operators of passenger ships occasionally experience blackout with subsequent temporary loss of propulsion. Fortunately, most incidents do not have significant consequences, as they usually occur while in transit in open sea. Still, more can be done to reduce the likelihood that such events occur, so that they do not happen in more high-risk situations. There is also a need to ensure efficient restoration of essential systems once a blackout and/or loss of propulsion has occurred.

The underlying causes of blackouts can often be traced back to the operation of complex integrated systems. In order to reduce the carbon footprint and utilize new technology in a cost-efficient way, the systems tend to become more complex at an ever-increasing level of integration. Today, the complexity and level of system integration challenges our ability to understand in-depth how these systems work. This has become an increasing concern for the whole industry.

The complexity and level of system integration challenges our ability to understand in depth how these systems work.

To support owners and operators in ensuring the safe and reliable operation of their fleet, DNV developed a stepwise approach for managing the risks of blackout and resulting loss of propulsion. This guidance paper provides recommendations and best practices for fleets in operation as well as newbuilds.

We invite you to compare these best practices against your own operations. We want to offer inspiration on how to ensure more robust and fault tolerant operations of your ships.

We look forward to engaging in discussions and receiving your feedback. Together, we can drive the safety in your business forward.

Hans Eivind Siewers

Segment Director Passenger Ships & RoRo

DNV

Reasons for concern

Blackouts and resulting loss of propulsion have long been considered a major accident hazard for the passenger industry. Depending on the operational situation, loss of propulsion may pose an imminent threat to the ship and its passengers and crew.

Blackout
The focus of this guidance paper is on blackout that results in loss of propulsion. Blackout occurs when there is a sudden total loss of electric power in the ship's main power distribution system. This could be caused by various mechanical or electrical failures in the power generation, distribution or propulsion systems, coupled with an ineffective operational response to the failure.

In ships with diesel or gas-electrical propulsion systems, a blackout will cause immediate loss of propulsion and steering. Propulsion is then lost until the standby generator(s) are started, the main source of power feeds the power distribution system, and propulsion units are re-connected.

Depending on the type of failure causing blackout, the system design and operational configuration, the blackout recovery process may be completed within a minute in the best-case scenario, but in the worst case, the recovery process may not happen in time to prevent a disaster.

Research from DNV found that in 2019, the media reported 12 power loss events on cruise ships that resulted in full or partial blackout while in transit or manoeuvring. This was a significant increase from four events in the previous year. These incidents are a driver for stakeholders in the passenger ship industry to stop and reflect on what can be done to reduce the risk of blackout and consequential loss of propulsion, in order to ensure safe operations.

Damage potential
Whether loss of propulsion poses an imminent threat to the ship and its passengers and crew depends on the operational situation. Incidents that occur during operations in confined waterways or during port manoeuvring, transit close to shore, combined with severe weather conditions, have a higher severity potential than incidents occurring while the vessel is in open sea. The time it takes to recover from blackout in these situations is critical, because it may be too late to restore propulsion in time to avoid accidents.

Depending on the type of failure causing blackout, the system design and operational configuration, the blackout recovery process may be completed within a minute in the best-case scenario, but in the worst case, the recovery process may not happen in time to prevent a disaster.

Major incidents may also negatively affect company reputation through global media coverage. Today's incidents almost instantly spread through social media. This may have a major impact on earnings, profit and shareholder value.

Time for a step change in safety

Blackouts should no longer be considered unfortunate or rare events. Through implementing the best practices and recommendations from this guidance paper, the industry can significantly reduce the risks of blackout and loss of propulsion, and thereby take a step change to improving safety.

Purpose of the paper
This guidance paper offers the passenger ship industry best practices to:

- Improve general understanding of the risks associated with blackout and loss of propulsion.
- Reduce the risk of blackout (e.g. by ensuring that power systems are redundant and fault tolerant).
- Ensure fast and reliable means of system recovery.

As such, this guidance paper offers support to improve how we approach and control blackout risk through prevention and recovery mechanisms. Through implementing the best practices and recommendations from this guidance paper, the industry should succeed in reducing the risk.

Scope
This guidance paper is written to predominantly spark discussions with passenger ship operators and owners, such as cruise, RoPax, and expedition/exploration ships. Many of the principles, however, may be extrapolated to other segments, to other safety-related issues, and to other industry stakeholders who play a role in the design, building, procurement and operation of ships, including designers, yards, vessel managers, class and flag.

The primary focus of the guidance paper is on ships with electrical propulsion (i.e. ships where a blackout immediately causes loss of propulsion). The main hazard of concern is loss of propulsion caused by blackout. The scope excludes loss of propulsion that is caused by mechanical failures related to shaft, stern tube bearing, propellers and pods.

A stepwise approach to prevent blackouts
This guidance paper builds on a study that was based on input received from the passenger ship industry and DNV's expert resources. During this study, DNV analysed incident statistics, performed literature reviews, conducted workshops with key industry operators and collaborated with expert resources to gain insight into:

a) The likelihood that blackouts occur
b) The underlying interrelated causes of failures that lead to blackout and consequentially loss of propulsion
c) The factors influencing successful blackout recovery

The outcome of the study is a stepwise approach to managing the risks of blackout as illustrated in Figure 1. This guidance paper is structured around each of the steps and concludes with best practices and recommendations to help the reader prevent a blackout and mitigate its consequences.

FIGURE 1

Stepwise approach to managing the risks of blackout

Step 1: Increase understanding of blackout

In order to achieve a step change in safety for loss of propulsion, it is necessary to gain an overall understanding of causes of blackouts and the regulatory framework. A barrier-based and holistic approach to managing risk offers practical tools and a helpful mindset.

1.1 Investigate the underlying causes of blackout

The purpose of an investigation should always be to maximize the lessons learned from unexpected events to prevent re-occurrence. However, while many organizations invest time and money in performing investigations, they often lack a feedback loop that allows the sharing of lessons learned and that helps the organization to learn from the outcome of an investigation. It is worth reflecting on how many major and minor blackout events are reported and/or investigated, and how many of these investigations have been shared to support organizational learning.

Establishing a feedback loop requires management commitment and a level of risk awareness that acknowledges the importance of incident investigations. This calls for a standardized, systematic and traceable investigation methodology that is embedded in the safety management system (SMS) and that allows organizations to identify the root causes of incidents and to derive the necessary cultural changes.

1.2 Understand the regulatory framework

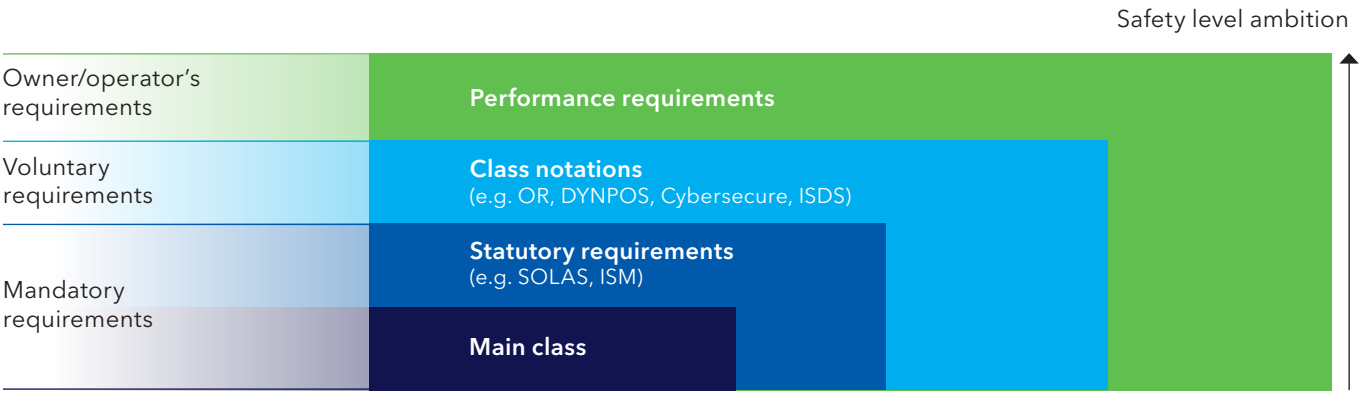
To understand blackout, one needs to understand how the regulatory framework influences ship design and operation. The main class rules of a classification society are the mandatory requirements that generally provide a minimum technical standard (Figure 2). Therefore, vessel owners may be inclined to exceed minimum requirements if they operate under functional requirements and have an ambition to achieve greater redundancy, reliability, operability and maintainability.

As the default requirements for shipyards is to fulfil mandatory class rules and statutory regulations, any improvements to the blackout prevention and recovery system need to be explicitly agreed in the shipyard contract for the vessel.

While main class rules focus mostly on system reliability and response to failures through standards for design, construction, commissioning and compliance inspections, a blackout may be caused by numerous technical or operational failures that may not conflict with the rules.

FIGURE 2

Level of safety based on layers of requirements



In certain market segments, a blackout and even a temporary loss of electrical power, propulsion or manoeuvring capabilities may impose an immediate and high risk, for instance in connection with diving operations, anchor handling or seismic streamlining.

The range of additional DYNPOS and RP class notations extend the requirements of main class and is intended to increase the fault tolerance and minimize the risk of functional loss in exposed operations.

A new class notation, OR, specifically targeting operational reliability, blackout prevention and system recovery in passenger ships was launched in 2021.

The following sections will summarize the rules and requirements concerning blackout prevention and recovery.

Main class requirements on blackout prevention and recovery
The most essential requirements in DNV's main class rules on **blackout prevention** are:

- The power system shall be arranged with automatic load shedding, or load reduction, to prevent overloading of the running generator(s).
- When several generators are running in parallel, tripping of one power unit shall not result in overload or tripping of the remaining unit(s).
- There shall be interlocks to ensure that enough generators are connected before large motors are started.
- Essential consumers serving the same service shall be distributed between the two sections of the main switchboard.
- There shall be discrimination in the electrical protection system to ensure that only the switching device nearest to the fault is activated.

The most essential requirements in DNV's main class rules on **blackout recovery** are:

- There shall be at least two main generator sets arranged for blackout starting, and these generator sets shall be connected to separate busbar sections of the main switchboard.
- Stored energy for blackout recovery:
  - At least two sources of stored energy shall be arranged for blackout recovery. The generator sets shall be divided between the power sources. The capacity shall be enough for three starting attempts on each engine.
  - If power supply to auxiliary systems, such as governors, voltage regulators, switchboard control, fuel supply, etc., is needed for the blackout start, the power supplies to these systems shall be arranged as the energy for starting. The capacity of these power sources shall correspond to the required number of starting attempts and/or last for at least 30 minutes.
- Engines in standby mode will usually be arranged with heating and/or lubrication oil priming. These systems do not have to be supplied during a blackout situation, provided start blocking is not activated within 30 minutes after the blackout.
- Automatic start and connection of the standby generator is required in case of blackout. The standby power source shall be started and connected to the main switchboard within 45 seconds. Essential auxiliaries shall then be automatically re-started.

The 45-second requirement is the maximum time for regaining power on the main switchboard. Still, additional time is required to connect propulsion units back on the grid.

If the vessel has an E0 notation (unmanned machinery), the propulsion plant shall be automatically re-started, or it shall be possible to be manually started from the navigation bridge. The starting arrangement shall be simple to operate.

SOLAS requirements on emergency power systems
The SOLAS requirements state that the main and emergency power systems shall be mutually independent, also with respect to blackout recovery. In case of blackout, the interconnecting feeder between the main and emergency switchboards shall be automatically disconnected, and the two systems shall recover from the blackout independent of each other. If the emergency power source is a generator, it shall be automatically started and supply the required services within 45 seconds.

Blackout recovery of both the main and emergency power systems is tested on board both during the newbuilding phase and annually when in service. The tests shall ensure that blackout recovery of the two systems are mutually independent.

SOLAS requirements for Safe Return to Port (SRtP)
The SRtP regulations apply to passenger ships above a certain size, and the overall intention is to increase the safety level and reduce the likelihood of evacuation. This is achieved through more redundant and segregated system arrangements, providing increased robustness and fault tolerance after incidents of fire or flooding.

Although SRtP does not specifically address blackout events, the SRtP regulations ensure redundancy and segregated machinery arrangements that, depending on the operational configuration, increase the reliability of the propulsion and steering function.

New class notation – Operational Reliability (OR)
A new additional class notation, OR, specifically targeting operational reliability, blackout prevention and system recovery in passenger ships was launched in 2021. The notation builds upon the general principles of the SRtP scheme and extends the requirements with key elements and practices from the dynamic positioning and redundant propulsion class notations. The OR notation addresses three main areas covered by different qualifiers:

ER – enhanced reliability of propulsion, steering and electrical power; minimizing the risk of functional loss and enabling quick restoration
EMR – enhanced manoeuvring reliability, targeting the reliability of the manoeuvring thrusters and the DP system
OP – operational flexibility and predictability during machinery damage or maintenance

Voluntary notations – Redundant propulsion (RP and RP+)
The range of RP notations give additional requirements to ensure that the propulsion and steering systems are redundant and arranged so that after a single failure as specified in the rules, propulsion and steering can be recovered within a specified time. For the RP(2,x) notation, the failure modes include component failure, while for the higher notation RP(3,x), the systems shall be arranged with segregation to also cover incidents of fire or flooding. For both RP(2,x) and RP(3,x), an additional qualifier, +, can be included to further reduce the risk of functional loss; the systems shall be designed for continuous availability.

Voluntary notations – Dynamic positioning (DYNPOS and DPS)
The range of class notations for dynamic positioning cover all types of vessels engaged in any dynamic positioning operation. The requirements to availability, fault tolerance and robustness in the dynamic positioning capabilities escalates with the higher level of the notations. For the highest level, DYNPOS (AUTRO) and DPS(3), the DP systems shall be designed with redundancy and arranged with segregation to provide continuous availability also in the event of component failure or incidents of fire or flooding.

Always be prepared for the unexpected
All owners and operators must have contingency planning for shipboard emergencies (as part of the ISM Code) in place that to some degree can manage the unexpected. Always being prepared for the unexpected is applicable to all operations and to all types of ships. We cannot rule out the unexpected, but this guidance paper can help to manage the expected.

1.3 Apply a barrier approach

The management of major accident risk requires good systems that capture the complexity and reduce the uncertainty associated with major accidents. Barrier management is an approach that enables stakeholders to have a comprehensive and common understanding – from design and throughout operation – of which barriers should be implemented to protect from hazards, and how these barriers should be verified, monitored and maintained.

For the barriers to be successful in preventing hazards from developing into a major accident and in mitigating the consequences of a major accident, barriers need to be managed so that they perform as expected.

Simplified bow tie for blackout

Bow tie is one of many barrier visualizations of risk models that are available to assist in the identification and management of risks. The benefits of using bow ties is that they visualize the risk you are dealing with in just one, easy to understand diagram. The diagram is shaped like a bow tie, creating a clear differentiation between preventive measures (reducing frequency/probability) and mitigating measures (reducing consequences).

Figure 3 shows a simplified bow-tie barrier diagram to present the threats and barriers that contribute to increasing/decreasing the likelihood of blackout and the mitigating barriers to improve recovery. The bow tie is a generic aggregation of multiple Swiss Cheese models [13], each presenting a single event trajectory.

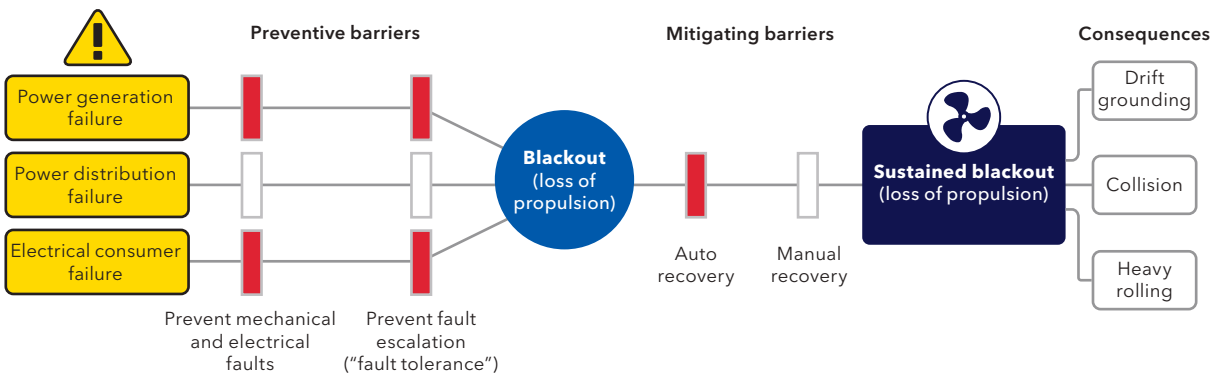
The purpose of this generic bow tie is to be able to apply it to any blackout incident to **a) retrospectively** understand what may have gone wrong during an incident, and **b) proactively** plan to improve the management of the relevant barriers.

In Figure 3, power generation, power distribution and electrical consumer failures (e.g. failures in pods) are threats that may result in blackout (and loss of propulsion). In general, there are barriers to prevent electrical and mechanical failure, and barriers to prevent fault escalation, in case the first barrier fails.

If the preventive safety barriers fail, it will lead to a blackout and ultimately loss of propulsion. Mitigation barriers are then intended to ensure automatic or manual recovery. The objective of the barriers is to avoid sustained loss of propulsion, with potential consequences such as drift grounding, an allision, collision or heavy rolling.

FIGURE 3

Simplified barrier model (bow tie) for blackout / loss of propulsion



1.4 Establish a holistic risk picture

Barriers have a function (a barrier function) that contributes to managing risk. Barriers can be characterized as technical or operational barrier elements. The nature of operational barrier elements can be organizational or individual. Risks can only be controlled if all factors influencing the human (H), organizational (O) and technical (T) barrier elements are identified and managed. A good understanding of how these three components of a system interact is also necessary. This interaction (HOT) is what ultimately manifests itself in human behaviour, indicating how well the system may be functioning.

A HOT approach to safety

DNV always challenges the industry to analyse each element in HOT as part of a larger system: technical findings should be questioned in light of organizational or human influencing factors, human factors were studied in light of technical and organizational factors, and organizational factors were discussed in light of technical and human factors.

As an example, a company's expectation that the ship reaches a port according to schedule can influence whether crew challenges the decision to sail in treacherous weather. Incomplete verification and/or testing of systems can lead to unsafe situations, while insufficient training and experience in combination with poorly designed systems can reduce the likelihood that system failures are detected before they escalate. Taking a HOT approach is relevant across the lifetime of a ship: from the design of a ship, to the operation and maintenance of a ship, as well as to the continuous process of learning from events.

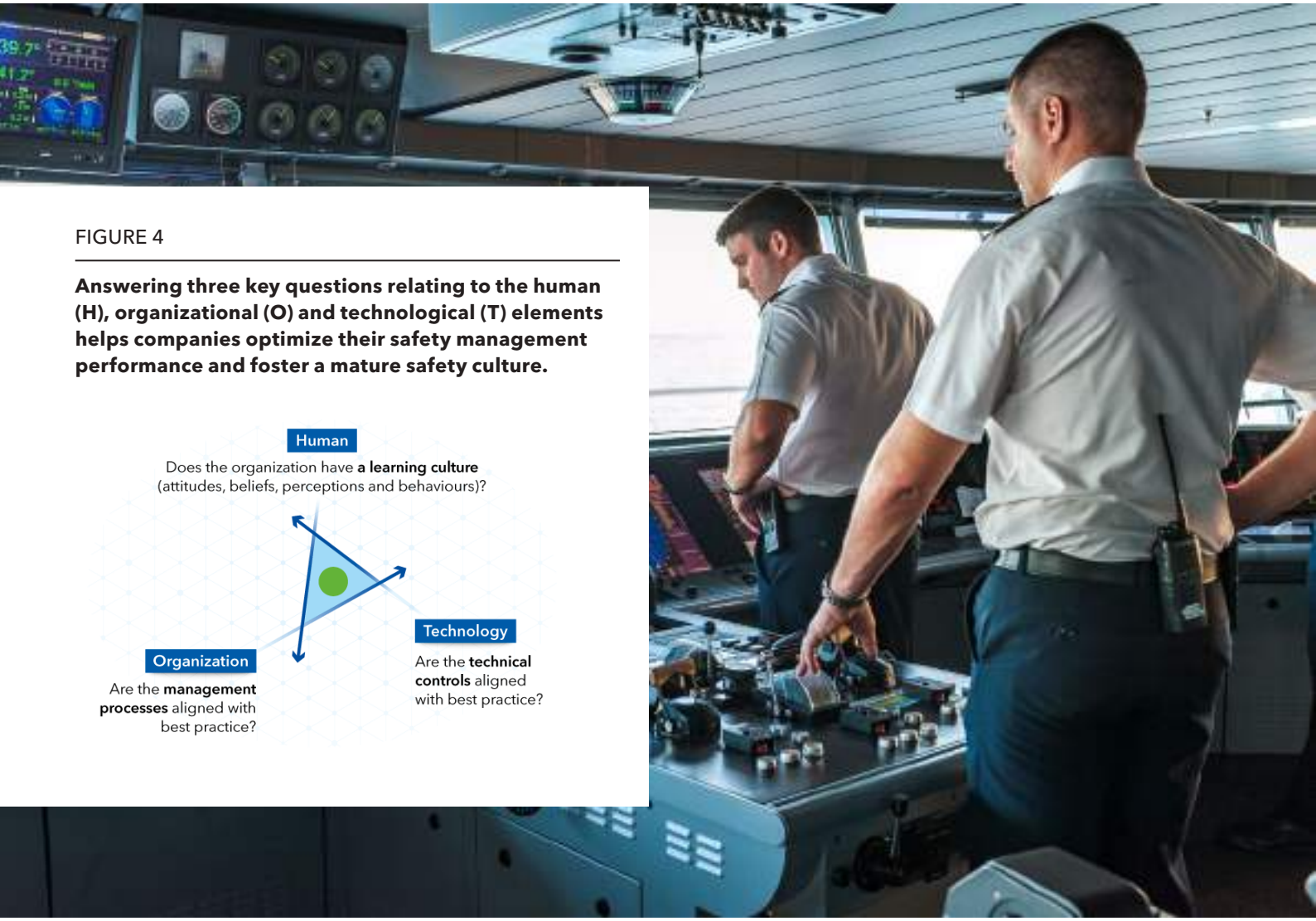


FIGURE 4

Answering three key questions relating to the human (H), organizational (O) and technological (T) elements helps companies optimize their safety management performance and foster a mature safety culture.

1.5 Recommendations and best practices

Recommendations and best practices for vessel managers and crew on board are provided in the table below.

Topic	Relevant for	Recommendations and best practices
Investigate the underlying causes of blackout		Systematically monitor trends in blackouts and propulsion losses, and report KPIs (e.g. recovery time during a drill) to senior management.
		Conduct follow-up meetings with equipment suppliers after incidents.
		Implement a standardized, systematic and traceable incident investigation process. Ensure that the interdependencies between the human, organizational and technological (HOT) factors are addressed in the incident investigation process.
		Share data and knowledge on causes of blackouts (e.g. anonymized data and lessons learned from incident investigations) with fleet, and possibly through joint industry collaborations.
		Report all incidents, near misses and accidents.
Understand the regulatory framework		Be familiar with the limitations of main class requirements regarding blackout and loss of propulsion.
		Understand the main differences between the various voluntary notations.
		Be familiar with the vessel-specific systems and their limitations which can prevent blackout and support recovery of propulsion.
Apply a barrier approach		Use barrier models as a tool to communicate with employees and suppliers about blackout risk and the importance of preventive and mitigating safety barriers.
Establish a holistic risk picture		Ensure that the interdependencies between the HOT elements are addressed in strategies and operational plans for blackout prevention and recovery.
		Communicate an aligned approach that accounts for each of the HOT elements in preventing and mitigating loss of propulsion.
		Create a low-hurdle infrastructure for all employees to communicate feedback on the strategies and operational goals back to the organization.
		Provide feedback to the organization to improve alignment between HOT elements. Examples: Suggestions for changes to training and system design to improve crew performance and meet company expectations.

Step 2: Define the organization's safety ambition and manage conflicting goals

Setting an ambition for minimizing the risk for and mitigating the consequences of loss of propulsion at an organizational level is the first step to ensuring safe and effective operations. Owners and operators need to agree internally on their ambition, so that they do not run the risk of prioritizing other organizational goals at the expense of safety.

2.1 Set your safety ambition

Compliance with existing safety requirements is often not enough to meet the organization's ambition on blackout and loss of propulsion. Historically, updates to rules and regulations have come only after a major accident. Therefore, major passenger ship owners and operators cannot afford to wait for regulations to raise the bar when it comes to safety.

Goal or vision?
An ambition is important because it drives how and to what degree the organization's vision, values and goals with respect to loss of propulsion are supported and implemented by the organization [3]. The organization needs to be clear on whether their ambition is a goal or a vision; the goals are the specific targets that move the organization towards the vision. Although a Zero Vision (e.g. zero blackouts, zero loss of propulsion, zero accidents) is tempting, it may be unrealistic. Setting unrealistic goals means that the goals will be unachievable, which is demotivating to the employees. A more realistic vision would be to aim for as few blackouts as possible and the goals to reach this vision can differ from ship to ship, as each ship has its own context to relate to.

The ambition-setting process
The process of establishing the safety ambition is valuable because it offers the opportunity for senior management to iron out any conflicting goals (see chapter 2.2) that may exist at the top level of the organization. The ambition-setting process should involve all stakeholders, including employees closest to operations, to ensure that all perspectives and relevant experience are made available and taken into consideration.

Once the ambition is set, the organization should prioritize effective communication of the ambition to all managers and employees. Employees do not need to know as many details of the ambition as managers do, but they should know and understand its major intentions. This is to encourage involvement and to ensure ownership of the ambition.

The ambition-setting process should involve all stakeholders, including employees closest to operations, to ensure that all perspectives and relevant experience are available and considered.

Examples of an organization's safety ambition

- Reduce number of loss of propulsion incidents in critical operations to X events per year.
- Reduce number of blackouts / loss of propulsion incidents to X events per year.
- Zero blackouts / loss of propulsion incidents in critical operations.
- Recovery of propulsion within X minutes/seconds.
- Recover propulsion before losing steering speed.
- No single failure of a component shall have a greater effect on the vessel's ability to maintain propulsion and steering than the loss of X generators/thrusters on the same bus section. Such a failure represents loss of X% of power capability.

2.2. Manage conflicting goals

Officers and crew often find themselves amid dilemmas that require management backing and appropriate policies. They may want to choose a more robust machinery mode when entering a critical operation but refrain from doing so because of increased fuel cost. They may want to test a function but cannot because of the itinerary or discomfort to passengers. During the newbuilding phase, sea trial testing is often reduced to the very minimum to save cost at the expense of system reliability.

From a management perspective, the rapid transformations in the industry associated with decarbonization, connectivity and digitalization require more than ever a need to pull the focus back to safety and to establish a safety ambition that lays the foundation for ways of working, for design of technology on board, and for regulatory requirements.

Some transformations and conflicts that may influence how management and crew operate ships today are:

- The focus on lowering costs (both CAPEX and OPEX)
- Stricter rules, regulations and company policies for minimizing the carbon footprint
- The expectation of increased connectivity
- Inter-organizational goals
- Commercial pressures
- Bonus scheme incentives

The focus on lowering costs
Operating in a conjunctural market, stakeholders in shipping seek to lower costs as far as practically possible. Over the years, capital expenditures (CAPEX) have reduced to a minimum, while more is expected to be saved on the par of operating expenses (OPEX). The more negotiations push down prices, the more measures to reduce cost are implemented at the expense of quality and safety. This will influence both the reliability and operability of assets as well as the competence and experience of the people working with the assets. This push and pull between lowering cost and freeing up enough financial resources to fund investments in assets and people can create conflicting goals that stand in the way of the overarching ambition to operate safely and effectively.

Stricter rules, regulations and company policies for minimizing the carbon footprint
The shipping industry is expected to act upon the Paris Agreement and reduce greenhouse gas emissions. In April 2018, the IMO adopted a greenhouse-gas reduction strategy with a vision to decarbonize shipping as soon as possible within this century. The aim is to reduce total greenhouse gas emissions from shipping by at least 50% by 2050.

This strategy will likely call for widespread uptake of zero-carbon fuels, in addition to other energy efficiency measures and new technologies. A natural way to save fuel and reduce emissions is to minimize the number of running engines on board and operate with closed bustie, which may have an impact on the system reliability and operational risk, as explained in chapter 3.2. Other examples are SECA regulations that set limits to SOx levels. If the fuel switchover procedure is done faulty, engines may be affected and shut down.

Expectation towards increased connectivity
Connectivity and digitalization are other significant technological changes in shipping. Organizational goals related to digital business transformations are emerging. This concerns how data is being generated, shared, stored and analysed, at an increasing speed. Increased connectivity between vessels and shore may lead to an increased exposure to cyber threats, and security measures should be implemented as an inherent part of the change management process.

Inter-organizational goals
Departments of many organizations tend to work in silos. This practice is rooted in how organizations historically developed to focus attention first on productivity, followed in time by quality, safety and reliability. As such, each department has goals to meet (higher revenue, lower cost, higher efficiency, highest reliability) which can be overshadowed by risks that threaten the prosperity or survival of the business.

Commercial pressures
The challenge for the workforce is that organizational goals may conflict with each other. To generate higher revenue, the ship must arrive in port on time and turnaround as soon as possible to reach the next destination as per customer expectations. A demanding itinerary contributes to crew fatigue, which can affect quality and safety of operations, especially if the ship has low par levels and there are difficulties in recruiting competent workforce. This creates a catch-22 situation where, despite maximum effort, crew cannot meet all expectations and receive negative feedback (e.g. audit findings, negative appraisals) from stakeholders in the organization whose requirements have not been met.

Bonus scheme incentives
Organizational goals like speed and production are often reinforced by performance agreements or bonuses. However, bonuses can have contradictory effects on the performance of a vessel in different situations. If a port call is to be made, senior on-board officers can feel pressured to do the call despite challenging circumstances, if they are incentivized by guest satisfaction comments which tend to be unfavourable for missed port calls. Similarly, if the ship must enter or depart from a port under challenging environmental conditions, then senior officers who are incentivized to minimize fuel consumption, could be pressured into running fewer engines and compromise safety during the operation.

These incentives should be reconsidered, because they can impede the organization's ability to maintain safe operations and meet their safety goals [4]. The organization will be better prepared to prevent and mitigate critical events, such as loss of propulsion, if incentives are connected to leading indicators such as how many corrective actions are reported.

2.3 Operationalize your commitment to change

Expressing the wish to make a step change in safety, setting a safety ambition and managing conflicting goals are essential foundations for making a difference. However, once this foundation is set, many organizations come to a point where they struggle to convert theory into practice. Often, a department or person is appointed as a dedicated resource to implement the change, but then these persons are left without management backing. This illustrates that managers spend a lot of time on input and output, but less on the throughput.

Management commitment is not only necessary to establish the organization's direction to prevent blackout and loss of propulsion, it is equally important to set aside time and resources to follow through on the organization's ambition, vision and goals. This means that the person who is put in charge of changing organizational practice should get time to work on the task and resources to help perform the task and to share knowledge and insight into what steps should be taken to complete the task successfully.

First, the overall ambition, vision and goals need to be broken down into concrete tasks that can be delegated to responsible entities in the organization. For each task, it should be made clear who is responsible and/or accountable for completing the task, who needs to be consulted, and who needs to be informed about progress. The work that the task entails should be planned along a timeline with mid-term goals, and criteria should be set for how success from mid-term goal to mid-term goal will be measured. This creates a structured and systematic approach that can guide through the process of operationalizing the organization's commitment to reducing the risk of blackout and loss of propulsion.

Management commitment is not only necessary to establish the organization's direction to prevent blackout and loss of propulsion, it is equally important to set aside time and resources to follow through on the organization's ambition, vision and goals.

2.4 Recommendations and best practices

Recommendations and best practices for vessel managers and crew on board are provided in the table below.

Topic	Relevant for	Recommendations and best practices
Establish and implement an ambition		Engage all stakeholders in establishing an ambition on blackout / loss of propulsion that fits the vision, values and goals of the organization with respect to minimizing the risk of blackout and mitigating its consequences.
		Implement the ambition in the organization's strategy and procedures and ensure continuity throughout the safety management system. Ensure that the organization's ambition is embedded in newbuild specifications.
Communicate the ambition		Establish a plan for communicating the ambition from one layer of the organization to the next to ensure that a unified view is shared with all employees.
Give continuous feedback to the organization		Create a low-hurdle infrastructure for: **(a) employees** to communicate any feedback on the organization's ambition and any conflicting goals back to the organization, **(b) the organization** to convert recommendations into actions and demonstrate continuous learning.
		Provide feedback on the organization's safety ambition and on any misalignments between the organization's ambitions and governance documentation, rules, regulations and/or regular practice on board (e.g. company ambition to prioritize safety versus unclear procedures, pressure to arrive on time, lack of relevant training, distracting alarm management systems, and/or missing protective equipment on board).
		Operationalize the safety ambition by identifying how the ambition influences one's daily operations.
Establish compatible goals within the organization		Establish a verification and validation process in which the organization's safety ambition and different department goals are regularly revisited and, if deemed necessary, adjusted to meet industry and/or organizational goals.
		Revisit the organization's goals and department goals to identify any conflicts that need to be resolved. The organizational and departmental goals should span business areas rather than conflict with each other.
		Review key performance indicators, bonus schemes and communicated messages to ensure that they reflect the organization's common safety ambition and how the ambition is translated into compatible goals.

Step 3: Identify measures to ensure safe and reliable vessel operations

To meet both the expectations of stakeholders and the organization's safety ambition, it may be necessary to improve safety and reliability of the existing fleet. The challenge is to establish cost-efficient measures to avoid blackout and loss of propulsion and to ensure quick and reliable recovery. Step 3 points to operational and technical measures that can be implemented by the organization.

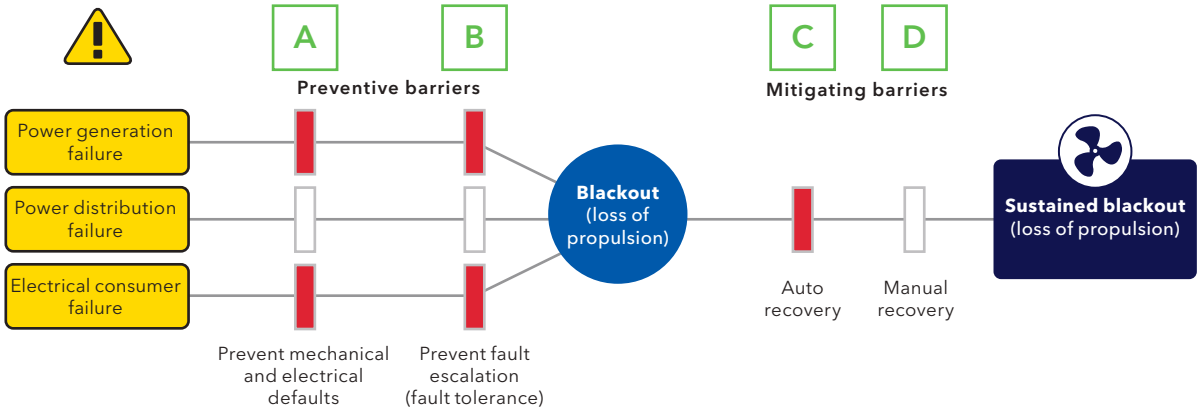
The following seven themes are covered in Step 3. Each theme matches different parts (A–D) of the bow tie as illustrated in Figure 5.

1. Implement robust operating modes [B]
2. Ensure safe and reliable closed-bus operations [B]
3. Ensure correct maintenance and operation of machinery [A, B]
4. Manage software and networks [B, C]
5. Provide decision support for crew [A, B, C, D]
6. Implement enhanced blackout testing [C, D]
7. Implement dynamic-barrier monitoring [A, B, C, D]

FIGURE 5

The themes in Step 3 relate to different parts of the bow tie.

UNDERSTANDING BLACKOUT AND OPERATING IN ACCORDANCE WITH A SAFETY AMBITION THAT HELPS TO MANAGE CONFLICTING GOALS



3.1 Implement robust operating modes

Some passenger ship operators set minimum requirements to machinery arrangements and manning levels based on risk, such as green, yellow and red operating modes. However, it is vital that the criteria for going into these modes are clearly defined, to provide the master with decision support for deciding to go from one operating mode to another. Different operators use different names for the different modes. A green condition typically refers to open waters, yellow for higher traffic density and distance to grounding line, and red for high traffic density, close distance to grounding line or port manoeuvre.

Procedures offering decision support
While it is the master who is responsible for vessel safety, procedures should function as a decision support tool during voyage planning and voyages. As such, procedures should to a larger extent show which conditions should qualify for green/yellow/red operations, depending on:

- Weather criteria:
  e.g. Beaufort level X should lead to operation red.
- Distance to shore/grounding line:
  e.g. distance X nautical mile should lead to status yellow.
- Traffic:
  e.g. high-density ship traffic should lead to status red.
- The condition and state of the vessel, its equipment and any operational limitations.

Likewise, the operating mode instructions should define the machinery arrangements in manoeuvring and transit modes with respect to:

- Power generation:
  - Number of generators online
  - Number of generators in standby
  - Ensuring number of remaining generator(s) after a failure has the capacity to maintain the navigational safety of the ship
  - Configuration of auxiliaries and cross-over lines / cross-feeders (i.e. common or separated auxiliaries for the machinery systems)

- Power distribution:
  - Closed or open bus-tie configuration

- Propulsion units (manoeuvring machinery / steering gear):
  - Number of units online
  - Number of units in standby

Risk-based approach
The procedures and decisions to enter green/yellow/red operations should be risk-based, in accordance with the company's risk acceptance criteria. For example, sailing with only one generator online in calm weather on open sea may not lead to severe post-blackout consequences. The risk acceptance criteria should reflect the company's safety ambition with respect to blackout.

3.2 Ensure safe and reliable closed-bus operations

It is common practice in the industry that vessels operate with a closed bus tie on the main switchboard (hereinafter referred to as closed-bus operations), meaning that redundant power systems are configured as one common system.

There are several benefits of this configuration. However, with a standard protection strategy used on passenger ships today, certain failures in a closed-bus configuration will create a failure propagation path leading to blackout, even with multiple gensets online. Unless additional technical measures are implemented, and the systems are tested and verified accordingly, blackouts may occur. This may be caused by failures such as short circuit, earth fault or excitation control fault and fuel control (speed governor).

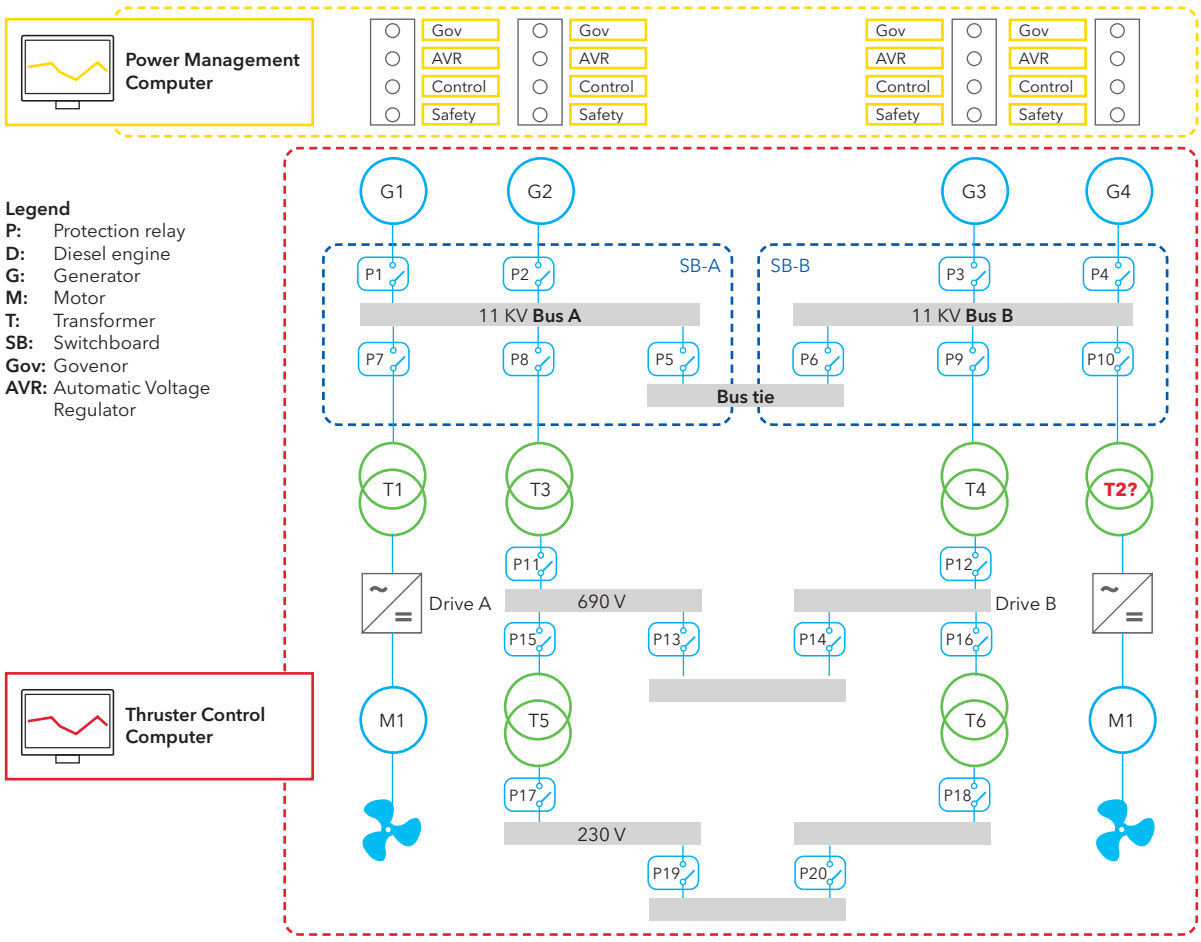
The following sections will focus on the risks associated with closed-bus operation, present typical failure modes and define possible barriers against failure propagation. Note that the only way to identify all failure modes is to run case-by-case analysis and define failures which are applicable for specific design solutions.

Figure 6 shows a simplified single-line diagram of a power generation and distribution system, showing the location of the bus tie. In this set-up, four gensets (diesel generator) are fed to a sectionalized bus (bus A and bus B) by two bus-tie breakers (P5 and P6). The power systems in most passenger ships can be isolated by means of bus-tie breaker(s), and each power system is then fed by at least one generator.

With a standard protection strategy used on passenger ships today, certain failures in a closed-bus configuration will create a failure propagation path leading to blackout, even with multiple gensets online.

FIGURE 6

Simplified single-line diagram of a power generation and distribution system



Advantages and disadvantages of operating with closed and open bus

Common practice in the industry is for vessels to operate with P5 and P6 closed. There are several benefits of this configuration, such as:

- Fewer running generating sets, less total fuel consumption, less consumption of lube oil, improved maintenance intervals, fewer engine hours, less wear and tear on the engine.
- It is more likely that gensets run on optimal load – lower fuel consumption and emission, and reduced environmental footprint.
- Decreased risk of partial blackouts caused by loss of a single generating set.
- Greater flexibility for preventive and corrective maintenance activities (depending on the power system arrangement).
- Increased grid frequency and voltage stability, because more generating sets are connected to the common bus.

However, as pointed out in the previous section, certain failures in a closed-bus configuration will lead to blackout, even with multiple gensets online, unless additional technical measures are implemented.

When operating with open bus, in other words redundant power systems are configured as independent systems (P5 and P6 open), the likelihood of full blackout is significantly reduced, as no electrical failures in bus A may propagate via the bus tie to bus B. However, this does not eliminate the risk for blackout completely, as there may be faults that can affect the expected independence. Examples of such faults are:

- Common mode failures resulting in loss of critical redundant equipment in both bus A and bus B.
- Combination of single failure in bus A, followed by hidden failure in bus B.
- When fully redundant systems are operated in a non-redundant manner; this is especially relevant for all auxiliaries (e.g. lubrication, cooling, and ventilation) when auxiliaries that belong to bus A are powered by bus B.

The benefit with this configuration is that it maintains availability of propulsion/thrusters during most failure modes, maintaining at least partial propulsion. However, the risk is that many failures can cause partial blackout incidents (i.e. loss of one busbar), with consequential reduction in propulsion capability.

The typical failure modes in closed-bus configurations for diesel/gas-electric power plants are listed in Table 1.

Several protection systems and functionalities are distributed throughout the power plant that are designed to handle one specific failure mode, such as load reduction, overspeed of a generator and reverse power. If these functionalities are not coordinated, they may work against each other and escalate the failures. For example, if an engine produces too much power due to a governor failure, it might trip the load reduction functionality. The faulty generator will force the healthy generators into reverse power, and they will be tripped by the reverse power protection. When the faulty generator is the only generator remaining at the switchboard, it will go into overspeed, be tripped and create a blackout.

The switchboard-breaker protections also need to be coordinated to handle a short circuit ride through. The propulsion drives may trip on low voltage before the short circuit protection in the generator breakers and the bus ties. This may, in turn, result in loss of propulsion and essential systems.

Generator set failures

Failure modes that can propagate through systems (i.e. in closed-bus operations) are mostly associated with faulty fuel control systems on the engine or excitation control systems on the alternator. These faults are not easily detected by the protection relay of the faulty generator. It can lead to a disconnection of any healthy unit which becomes overloaded or starts to absorb power to maintain correct system frequency and voltage.

Therefore, good practice for the power systems operating in closed-bus modes is to equip the protection scheme with an additional safety barrier that supervises the generating set's behaviour. This functionality should be realized by independent control systems that have a dedicated set of interfaces, or it should be executed via power management systems with functionalities that extend to generator supervision modules.

Good practice for the power systems operating in closed-bus modes is to equip the protection scheme with an additional safety barrier that supervises the generating set's behaviour.

The supervising systems should be independent from the fuel control system and excitation control system so that there are no common mode failures which would influence the fuel/excitation control system and simultaneously disable or influence the supervising system functionality. In this guidance paper, such a system is referred to as generator protection (GP).

GP should detect the faulty generating set and issue start command to standby generators. Sometimes, it is enough to increase the number of generators to stabilize the power system. If this does not help, and failure deteriorates (or simply develops too fast), the GP should trip the generator associated with the faulty control system. Usually, one more protective barrier is implemented as part of the algorithm, which causes a trip (opening) of the bus-tie breaker(s).

As the GP system has a tripping functionality to all generating-set breakers and bus-tie breakers, it will also represent a potential source of failure. Like all other systems, the GP shall be reviewed with respect to autonomy, architecture and analysis of consequences against spurious trip commands.

Switchboard and associated feeder line failures
The integrity of closed-bus systems depends on the ability of the power distribution grid to detect and isolate the failure and to ensure that the various essential consumers are capable of "riding through" the voltage transients without tripping. Therefore, power systems should be analysed to define what applicable faults might occur in the specific design and discuss the transient nature of the failure.

Busbar protection should primarily be addressed during the newbuild process (see chapter 4.2). However, operators should ensure regular checks of critical circuits which control opening and tripping functions in the breaker's relays and verification of barriers which prevent hidden failures.

System synchronization failures
Power system synchronization (power generation to switchboard and switchboard to switchboard) is a regular activity in all power grids. A faulty synchronization process might result in severe disturbance in both power systems.

Power management system (PMS)
The PMS is a system that automatically controls the power generation and distribution system in accordance with the power demand. It is also a barrier that prevents load variations from causing blackout. However, the increased number of functions, the ability to open or trip all feeders and bus-tie breakers, and the interface with propulsion systems and other vessel-specific functions create potential sources of failures. Since it is a centralized control unit with measurements and command signals to both power systems A and B, failures in the control loops or communication links between the redundant PMS programmable logic controller (PLCs) might lead to blackout, even in open-bus operation. Hence, from a safety perspective, the number of centralized functionalities and connections should be minimized.

TABLE 1
Categorization of failure modes in closed-bus operations

Origin system	Example failures leading to blackout
Generator set	Sudden trip of single generator set without prior warning, together with degraded performance of PMS (i.e. not enough power limitation from preferential trip or load limitation on drives), may potentially cause overload and underfrequency of remaining generator sets in power plant, forming a common electrical system.
	Internal failures in speed control (e.g. governor, actuator, speed pick-ups, load sharing lines) leading to active power imbalance in a common electrical system. This may trip healthy generator sets on reverse power protection.
	Mechanical blockage of fuel rack following a load reduction demand resulting in inability to reduce fuel to the engine. This may cause other generator sets to be offloaded and consequently trip on their reverse power protection.
	Loss of voltage sensing to automatic voltage regulator. This may lead to overexcitation and significant reactive current in the power system. If not detected and isolated fast enough, it may consequently result in tripping breakers on other healthy generator sets due to over/under-voltage.
Switchboard and associated feeder line	Earth fault in outgoing feeder causing trip of generator sets. This may be caused by protection scheme against earth faults that has not been properly coordinated across breakers.
	Short circuit in single outgoing feeder which has not been cleared out by dedicated breaker due to mechanical failure. This may lead to trip of all generator sets from both power systems.
System synchronization	Faulty synchronization device or mechanical fault of generator breaker may lead to unintentional connection of unsynchronized generator set (crash synchronization event) to common electrical system.
Power management system	Calculation of power available signal by PMS is not fast enough to activate load limitation in propulsion drives and consequently mitigate underfrequency effects in case of sudden shutdown of on-line generating set.
Transient states in the power system	Short circuit followed by transient voltage dip in common electrical power system. This may cause under-voltage trip of auxiliary machinery and consequently resulting in shutdown of running generator sets or propulsion.

Examples of typical features and failures in the PMS system that must be considered are:

- Failures in communication links
- Barriers against unintended operations
- Barriers against unintended automatic actions (e.g. actions which could result in unnecessary blackout, partial blackout or unintentional power reduction)
- Signal validation, faulty signal, loss of signal

One of the essential barriers in this regard is to implement a mechanism for the validation of feedback signals to the PMS to prevent:

- Generator (or bus-tie) connection without synchronization
- Unintended load reduction of thrusters
- A decrease in generator frequencies to a level that increases the risk of automatic load reduction of drives and/or tripping of drives
- An increase in frequency to a level that causes systems to trip

Disturbance in power systems operating in closed-bus modes is seen throughout the entire power system. The set points and protective functions in the PMS should be aligned with possible power oscillations to avoid spurious activation of protective functions or spurious blackout detection. Also, all systems activating trip or load reduction of thrusters must be identified.

Transient states in the power system

Failure modes that could cause spurious tripping of running machinery or the spurious opening of circuit breakers cannot be eliminated. Thus, power systems shall be optimized, operated and tuned to be stabilized after a sudden loss of power generation. Severe failures, which cannot be tested, might be analysed by transient state simulations.

3.3 Ensure correct maintenance and operation of machinery

Even though redundancy may be incorporated into the design, there are still failure modes that can contribute to a failure on multiple units within a short period of time. Such incidents are referred to as common mode failures. This chapter will mainly focus on mechanical common mode failures, and the following categories in particular:

- Auxiliaries and sub-system failures
- Maintenance failures
- Operational failures

The failures covered in this chapter are not exhaustive but rather meant as practical examples for what could lead to blackout and loss of propulsion.

EXAMPLE EVENTS

- **Clogged fuel filters:** Fuel tanks can experience accumulation of sludge, water and deposits. In rough weather, the accumulations can swirl up in all tanks simultaneously due to vessel motion and subsequently clog fuel filters.
- **Loss of lube oil suction:** The engine lube-oil system may also be subject to unexpected behaviour during rough vessel motions, either by means of loss of oil suction or triggering of low-level alarm due to sloshing in the lube-oil tanks. As these tanks might be of identical design on all engines, and at the same time be subject to identical motion, it is possible that they will simultaneously experience the same kind of problem with the lube-oil system.
- **Lack of fuel management:** The quality of newly filled fuel can cause severe problems. This may particularly be the case with compatibility with new, compliant fuels. New regulations introduce the need for frequent fuel changeovers which increases these risks. Several blackouts have been caused by two different fuels that coagulated, where the viscous fuel blocked the filters to the generators.
- **Failure in common auxiliary systems:** Redundant machinery systems arranged in separate engine rooms are normally provided with separate auxiliary systems (cooling water, fuel-oil, lub-oil, ventilation, etc). However, these auxiliaries are normally arranged with cross-over pipes/ducts to provide operational flexibility. Operating with common auxiliaries may reduce the operational cost but will also expose the redundant machinery to common mode failures in the auxiliary systems, potentially causing blackout.

Auxiliaries and sub-system failures
Common failures are typically more prone to systems that are connected to the same sub-system, or systems that are designed and built similarly for the redundant systems, and hence will behave similarly. Some of these systems are not necessarily operated every day, making hidden faults in the system and any issues with maintenance and/or watchkeeping routines less apparent.

Maintenance failures
Poorly maintained equipment and mistakes made during maintenance operations can lead to blackout and loss of propulsion.

EXAMPLE EVENTS

- **Maintenance on multiple gensets:** A failure is particularly critical when all DGs are subject to the same maintenance operation. This may be the case when the wrong type of lube oil is filled in all DGs, when the torque of a big end lower half is not sufficiently tightened, when a control valve is left in the wrong position for each engine after a regular maintenance, or when a replaced part is not fit for purpose.
- **Using grease that is not compatible:** Some DGs have manual greasing intervals where a grease gun is used to press new grease into the roller bearing. If grease is used that is not compatible with what is already used, a sudden loss of lubricity with seizure as consequence may occur. If the greasing of the DG is done on all units at the same time as part of a regular maintenance program, then the failure of the bearings can occur for all DGs in a short period of time.
- **Fuel rack free movement:** Fuel rack free movement and links to the governor actuators need frequent inspections to ensure that they are in order and that the fuel racks are free to move. Similarly, fuel pump barrel and plunger interaction should be checked frequently because they may influence the DG operation, especially when the need for large load change appears.
- **Fuel pump plunger-barrel:** During operation, the clearance between the fuel pump plunger and the barrel increases due to wear. If the fuel is changed to lower viscosity, this clearance might be too high for a stable operation of the engine at low speed – and no indications were seen with the higher viscosity fuel.
- **Maintenance of equipment during critical/high risk operations:** Maintenance of equipment during critical operations could reduce the system's ability to handle peak loads and unforeseen situations.

Operational failures
Crew is responsible for optimizing the operation of the ship systems. This includes starting and stopping different sub-systems and switching valves to have the best flow in fuel, air and cooling-water lines. Mistakes in these operations may create situations where the system is not capable of handling the demand for power, and where an operation with reduced redundancy, for instance, might develop to a critical situation. It is essential that the risks involved in these operations are understood and that there is sufficient competence development, mentoring and supervision available to oversee the planning and performance of critical operational tasks

EXAMPLE EVENTS

- **Fuel switchover:** For the vessels where a fuel switchover is required to meet local regulations, the procedure for ensuring a correct switchover is crucial. The switchover procedure is usually slow to avoid thermal shock and should be done at low engine load. Failure to follow this procedure may result in seizure of the fuel pumps or other thermal shock-related issues, affecting all DGs.
- **Valve operations:** If a valve that should be opened is not opened fully, it could restrict the flow of fuel to one or several gensets. If, perhaps through an operational mistake, the load demand then increases, the flow could be insufficient and eventually create a shutdown.

3.4 Manage software and networks

Power generation and distributions systems contain numerous programmable controllers that are coupled together via network connections to a highly integrated system with multiple sub-systems. In most sub-systems like control, monitoring, alarm and safety functions, their functionality is programmed as software functions. In some cases, faults in individual software modules or in the interaction between the sub-systems can cause a blackout.

In general, software-related failures can be divided into the following three main categories:

1. Software defects present at the time of handover of the system/vessel to the owner
2. Software defects introduced during the operation phase when the software or related hardware is updated
3. Erroneous parameterization and configuration of the software

Categories 2 and 3 will be addressed in this section, as they relate mostly to ships in operation, while Category 1 will be addressed in Step 4 (for newbuilds).

Software management
Software differs from hardware components regarding defects and failures, because it does not change characteristics over time. No software failure appears as a result of wear and tear of the software; software failures are a matter of the software behaving unexpectedly to a given set of input parameters.

This means that all software defects are systematic in nature and can be managed with proper quality assurance and verification activities. This includes verifying and validating that the system behaves exactly as expected before it is taken into operation.

The only known way to control the unruly nature of software is to apply a structured process of verification activities throughout the whole software life cycle.

Different versions of software can be verified and deployed in a controlled way while the vessel is in operation by **(a) applying a strict version-control regime**, and by **(b) exchanging relevant meta-data** about the software versions between the system supplier and the vessel operator. If critical functions shall be tested without interfering with the vessel operation, then it will be necessary to use a replica system or a simulator of the target system.

Software defects are systematic in nature and can be managed with proper quality assurance and verification activities.

Software can also easily be made flexible: a single piece of software can be programmed to take into account a number of different parameter settings and different hardware configurations. This makes it even more important to strictly control the parameters, ensuring that the relevant parameterization is indeed verified, and that no unintended changes are made to the parameter values after they have been verified.

Typical software failures that may cause a blackout
There is nothing special about the software involved in power generation and distribution compared to the software involved in any other control system on board the vessel. Yet, because of the potentially severe consequences of blackout, software manufacturers must pay special attention to the design, construction, verification and change management of the software in the involved sub-systems.

EXAMPLE EVENTS

- **Inadequate integration or cooperation between multiple programmable systems** (e.g. gas-fuel mode / diesel fuel mode, damping of control responses, latency of signal communication).
- **Running on an old version operating system** (not updated anymore)
- **Faulty uploads of new software**
- **Old parameters** (which are tuned to fit the vessel's operation) are overwritten and/or reset resulting in blackout caused by usual load scenario.
- **Presence of "dead code" in the control software**
- **Incorrect configuration of a protection relays**
- **Poor tuning of the PMS parameters** that regulates load reduction, leading to fluctuations, etc., which may escalate and result in blackout.
- **Functionality errors/poor logic**, leading to unexpected system behaviour.

3.5 Provide training and decision support for crew

It can be argued that the extent to which ships can diagnose their situation and determine the severity of the consequences of loss of propulsion depends on whether crew on board are appropriately trained and have the necessary experience. But they also need to know and feel that they can get the support they need from the technical systems and from shore. This section will elaborate on training and decision support that is necessary to increase the likelihood of successful human performance.

Enabling successful human intervention
As emphasized by the IMO, the role of the human element is "a complex multi-dimensional issue that affects maritime safety, security and marine environmental protection" [8]. Indeed, the human element is increasingly being recognized as an essential safeguard to maritime safety rather than the main cause of accidents [9].

For the vessel to recover as quickly as possible from loss of propulsion, operators need to be able to act swiftly and appropriately. The probability that a person will correctly perform some system-required activity during a given time period (assuming time is a limiting factor) greatly depends on the combined effects of factors that influence performance [10]. Examples of factors that directly influence operators are access to appropriate information in a user-friendly interface, local communication and collaboration practices, and operator's skills and levels of experience. More latent factors include work processes in the company, company culture, as well as quality and accessibility of procedures and training.

In companies with a mature safety culture, operators are more inclined to raise a red flag before starting or during an operation that they are not comfortable with.

Mature company safety cultures promote safety rather than short-term profit objectives, encourage reporting as a timely way to uncover problems, have standards, rules and procedures in place to prevent non-compliance, and have clear processes in place for communicating critical design and operational factors [10]. In companies with a mature safety culture, operators are more inclined to raise a red flag before starting or during an operation that they are not comfortable with. These operators respond strongly to weak signals, which is a prerequisite for detecting and acting on a critical situation such as loss of propulsion.

Ensure support from shore organization
Adequate shore support is a manifestation of management commitment to minimizing risk and optimizing performance. Adequate shore support means the shoreside organization has identified who is responsible for addressing ship questions about regular operations, for helping the ship during troubleshooting, and for offering practical and technical support in case of an emergency. This also includes offering management support to make decisions that come with a cost.

Perceived support from shore is an important factor that can reduce crew workload during an emergency, which in turn helps them in their ability to make decisions and act appropriately. A common criticism from ships to their shoreside organization is that crew perceive employees in the office as lacking the maritime knowledge and/or updated experience that is necessary to provide ships with the support they need in their day-to-day and exceptional operations.

For ships to quickly recover from a loss of propulsion situation, they need to get prompt access to the required support. The best-in class operators support their fleet in areas of:

- Ship nautical operations: voyage planning, weather routing, port calls, etc.
- Technical operations: Equipment and system malfunction
- Emergency operations: casualty/damage assessment, damage stability and residual strength calculations, contingency plans, 3rd party emergency services, etc.

Training for competence and experience development
Crews should regularly be trained and mentored on the operation of systems and handling of emergency cases such as local operation of the essential functions in the power system (e.g. manual synchronization and load control). The objective of the training should be for crew to be able to recognize and demonstrate their understanding of situations where damage to or maintenance on redundant components can result in reduced fault tolerance.

Crews are essential barriers for preventing the escalation of situations where power and propulsion systems do not recover automatically. Therefore, it is essential that crews know exactly what to do when such a situation arises. This requires crews to be familiar with the vessel-specific systems, and equally important, the limitations of these systems. The expected response to a blackout situation should also be part of the familiarization and handover procedures.

3.6. Implement enhanced blackout testing

Company policies must instruct and allow for adequate blackout testing, explaining requirements with respect to, for example, frequency, responsibilities, and timing of testing. Blackout tests must be arranged regularly in order to verify the system responses to different blackout failures and to contribute to enhancing crew competence on blackout scenarios.

Crew can then:
- Test what manual actions may be required for blackout restoration.
- Learn to identify blackout conditions, observe power system automated actions and troubleshoot problems should the sequence of blackout recovery fail.
- Identify areas for improvement in the technical and operational barriers.
- Become more confident with emergency response procedures and checklists in the event of power system failures.

A proper blackout test involves both the main power system and the emergency generator start-up. This is because a blackout recovery sequence consists of these two parallel processes which start up independently without any operational delays. As the blackout test is a logistic challenge, it should be prepared well in advance.

It should be ensured that the blackout test is created by different conditions (i.e. different failures), to verify system response triggered by different circumstances and to prepare crew for various scenarios.

It is important that tests verify the functions of the blackout prevention measures and the blackout recovery measures (i.e. testing full blackout).

Recommendations and best practices for blackout prevention and recovery tests are provided in Appendix E (blackout prevention) and Appendix F (blackout recovery).

KEY ELEMENTS OF BLACKOUT TESTING PROCEDURES

- **Objective** describing need, motivation and targets.
- **Prerequisites** describing activities which shall be performed prior to the test.
- **Set-up for power system** describing operating mode during the test, how many DGs are running, how the switchboards are assigned to redundancy groups, and which equipment is running prior to the test, etc.
  - Typically, the power system shall be configured as during the regular operation.
  - This part might also describe the specific loading condition for the power plant.
- **Reference** to other documents, procedures, and vessel maintenance schemes.
- **Test method** describing how the test shall be performed.
  - Procedure shall be detailed enough to give an overview of what shall be tested and how.
  - Good practice is to include breakers tags and other information which makes the entire process short and straightforward.
  - The method shall include a list of manual actions with specific information on what should be operated where and how, so that the procedure can be understood irrespective of crew rotation.
- **Expected results** describing how the power system shall prevent and/or recover from blackout, how the power system shall split and what the expected time for:
  - Power generation start-up
  - Power generation connection to main switchboards and synchronization with system (if necessary)
  - Propulsion recovery
- **Results found** describing the real results. If the results found deviate from results expected, this shall be described, explained and concluded for acceptance or rejection.
- **Comments to note,** such as additional information, drawings or sketches.

3.7 Implement dynamic-barrier monitoring

The barrier approach described in chapter 1.3 created a theoretical foundation for the project, which resulted in a simplified bow tie that facilitates communication about loss of propulsion. However, in order to use barrier models as decision support tools in daily operations, the principles of dynamic barrier monitoring should be applied.

Monitoring the health status of safety barriers
Barrier performance is not static, meaning that the integrity of a barrier (its status) may degrade over time. This makes establishing the status of the barrier difficult. Dynamic-barrier monitoring ensures continuous insight into the barrier health status and enables real-time decision support. A live status dashboard alerts crews and management teams about degraded barriers and how the risk levels may potentially increase unless mitigating actions are implemented.

Dynamic-barrier monitoring uses quantitative data (e.g. by sensor feeds) or qualitative input (e.g. through assessments). The figure below illustrates the process of building a barrier model, followed by applying dynamic checklists (i.e. reporting on barrier status) via applications to generate an overall risk status.

FIGURE 7

Example of a dynamic-barrier approach

3.8 Recommendations and best practices

Recommendations and best practices for vessel managers and crew on board are provided in the table below.

Topic	Relevant for	Recommendations and best practices
Implement robust operating modes		Ensure that procedures for power system and propulsion arrangement (e.g. green, yellow, red modes) are based on operational exposure, e.g. weather states (Beaufort level), distance to shoreline, traffic density and operational status of the vessel .
		As part of the procedures, define the vessel's critical/high risk operations and corresponding 'safest mode of operation'.
		Clarify what is expected from the crew in different operation modes.
		Provide feedback on procedures, malfunctioning systems and report discrepancies between the procedures and any alternative practices on board.
Ensure safe and reliable closed-bus operations		Implement more advanced protection measures to ensure fuel and voltage control of gensets (e.g. generator protection [GP]).
		Ensure maintenance/overhaul of speed governors and correct automatic voltage regulator (AVR) settings.
		Maintain the integrity of switchboard and associated feeder lines: - Implement checks of critical circuits that control opening and tripping functions in breaker's relays. - Ensure that bus-tie cables are mechanically protected and insulated, and that busbars in switchboards are insulated.
		Maintain the integrity of system synchronization by implementing synchronization operations in the operational procedures. Avoid switchboard-to-switchboard synchronization during critical operating modes.
		Maintain the integrity of PMS systems by: - Monitoring hidden failures in trip circuits for the generator and tie-breaker. - Implementing high-integrity serial communication or direct HW open command signals to each generator and bus-tie breaker. - Implementing redundant open command signals to each generator and tie-breaker. - Providing clear indications of local/remote status of the tie-breakers, making autonomy and distribution of functionality available. - Implementing dual action functionality for preventing unintended acts of operation and ensuring validation of feedback signals to PMS.
		Ensure that desktop studies (e.g. FMEA) are supported by dynamic computer simulations. Simulations should address failures that cannot be tested and cannot be concluded on during a regular desktop exercise such as in FMEAs (e.g. transient states and "ride through" verification).
Ensure correct maintenance and operation of machinery		Ensure that procedures address common failure modes and maintenance operations that could potentially result in reduced fault tolerance.
		Ensure that no simultaneous maintenance and upgrade of similar equipment is performed and identify where equpment maintenance should be avoided.
		Ensure that overhauled or upgraded equipment is thoroughly tested before sailing.
		Ensure that newly filled fuel is not used and mixed with other fuel before the test results confirm compatibility.

Topic	Relevant for	Recommendations and best practices
Manage software and networks		Appoint an accountable/responsible person to follow-up on software updates that are conducted on board. This OT position (engine department) should be separated from an IT position, as it is more focused on network machinery and automation as opposed to software and network issues (hotel department).
		Ensure comprehensive verification and validation processes before new software versions are put in operation (i.e. implement proper change management).
		Actual tests should be performed on board and in simulators (if possible). Special attention should be put on system safety-critical parameters.
		Refrain from making changes to software during critical operations.
		The operator should also ask for records that show that the suppliers have indeed performed sufficient verification activities on the software.
Provide training and decision support for crew		Establish a competence development plan for crew to demonstrate their understanding of and ability to operate systems, including emergency cases, e.g. local operation of the essential functions in the power system (e.g. manual synchronization and load control) and cases where power and propulsion systems do not recover automatically from blackout.
		Ensure that the crew understands and recognizes situations where damage to or maintenance on redundant components can result in reduced fault tolerance.
		Perform a human-reliability analysis (HRA) to verify that the system provides the necessary support for users to timely act on threats to and escalations following loss of propulsion.
		Include progress of the continuous and iterative improvement process of the alert management system in the safety management system (SMS).
		Ensure that roles, responsibilities and training/competence requirements for the shore-support team are defined (incl. designated person ashore [DPA] responsibilities).
		Study the organizational structure of dedicated resources who can assist during troubleshooting and emergency situations.
Implement enhanced blackout testing		Perform a job safe assessment prior to testing.
		Perform a partial blackout test prior to the full blackout test. This will highlight whether the power system is free from any items that could fail the blackout recovery sequence, and whether a healthy, energized redundancy group has no unintentional crossovers with the redundant group that failed.
		An extension of this test is to leave the one redundancy group in failed condition for a longer period of time (typically for 30 minutes which is equivalent to typical UPS units discharge time) to verify that all essential vessel capabilities are maintained. Alternatively, disconnect batteries in UPS units prior to the test, to verify that the healthy side is fully operational during the partial blackout. This simulates worst case failure design.
		Consider recommendations and best practices for blackout prevention test and blackout recovery test provided in Appendices E and F, respectively.
Apply dynamic barrier reporting and monitoring		Use dynamic-barrier models as decision support tools in daily operations and include barrier condition reporting in vessel manager inspection reporting

Step 4: Identify measures to ensure safe and reliable newbuilds

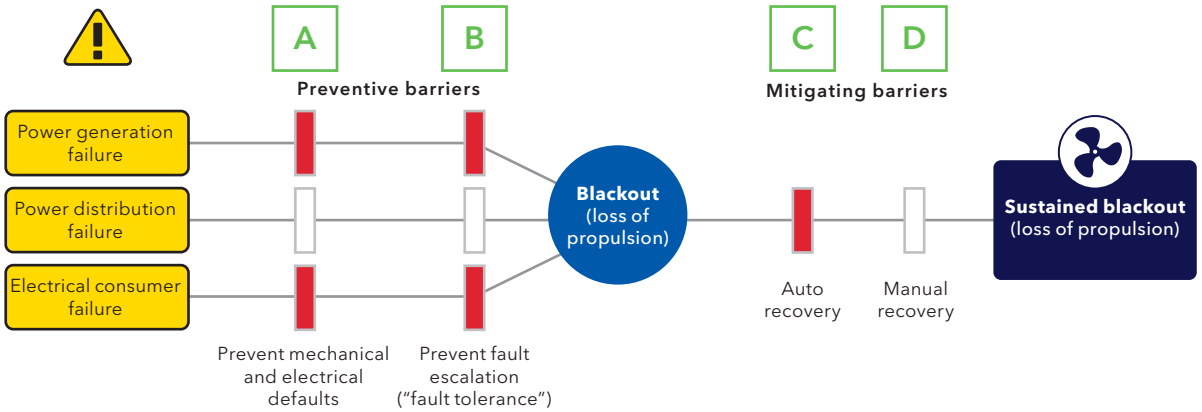
To meet the expectations of stakeholders and the organization's safety ambition, it may be necessary to improve safety and reliability of newbuilds. The challenge is to establish cost-efficient measures to avoid loss of propulsion and to ensure quick and reliable recovery. Step 4 points to technical measures that can be implemented by the organization.

The following five themes are covered in Step 4. Each of the themes matches different parts of the bow tie as illustrated in Figure 8.

1. Human-centred design [A, B, C, D]
2. Ensure robust design for closed-bus operations [B, C]
3. Improved integration, testing and verification [A, B, C, D]
4. Design effective blackout recovery systems [C, D]
5. Utilize battery systems [B, C]

FIGURE 8

The themes in Step 4 relate to different parts of the bow tie.



UNDERSTANDING BLACKOUT AND OPERATING IN ACCORDANCE WITH A SAFETY AMBITION THAT HELPS TO MANAGE CONFLICTING GOALS

4.1 Apply the principles of human-centred design

Historically, there has been a tendency to blame the operator and over-rely on training rather than creating systematic improvements in human performance through improved system design [10]. Although training is important, people will still make mistakes if the system is not designed to meet human capabilities and limitations. Also, a system that is well-designed and consistent with users' needs is easier to operate and therefore easier to train, potentially reducing training requirements as well as improving human performance. As such, the focus should not lie on operator errors alone, but rather on how operator errors are symptoms of sub-optimally designed systems. Lack of human-centred design manifests itself in issues with user-friendly design, maintenance, testing and verification. These issues are covered in detail in the remaining parts of Step 4.

Improving human performance through improved system design

Operators work in a context that shapes their perceptions, decisions and actions. This is particularly the case in such an acute situation as during loss of propulsion, where operators are under pressure and promptly need to make sense of their situation and act accordingly. Therefore, to understand why operators make mistakes, one must put oneself in the shoes of the operator. This requires close cooperation between designer and end-user, testing and revising design in an iterative process (ISO 9241-210:2010). This helps to uncover any discrepancies between how the tasks are expected to be performed ("work as imagined") compared to how the tasks are actually performed ("work as done"). The company should then act to understand why there is a misalignment between work as imagined versus work as done and how the gap can be closed.

Design of alarm systems

An alarm management system should alert, inform and guide operators, allowing them to diagnose problems and keep the vessel operating within its "safe envelope" [5]. Yet, despite the abundance of guidelines, best practices, international and national requirements, and class- and company-specific rules, alarms are often said to be least useful when they are most necessary. Operators are distracted by nuisance alarms, experience unnecessarily high workloads from redundant alerts, struggle with alarm texts that are difficult to understand, and are overwhelmed by the amount of non-critical information that is presented to them [6].

This shows that current practice in the maritime industry on alarm management does not take into account the strengths and limitations of human perception and performance. The result is that the weight of the responsibility for safe and efficient operations is mostly placed more on the shoulders of the operator.

Current practice in the maritime industry on alarm management does not take into account the strengths and limitations of human perception and performance.

There are many reasons for why the design of alarm management systems has become so complicated that it has lost sight of the needs of the end-user. Some of them are:

- The lack of system integration where each sub-system adheres to its own alerts.
- The design of systems is sometimes focused on normal state operations rather than on emergency situations, resulting in the triggering of unnecessarily many alerts.
- The link between system modifications and/or changes and the introduction of new alerts may be missing. There may be an imbalance between what is considered a hazard and what is therefore alerted, compared to the risk of the system as a whole.
- Alarms are often put in place because it is difficult to automate a process and because they are designed to protect the machinery. This creates a control system that puts the responsibility to act on the operator, and it thereby relies on the operator's perception of safety.
- There may not be a clear enough link between a company's alert system philosophy (if it even exists), redundancy and causality underlying major accident hazards such as loss of propulsion.

Presenting what is most relevant to the end-user
The maritime industry should expand its view on an alarm management system from a traditional view of a system for logging events (mostly of interest to an engineer) to a more user-centered definition (i.e. presenting that what is most relevant to the end-user). This requires improved system integration, meaning that the roles and responsibilities of the stakeholders involved in alarm management system design are defined, that the number of alarms that have access to the end-user are reduced, and that the presentation of alarms is improved [7] (see also chapter 4.3).

KEY PRINCIPLES OF ALARM DESIGN AND MANAGEMENT

- **Alarms should direct the operator's attention** towards vessel conditions requiring timely assessment or action.
- **Alarms should inform** and guide required operator action.
- **Every alarm should be useful** and relevant to the operator and have a defined response.
- **Alarm levels should be set** such that the operators have enough time to carry out their defined response before the situation escalates.
- **The alarm system is to accommodate** human capabilities and limitations.

4.2 Ensure robust design for closed-bus operations

In the passenger and cruise segment, it is common practice to operate the power plant with closed-bus-tie-breakers. It is therefore essential to consider robust design for closed-bus operations in the design phase. This includes implementing more advanced generator protection capable of handling various failures related to voltage-related failures (AVR) or governor (fuel-related failures), which basic generator protection will fail to handle.

It involves using high-integrity switchboards and implementing measures to reduce the risk of connection of non-synchronized power systems. Finally, it requires measures to reduce the risk of PMS failures and to ensure power system stabilization.

Detailed recommendations and best practices for enhanced protection measures for safe and reliable closed-bus operations are provided in Appendix C. The configuration and operations with closed-bus in operation (chapter 3.2) are also relevant.

4.3 Improved integration, testing and verification

The industry is facing increasing demands towards complexity and efficiency during a newbuilding process. Yards need to meet delivery deadlines and integrate increasingly complex systems into the newbuilds. That combination of complexity of integrated systems and time pressure often introduces risks related to software failures that are still present when the vessel is handed over to the owner.

Testing and verification of the robustness and functionality of integrated systems is essential for the shipowner to rule out failures during operation. Too often, issues come up after vessel delivery. Thoroughly tested and verified safety critical systems during early newbuild phase will lead to both cost efficiencies for yards during commissioning and sea trials, and for more robust and reliable systems during operation for the ship operators.

Detailed recommendations and best practices for enhanced integration and verification during newbuilding processes are provided in Appendix C.

Maintaining integrity in computer networks

The main challenge with computer networks in a power generation and distribution system is that it may not be clear who is responsible for the totality of the network and its performance. Even if the network design from the individual suppliers has been through testing as a part of the class approval process, there may be a challenge to get all parts working together as whole. Not all companies have dedicated OT operators and rely on their IT department to cover all issues concerning network machinery and automation.

Even if cabled Ethernet-based networks are supposedly "plug and play", there may be some details in the different systems' communication mechanisms that impact the interaction between the systems. This is especially true in the cases where the network has a high load, either because of high normal traffic, or because of a defect leading to a network storm.

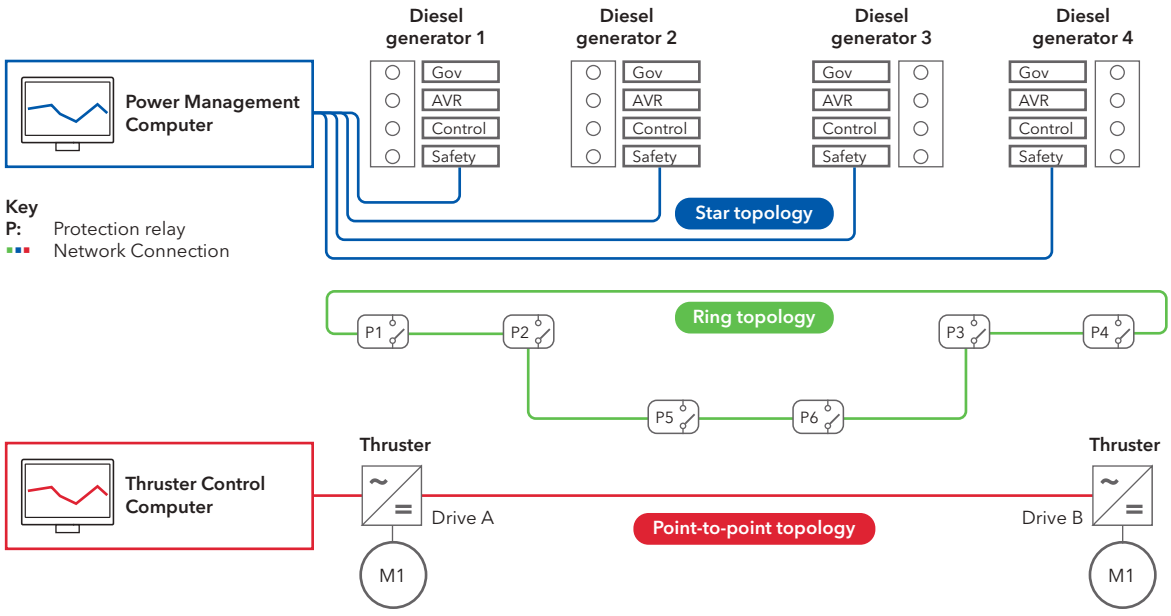
The PLCs in the different redundancy groups may be connected. This might lead to the spreading of a failure to several redundancy groups, such as in a network storm.

The topology (design) of the network also determines its robustness in case of failures and network storms. Ring, bus, mesh and star topologies are common topology variants that show different tolerances for and behaviours during individual failure scenarios. It is also common to apply double network (e.g. double ring) for critical systems to increase robustness towards failures. However, this requires more cables and configuration and may lead to unexpected behaviours.

It is important that the consequences of high-load and failure scenarios for the actual network design are examined and understood. Even in the simple example shown in Figure 9, at least three different computer networks are present. These may again be connected to an engineering station or shore to allow for maintenance and trouble-shooting. The networks may also contain different kinds of network switches and routers.

FIGURE 9

Simplified view of the network connections with different topologies



4.4 Design effective blackout-recovery systems

During most blackouts, the power-generation system starts up quickly without significant delays in the restoration process. However, there are several conditions that can hinder successful recovery from a blackout even if the power management system is operating correctly.

Therefore, it is essential to design the blackout-recovery system in a simple way, and to test the blackout recovery on a regular basis throughout the lifetime of the vessel. Recommendations and best practices for enhanced blackout recovery reliability is provided in Appendix C.

TYPICAL REASONS FOR FAILURE IN AUTOMATIC BLACKOUT RECOVERY

- **Interlocks that may not have been properly evaluated and tested** may delay or fail blackout recovery on every level of the power system.
- **The complexity in interfaces** and the high number of permissions and blocking signals increase the risk of failure.
- **Failure mechanisms which led to the blackout incident may trigger safety functions** that disable machinery start-up or set HV breakers to trip and block a position. The system needs to be intelligent enough to move to the next separate system or start this system up at the same time.
- **Automated blackout recovery requires detailed tuning** to coordinate signals exchange between the power management system, HV system, drives, and other control systems. Even minor changes in logic, during the maintenance or service activities, can disable the recovery process. Any change creates a recovery situation which requires appropriate procedures and permissions.

4.5 Utilize battery systems

More and more energy storage systems based on batteries are being installed on smaller RoPax and expedition vessels with smaller propulsion engines. Although this trend is mainly driven by environmental regulations and the ambitions to save fuel, batteries can also be utilized to reduce the risk of blackout.

Installing battery systems is neither straightforward nor cheap. It increases the complexity of the electrical systems and requires more advanced controllers for the power flow. Further, batteries increase the investment cost, they need to be replaced after approximately ten years, and battery installation requires maintenance and extra space on board. Nevertheless, there are several important advantages of having battery systems on board to prevent blackout and increase safety.

Bridging the power gap
Batteries can store energy for a limited amount of time, but for many failure modes, a battery can bridge the power gap during a power outage until a standby generator is online. Such a transitional source of power is a requirement in passenger ships. Batteries that are large enough can therefore be used to prevent loss of propulsion in passenger ships. A local battery system can also support power to the steering gear, thereby preventing loss of steering during blackout.

Batteries will have energy for a limited amount of time, but for many failure modes a battery can bridge the power gap until a standby generator is online.

Large dynamic load changes
Batteries can also be used to slow down large load changes by taking energy from the batteries while the engines are ramping up. A gas engine that may have problems with delivering power during large dynamic load changes could greatly benefit from battery assistance, as this prevents the shutdown of generators and, ultimately, blackout.

The batteries could also be used for preventing power fluctuations. The batteries can deliver its dynamic power much faster than combustion engines. This is typically an issue on installations with high loads and smaller power-generating sources.

Load levelling
Battery system installations can be used for load levelling, where they allow the engines to run on optimum load (i.e. enhancing fuel efficiency) while the batteries take the dynamic load variations. Large enough batteries can support zero-emission operations, meaning that the vessel can operate on batteries only, for a limited load during a limited period of time.

4.6 Recommendations and best practices

Recommendations and best practices for vessel managers and crew on board are provided in the table below. For the full list of details, see Appendix C (Enhanced protection measures for closed-bus operations) and Appendix D (Enhanced system integration and verification for newbuilds).

Topic	Relevant for	Recommendations and best practices
Improve human performance through human-centred system design	Newbuilding department	Ensure that the design process of setting requirements to technical functionalities and creating human-machine interfaces adheres to the principles of human-centred design and that the result is compatible with basic human capabilities.
	Newbuilding department	Ensure close cooperation between designers and employees with recent operational experience (the end-user).
	Vessel manager, Newbuilding department	Actively be a part of defining the system's design criteria and apply the principles of user-centred design in the procurement process.
	Vessel manager, Newbuilding department	Cooperate with competence and experience in operations to set the requirements for the technical functionality and interface of equipment.
	System supplier	Rationalize the alarms and improve the quality of alarm texts through a process of human-centred design.
Continuous feedback to the organization	Vessel manager, Crew	Provide feedback to the company about improving the alarm management system (e.g. alert texts, alert priorities). The company should explicitly encourage crew to provide feedback on improving the alarm management system (e.g. alert texts, alert priorities).
Improved integration, testing and verification	Newbuilding department	Engage a system integrator that takes a central role in the design process from the earliest stages of the project.
	Newbuilding department	Perform early-phase assessments by reviewing documentation of the vessel and by performing a Hazard Identification (HAZID) study of automation integration.
	Newbuilding department	Get insight into the suppliers' tests.
	Newbuilding department, System supplier	Perform integration testing on the total integrated system.
	Newbuilding department	Implement an Integrated FAT(IFAT).
	Newbuilding department	Perform Failure Mode and Effect Analysis (FMEA) and FMEA sea trials. See guidance on FMEA analysis in Appendix B.
	Newbuilding department	Use a well-defined and transparent software-development and delivery process by knowing what to expect and by ensuring process adherence.
	Newbuilding department	Apply a change management procedure for key parameters and system configurations.
	Newbuilding department	Consider relevant voluntary class notations and guidance (e.g. RP, RP+, HIL and ISDS).
	Newbuilding department	Perform a network-failure analysis, network tests and manage the network configurations as key system parameters.
Robust design for closed-bus operations	Newbuilding department	Ensure robust design for closed-bus operations. See list of recommendations in Appendix C.
	Newbuilding department	Design effective blackout recovery systems. See list of recommendations in Appendix C.
	Newbuilding department	Consider using batteries as effective barriers to prevent blackouts. Consider the best practices and recommendations in Appendix D, to mitigate the increased complexity of systems and integration that batteries can contribute to.

Vessel manager Crew Newbuilding department System supplier

Step 5: Prioritize and implement cost-efficient prevention and mitigation measures

The implementation of preventive and/or mitigating measures should be based on cost-benefit evaluations that compare the monetary value of benefits against cost. The challenge, however, is how to assess and monetize the impact of different measures on safety.

5.1 Cost-benefit evaluations

How safe is safe enough?
After setting a safety ambition, as described in chapter 1.5, the shipowner and operators will face typical questions such as:

- Should we invest in additional safety measures for our existing fleet? What measures should be implemented?
- What types of safety features should be specified for our newbuilds?
- What class notations should be selected to support our ambition?
- Whether a type of ship which has suffered many accidents should be modified, and if so to what standard, and should the whole fleet then be modified?

To answer such questions, the decision-maker must have criteria at hand to be able to decide when the newbuilds and existing fleet can be considered safe enough. This requires the decision-maker to look at the organization's safety ambition. If the ambition goes beyond the minimum requirements set by class and statutory requirements, then the focus will be on deciding what measures should be implemented to progress towards the ambition.

The previous chapters of this guidance paper provide owners and operators with recommendations for how to reduce the risk of blackout based on best practice. As such, it covers measures related to updating procedures, change management, safety and failure mode assessments, installing equipment and systems, verification and testing. Before implementing new measures, you need to consider the impact it will have on safety and associated implementation costs.

Cost-benefit evaluation
Cost-benefit evaluations help to assess the benefit of the proposed safety measure, in terms of the risk that would be averted against the cost of implementing the measure. The evaluation has two main objectives:

- To determine if an investment in an additional safety measure should be initiated and assess by how much its benefits outweigh its costs.
- To provide a basis for comparing safety measures and comparing the total expected cost of each measure against its total expected benefits.

Cost-benefit analyses may have different outcomes for different shipping companies, at different times and for different vessels. This is because the operational and technical context of each vessel will determine what may be considered too high cost and how much a vessel will benefit from one measure compared to another. Vessel managers should therefore start a cost-benefit evaluation by setting criteria for determining cost-benefits that are relevant to the vessel's and company's situation.

Investments do not necessarily need to be significant. Updating procedures and crew training may have a significant impact on safety, while the associated cost may be less than an investment in system retrofits. Testing is also a low-cost measure, provided it does not impact operating schedule (e.g. testing in-between operations) and that the test is properly planned to avoid surprises and system damages during testing. Often, it is not the test itself that may be time consuming or costly; it is the afterwork that may be needed if things do not go according to plan. Again, planning, competence and contingency measures are essential for relatively low cost compared to benefit.

When 1+1=3: adding value through a combination of measures

It is the combined effect of measures that will have the greatest impact on safety. For example, setting up robust modes of operation in combination with more sophisticated protective functions in software and hardware. Combining this with regular testing and verification will undoubtedly have significant positive impacts on vessel safety and reliability.

Passenger ship owners and operators should also ensure that their strategies and additional measures for blackout prevention and recovery address the interdependencies between human (H), organizational (O) and technical (T) elements that influence the risk of blackout. This HOT approach should be an integral part of the risk management process, supporting the identification of effective recommendations and measures to improve safety and system reliability.

5.2 Recommendations and best practices

Recommendations and best practices for vessel managers are provided in the table below.

Topic	Relevant for	Recommendations and best practices
Perform cost-benefit analyses		Decide which measures to implement based on cost-benefit criteria.
		Use insight from internal and external blackout statistics and root cause analyses to identify which measures will have greatest impact.
		Ensure measures address the interdependencies between the human (H), organizational (O) and technical (T) elements (the HOT approach).
		Consider a combination of measures to ensure greatest effect on vessel safety and reliability.
		Introduce discussions about cost for preventive and mitigating measures early in the procurement process with vendors.
		Measure the return of investment by establishing key safety performance indicators that cover both leading and lagging indicators.

Conclusion

To support owners and operators in ensuring the safe and reliable operation of their fleet, DNV developed a stepwise approach for managing the risks of blackout and resulting loss of propulsion. Through implementing the best practices and recommendations from this guidance paper, the industry should succeed in reducing the risk.

The five steps and the key elements in each step are summarized below.

To challenge the status quo within organizations and to initiate a discussion on blackout prevention and recovery, owners and operators are encouraged to use the "Blackout Preparedness – Self Assessment" in Appendix A. This assessment is a set of questions that is intended to raise awareness about blackout and what can trigger escalation after a blackout.

STEP 1 Increase understanding of blackout

In order to achieve a step change in safety for loss of propulsion, it is necessary to gain an overall understanding of causes of blackouts and the regulatory framework. Increasing understanding of blackout requires that organizations investigate the underlying causes of blackout and that they understand the regulatory framework. A barrier-based and holistic approach to managing risk offers practical tools and a helpful mindset.

STEP 2 Define safety ambitions and manage conflicting goals

Setting an ambition for minimizing the risk for and mitigating the consequences of loss of propulsion at an organizational level is the first progression towards ensuring safe and effective operations. Owner and operators need to agree internally on their ambition, so that they don't run the risk of prioritizing other organizational goals at the expense of safety.

Managing conflicting goals implies also that organizations are ready to set aside time and resources to operationalize their commitment to change.

STEP 3 Identify measures to ensure safe and reliable vessel operations

To meet the expectations of stakeholders and the organization's safety ambition, it may be necessary to improve reliability on the existing fleet of vessels. Step 3 points to operational and technical measures that can be implemented by the organization. These include:

- Implementing robust operating modes based on sound procedures that offer decision support
- Taking measures to ensure fault tolerant operations through safe and reliable closed-bus operations
- Maintenance and operation of machinery to tackle common mode failures
- Managing software and networks
- Providing training and decision support for crew
- Implementing enhanced blackout testing
- Implementing dynamic-barrier monitoring

STEP 4

Identify measures to ensure safe and reliable newbuilds

Step 4 addresses technical measures for newbuilds that can be implemented by the organization to avoid blackout and loss of propulsion and to ensure quick and reliable recovery. These include:

- Applying the principles of human-centred design
- Ensuring robust design for closed-bus operations
- Improved integration, testing and verification
- Designing effective blackout recovery systems
- Utilizing battery systems

STEP 5

Prioritize and implement cost-efficient prevention and mitigation measures

The implementation of preventive and/or mitigating measures should be based on cost-benefit evaluations that compare the monetary value of benefits against cost.

The challenge, however, is how to assess and monetize the impact of different measures on safety.

It addresses the most prominent HOT elements and their interactions in relationship to risk for blackout, and it offers recommendations and best practices for each step in the five-step approach to preventing and mitigating blackout.

References

[1] ISO 9241-210:2010. 2010. Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems. Geneva: International Standards Organization.

[2] Norwegian Shipowners' Association and DNV (2014) Barrier management in Operation for the Rig Industry – Good Practices. Report 2013-1622. Rev1.

[3] DNV (2019). ISRS Book of Knowledge. Available on www.isrs.net with login credentials.

[4] European Safety, Reliability & Data Association (2015). Barriers to Learning from Incidents and Accidents.

[5] EEMUA 191 (2013), Alarm Systems: A Guide to Design, Management and Procurement Edition 2. The Engineering Equipment and Materials Users Association.

[6] Sherwood Jones, B., Earthy, J. V., Gould, D. (2006). Improving the design and management of alarm systems. Paper presented to the World Maritime Technology Conference, 18.03.2006.

[7] DNV (2016). Human-centred design of alert management systems on the bridge. Report 2016-1147.

[8] IMO (2003). Resolution A. 947 (23) Human element vision, principles and goals for the organization. London: IMO

[9] Eurocontrol (2013). From Safety-I to Safety-II. A white paper.

[10] Endsley, M. R. (2019). Human Factors & Aviation Safety. Testimony to the United States House of Representatives. Hearing on Boeing 737-Max8 Crashes on December 11, 2019. Human Factors and Ergonomics Society.

[11] DNV (2015) Recommended Practice – Dynamic Positioning Vessel Design Philosophy Guideline. DNV-RP-E306. Edition July 2015.

[12] DNV (2012) Recommended Practice D102 - Failure Mode and Effect Analysis (FMEA) of Redundant Systems

[13] J. T. Reason (1997). Managing the risks of organizational accidents

Abbreviations and definitions

AC	Alternating current
AVR	Automatic Voltage Regulator
BMS	Battery Management system
BF	Beaufort (scale)
CAPEX	Capital Expenditures
DC	Direct Current
DG	Diesel generator
DP	Dynamic Positioning
DPA	Designated Person Ashore
ER	Engine Room
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
GP	Generator Protection
HAZID	Hazard Identification
HIL	Hardware in the Loop, independent simulator-based testing
HOT	Human, Organization and Technology
HSEQ	Health, Safety, Environmental & Quality
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HV	High Voltage
I/O	Input/output
IAS	Integrated Automation System
IEC	International Electrotechnical Commission
ISDS	Integrated Software Dependent Systems
ISO	International Organization for Standardization
IT	Information Technologies
JIP	Joint Industry Project
LV	Low Voltage
OPEX	Operating Expenses
OT	Operational Technologies
PLC	Programmable logic controller
PMS	Power Management System
RP	Redundant Propulsion
SMS	Safety Management System
SOTF	Switch-on-to-fault
SRtP	Safe Return to Port
TQ	Technology Qualification
UPS	Uninterruptible Power Supply

Availability:	Ability to be in a state to perform as required (ISO 14224).
Blackout:	Blackout situation occurs when there is a sudden loss of electric power in the main distribution system and remains until the main source of power feeds the system. All means of starting by stored energy are available (DNV Rules for Ships, Part 4, Chapter 8, January 2018).
Busbar:	Low-impedance conductor to which several electric circuits can be separately connected (IEC 61439-1).
Bus-tie breaker:	Circuit breaker to sectionalize the busbar.
Circuit breaker:	Mechanical switching device, capable of making, carrying and breaking currents under normal circuit conditions and also making, carrying for a specific time and breaking currents under specified abnormal conditions such as those of short circuit (IEC 60947).
Common cause/ mode failure:	Failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause. Common cause failures can also be common mode failures. Components that fail due to a shared cause normally fail in the same functional mode. The term common mode is therefore sometimes used. It is, however, not considered to be a precise term for communicating the characteristics that describe a common cause failure (ISO 14224).
Failure (of an item):	Loss of ability to perform as required. A failure of an item is an event, as distinct from a fault of an item, which is a state (ISO 14224).
Failure mode:	The effect by which a failure is observed on the failed item [12].
(Single) Fault tolerance:	(Single) fault tolerance is the ability of a system to function without interruption after a single failure [11].
Hidden failure:	A failure that is not immediately evident to operations and maintenance personnel.
Modes:	The vessel operational mode specifies the high-level system set-up and redundancy design intention for a specified set of vessel operations. Examples of vessel operations are transit, positioning keeping, manoeuvring, etc.
Reliability:	The probability that an item can perform a required function under given conditions for a given time interval [11].
Redundancy:	The existence of more than one means of performing a required function [11].
Separation:	With reference to systems or equipment intended to provide redundancy. Reduce the number of connections between systems to reduce the risk that failure effects may propagate from one redundant system to the other [11].
Switchboard:	A main switchboard is a switchboard directly supplied by the main source of electrical power or power transformer and intended to distribute electrical energy to the vessel's services (DNV Rules for Ships, Part 4, Chapter 8, January 2018). An emergency switchboard is a switchboard, which in the event of failure of the main electrical power supply system, is directly supplied by the emergency source of electrical power and/or the transitional source of emergency power and is intended to distribute electrical energy to the emergency power consumers (DNV Rules for Ships, Part 4, Chapter 8, January 2018).

Appendix A:
Self-Assessment for blackout preparedness

1. UNDERSTANDING OF BLACKOUT

- ☐ a. Are you familiar with what failures may cause blackout?
- ☐ b. Are you familiar with the minimum regulatory requirements for blackout prevention and recovery (e.g. class, statutory)?
- ☐ c. Are you familiar with how additional class notations may help to prevent blackout and ensure efficient recovery?
- ☐ d. Do you know what the typical duration of blackout is before full propulsion is restored?

2. DEFINE THE ORGANIZATION'S SAFETY AMBITION AND MANAGE CONFLICTING GOALS

- ☐ a. Has your organization defined a safety ambition for blackout or loss of propulsion?
- ☐ b. Do you manage your organization's conflicting goals?

3. ENSURE SAFE AND RELIABLE OPERATIONS OF FLEET

- ☐ a. Where have you identified your critical operations?
- ☐ b. Do your procedures define set-up of machinery/power system for critical operations?
- ☐ c. Do you have additional protection measures implemented for closed bus-tie operations in critical operations?
- ☐ d. Do your organization's procedures support Master's decision regarding critical operations (e.g. severe weather, close to shore)?
- ☐ e. Is your crew familiar with the limitations of their systems and what to do in case manual blackout recovery is needed?
- ☐ f. Do you have sufficient onshore technical expertise and support to assist in emergency situations on board?

4. ENSURE SAFE AND RELIABLE NEWBUILDS

- ☐ a. Is integration testing of automation and software systems done during newbuilding process?
- ☐ b. Is closed-bus operation considered in your newbuild specification?
- ☐ c. Do you consider blackout recovery system functionality during newbuild specifications?
- ☐ d. Do you apply principles of human-centred design for the design of man-machine interfaces and alarm management systems?

Appendix B:
Guidance for FMEA/FMECA analysis

	Potential hazards that should at least be adequately addressed	Technical barrier
Active and reactive load sharing	• Active power load sharing failure (e.g. caused by governor failure, insufficient, excess or unstable active power, fuel-rack failure, active-power or frequency sensor failures, signal failures, load-sharing line failures) • Reactive power-load sharing failure (e.g. caused by AVR failure, insufficient, excess or unstable reactive power, reactive power-sensor failures, voltage-sensor failures, signal failures) • Detection methods and actions to bring the system to a safe state with conditions and time responses	• Generator protection • PMS upgrade
Consequences of voltage transients	• Reference to analysis of worst-case voltage dip (depth and duration) on healthy bus after short circuit on other bus (in closed tie-breaker operation) • Document adequate voltage dip "ride-through" capability of necessary systems to remain in position: thruster drives, computer systems, networks, contactors, pumps, ventilation, and other axillaries.	• System optimization and tuning for entire protection strategy (HV, LV, GP, PMS, load reduction functionality inside converters)
Risk for simultaneous trip or load reduction of all thrusters	• Are there built-in protections in thruster variable speed drives that cause trip or load reduction? If yes, how is it ensured that not all thrusters are lost at the same time by the same trigger? Examples of such protection can be high/low voltage and/or frequency. • Are there situations where all thrusters will reduce their power simultaneously to such a level that position cannot be maintained? Such as built-in load reduction functionality in drives that may reduce power to zero if one diesel engine fails to full speed.	• System optimization and tuning for entire protection strategy (HV, LV, GP, PMS, load reduction functionality inside converters) • All protective functions included in the coordination study and mapped with the computer model used for transient state simulation
Ensure that no hidden failure renders it impossible to open tie-breaker from PMS or other protection devices	• Does the PMS have direct HW open command signals to both tie-breakers? • Is it sufficiently ensured that tie-breaker is not in local mode during operation (e.g. clear indication of local/remote status on PMS GUI)? • Include check of tie-breaker operability in procedures	• Redundant open command signals • Fail safe system that trips breaker on wire break on open command signal • Signal monitoring

Fault tolerance in PMS system	• How is it ensured that a single feedback failure to PMS does not cause the PMS to carry out actions that result in loss of position?
	• Can, for instance, a single failure on feedback signal to PMS cause:
	  ◦ PMS to connect generator (or bus-tie) without synchronization?
	  ◦ Force full load reduction to all running thrusters simultaneously?
	  ◦ PMS to decrease generator frequencies to a level that causes risk of automatic load reduction of drives / tripping of drives?
	  ◦ PMS to increase frequency to a level that causes systems to trip?
	  ◦ PMS to jump to manual mode?
	  ◦ Can single PMS operator failure cause blackout?
	  ◦ Can one single PMS unit trip all generator breakers?
	  ◦ Failure to start and connect
	  ◦ Crash synchronization on connect
	  ◦ Connection of a stopped generator
		• I/O mapping fitted to nodes / field stations to define possible common mode failures
		• PMS response during ride through, e.g. short circuits
		• Protective function which results in feeder trip / bus-tie breaker trip

Documentation, analysis and simulation	
Documentation and verification of protection settings	• Is there protection functionality in PMS that can trip generator breakers and thus need to be included in discrimination analysis? • Requires tables with settings of all protection equipment both in relays on breaker and in PMS • As part of FMEA: verify all protection settings on breakers, not only short circuit by on board inspection. • Discrimination analysis which includes protective functions fitted to HV system, LV system, PMS, BMS, converters and GP. • Power system shall be discussed to identify applicable failure modes (FMEA). • Failure mode shall be analyzed to identify effects on the overall system, including consideration of an entire protection strategy scheme which typically includes protection relays at the HV system, protective functions implemented to PMS / IAS, ability of speed governors and AVRs to stabilize the power parameters. • Computer simulations which demonstrate ride through capability
Short circuit selectivity between bus-tie and generator breakers	• Is selectivity documented also for highest maximum short circuit current? • Zero delay in bus-tie short-circuit protection?
Mode monitoring in PMS/IAS system	• Is there a warning/alarm if power system set-up is in conflict with defined prerequisite for the operational profile?
Loop monitoring (or similar)	• Loop monitoring needs to provide feedback to PMS, etc.
Bus-tie breaker shunt-trip, can this be used?	• Need to be able to open in case of voltage dip

Appendix C: Enhanced protection measures for closed-bus operations and blackout recovery

Recommended protection measures for enhanced fault tolerance in closed-bus operations	
1.	**Implement advanced generator protection (GP) to protect the power system against faulty fuel and voltage-control systems**
☐	a. Each generating set should be equipped with dedicated GP.
☐	b. GP should give trip commands via hard-wired interface to the generator breaker and to the tie-breakers.
☐	c. GP should be fitted with a dedicated set of interfaces and reference signals.
☐	d. Signals from different secondary cores of feeder current transformers and independent transducers for GP and PMS should be used.
2.	**Use high-integrity switchboards, high-voltage switchboards**
☐	a. The main switchboard should be designed and prepared for possible short-circuit and earth-fault testing.
☐	b. Depending on design, various measures may be implemented to increase the robustness of critical systems or components: • Implementing additional physical protection of equipment • Selecting high-end components with good performance and low failure rate • Using single core bus-tie cables • Implementing mechanical protection of bus-tie cables and insulated busbars in switchboards • Implementing additional fire and flood monitoring systems

3.	Reduce the risk of connection of non-synchronized power systems
☐ a.	Arrange two sync-check barriers in series. Such arrangements will imply a small residual risk for a non-synchronous closing to happen (e.g. in case of mechanical defects in breakers).
☐ b.	Establish a protection strategy against crash-synchronization failure through: • Switch-on-to-fault (SOTF) protection, understanding that this function does not protect the system against severe consequences of crash synchronization. • Analysis of typical function in the protection strategy scheme. Typically, crash synchronization results in high current and might be cleared on the short circuit protection fitted to DG feeder or bus-tie breakers. • A transient state analysis to verify system behaviour during crash synchronization failures.

4.	Reduce the risk of power management system (PMS) failures
☐ a.	Monitor to prevent hidden failures in trip circuits for the generator and tie-breaker.
☐ b.	Implement high integrity serial communication or direct HW open command signals to each generator and bus-tie breaker.
☐ c.	Implement redundant open command signals to each generator and tie-breaker.
☐ d.	Introduce clear indications of local/remote status of the tie-breakers.
☐ e.	Ensure autonomy and distribution of functionality.
☐ f.	Implement dual action functionality to prevent unintended acts of operation.
☐ g.	Implement a mechanism for validation of feedback signals to PMS to prevent: • Generator (or bus-tie) connection without synchronization • Unintended load reduction of thrusters • Decrease of generator frequencies to a level that increases the risk of automatic load reduction of drives and/or tripping of drives • Increase in frequency to a level that causes systems to trip
☐ h.	Minimize centralized control functions and signal and communication link connections across the redundancy groups.

5.	Ensure power system stabilization
☐ a.	Discuss the power system to identify applicable failure modes.
☐ b.	Analyze the failure mode to identify effects on the overall system and establish an encompassing protection strategy scheme.
☐ c.	Discuss the phenomena that may interrupt the LV system (including auxiliary systems).
☐ d.	Examine the propulsion drives, including its safety functions. Since propulsion drives are typically each fitted with the same protective functions, an event that occurs in the entire power distribution system may trigger drives that trip on the same parameter.
☐ e.	Perform a coordination study that covers all essential systems (HV, LV, DC distributions and GP).
☐ f.	Ensure that desktop studies are supported by computer simulations.

Recommended protection measures for enhanced blackout recovery reliability	
1. Ensure switchboard sectioning and that each section has an autonomous blackout-recover functionality	
☐ a.	Ensure that main switchboards are split into sections between each generator by means of bus couplers. A bus coupler can limit effects of failures and possibly provide simplified and faster blackout recovery as well as more autonomous systems.
☐ b.	Ensure that each section has an autonomous blackout-recover functionality. This will limit the logic to only one section, which speeds up the recovery and reduces the risk of failure of recovery for the entire system.
2. Implement barriers against unintended automatic blackout recovery actions	
☐ a.	Ensure that no action can result in unnecessary blackout or partial blackout, e.g. in scenarios where power system recovers from severe failures, which are followed by active and/or reactive power stabilization.
☐ b.	Failure modes related to voltage and frequency shall be considered including signal failures (I/O failures) and situations where the actual voltage and/or frequency deviates from normal values.
☐ c.	The setpoints and protective functions in the PMS shall be coordinated with possible power oscillations (power oscillation and stabilization, and the expected stabilization time) to avoid spurious activation of protective functions or blackout detection.
3. Ensure integrity of blackout recovery sequence	
☐ a.	Explicitly plan and discuss the blackout recovery process. Such an exercise should involve all vendors to plan and optimize the recovery sequence from blackout detection, up to full recovery including automatic start of propulsion. A blackout recovery sequence that requires high level of permission signals exchanged between the control systems prolongs the process and increases the risk of sequence failure.
☐ b.	Evaluate severe failures which could be considered as initial conditions prior the blackout incidents in terms of protective functions that are implemented to the entire protection strategy system.
☐ c.	This typically means that safety functions which are implemented in HV relays, control and safety in power generation sets, propulsion drives, other drives implemented in the system should be evaluated and concluded if might set the system to "trip and block" position and be source of recovery failure. For power systems operating in closed-bus modes, such condition would disable the blackout recovery sequence throughout the redundant groups.
☐ d.	Ensure that systems that are blocked upon consecutive starts are not used for critical equipment
☐ e.	Implement an override functionality (preferably external) that disables the interlocks that prevent blackout recovery for the scenarios where power systems cannot promptly be recovered.
☐ f.	Reduce the need for manual actions that could delay the recovery process.
☐ g.	See checklist in Appendix F for full blackout recovery test.

Appendix D:
Enhanced system integration and verification for newbuilds

Recommendations and best practices for improving human performance through human-centred system design	
Ensure human-centred system design	
☐ a.	Ensure that the design process of setting requirements to technical functionalities and creating human-machine interfaces adheres to the principles of human-centred design and that the result is compatible with basic human capabilities (ref ISO 9241-210:2010).
☐ b.	Ensure close cooperation between designers and employees with recent operational experience.
☐ c.	Actively be a part of defining the system's design criteria and apply the principles of user-centred design in the procurement process. This includes updating the safety management system (SMS) with the continuous and iterative improvement process of the alert management system.
☐ d.	Cooperate with competence and experience in operations (HSEQ and Masters) to set the requirements for the technical functionality and interface of equipment.
☐ e.	Rationalize the alarms and improve the quality of alarm texts through a process of human-centred design.

Recommendations and best practices for improved integration, testing and verification

1. Engage a system integrator

- ☐ a. Ensure that the system integrator is responsible for integrating all components of the system, applying and advocating the principles of human-centred design, being a driver for reducing the number of alerts and being responsible for managing the improvement process of the alarm management system during operations.
- ☐ b. The equipment manufacturer should deliver equipment in accordance with the requirements that are set by the system integrator and the system logic.

2. Perform early-phase assessments

- ☐ a. Review documentation of the vessel in order to mitigate any design flaws.
- ☐ b. Perform a Hazard Identification (HAZID) study of automation integration to enable the vendors to agree on who is responsible for what functionality, especially in the interface between complex safety critical systems.

3. Perform comprehensive verification and validation of systems

- ☐ a. Perform failure mode and effect analysis (FMEA or FMECA).
- ☐ b. The objective of failure mode and effects analysis of power and propulsion systems is to provide objective evidence of required redundancy and fault tolerance.
- ☐ c. The FMEA should address all operational modes of a vessel, which it is intended to be valid for.
- ☐ d. For each of the vessel's operational modes, the technical system configuration shall be assessed and prerequisites for achieving the required failure tolerance and redundancy shall be included.
- ☐ e. Get insight into the suppliers' tests.
- ☐ f. Multiple tests (e.g. software-module tests, performance tests, FMEA tests, etc.) are normally performed by the supplier before the system is brought on board the vessel. However, the yard and owner have little insight into the extent and results of these tests. It is recommended that the yard or owner asks to get insight into the tests that have been performed, and it is also possible to ask a 3rd party to verify the sufficiency of the performed tests.
- ☐ g. Perform integration testing.

4. Use a well-defined and transparent software-development and delivery process

- ☐ a. Know what to expect:
  By utilizing a development and delivery process that encompasses all stakeholders like the supplier, yard and owner, all parties know what to expect and how to control their part. It also makes it easier for the different stakeholders to understand what to expect from the others. There are several relevant standard processes available, and DNV has also published one in DNVGL-OS-D203 (Integrated Software Dependent Systems [ISDS]).
- ☐ b. Ensure process adherence:
  3rd party may follow up if the defined and agreed processes are followed by all parties. This ensures that the different organizations keep focus on the agreed way of working.

5. Apply a change management procedure for key parameters and system configurations

- ☐ a. Identify the key parameters:
  The key parameters of the system should be identified and agreed.
- ☐ b Analyse key parameters before changes are made:
  Some parameters may affect the performance of the whole system and should not be changed until the change has been agreed between the owner/operator and the supplier in question.
- ☐ c. Verify key parameters after software changes:
  After a software update has been performed, the key parameters should be verified before the system is brought back into operation. If the update introduces or removes parameters, the list of key parameters should be revised.
- ☐ d. Implement changes to software between FAT and vessel delivery under strict change management:
  After FAT, the software should be under version control. Both supplier and system integrator should have full transparency into the changes being made.

6. Consider relevant rules and guidance

- ☐ a. Approval of manufacturers regarding system and software engineering (described in DNVGL-CP-0507), DNV's class notations; Integrated Software Dependent Systems (ISDS) (described in DNVGL-OS-D203, Redundant Propulsion (RP), Cyber Secure, Enhanced System Verification (ESV).

Appendix E:
Enhanced blackout prevention test

Test of load management – power management system (PMS) functions	
Power system disturbance caused by loss of one diesel generator (DG).	☐ 1. Set up the power system with two DGs, for instance, operating with typical and realistic load. Power system should be set up according to operating profile, e.g. closed bus. ☐ 2. Set remining DGs to standby start. ☐ 3. Trip one DG and verify safety functions like load shedding, load reduction, phase back system. ☐ 4. Verify that remaining DG can withstand load increase with no spurious trip of tie-breakers or loss of essential and important consumers.
Power system disturbance followed by loss of big consumer.	☐ 1. Set up the power system with two DGs, for instance, operating with highest possible load (i.e. slightly below stand-by start setpoint). Power system should be set up according to operating profile, e.g. closed bus. ☐ 2. Load the power system as much as possible and trip a large consumer (e.g. propulsion). ☐ 3. Verify that speed and frequency increase does not cause spurious trip of DGs.

Test of voltage ride through capabilities (i.e. power system response to voltage dip caused by short circuit)	
Note: Most systems will have equipment which will have problems to ride through a short period with a reduced voltage level, e.g. frequency converters, motor starters, circuit breakers with undervoltage protections, power supplies, any PLC system without battery backup, changeover system, etc. Note that quick opening and closing of feeder or tie-breakers might be interlocked and not easily accessible in the HV systems.	
Consequence of a short circuit at a high level in the power system will be a voltage dip.	Expected voltage dip time applicable in the system shall be verified prior to the test. Test can be conducted in different ways, such as: ☐ Quickly opening and closing feeder breakers to an essential consumer (e.g. propulsion thruster) ☐ Opening and closing bus ties to switchboard sections without generators connected ☐ Opening one generator breaker and quickly closing another

Test of power system response to active and reactive load oscillations	
• Below tests should be arranged in the closed-bus mode. This is to verify the impact of power imbalance on redundant systems. • Tests should be arranged with the minimum operating set-up, which is typically two DGs online (connected to redundant systems). • Power system set-up shall be agreed prior the test. Test shall be document by plots, records and any other means which allows to verify the results and reproduce the failure mechanism (if test fails).	
Speed-governor failures	☐ a. Disconnect communication between fuel regulator or load-control system. Do a significant load change. ☐ b. Apply a speed increase to the diesel by pulling fuel rack of connecting a laptop to the governor. ☐ c. Apply a speed decrees to the diesel by pulling fuel rack of connecting a laptop to the governor.
Automatic voltage regulator (AVR) failures	☐ a. Disconnect communication between AVRs if it exists. Do a significant load change. ☐ b. Disconnect the voltage sensing to the AVR (usually done by shorting the current transformer [CT]). ☐ c. Apply a voltage increase to the generator by connecting a simulator to the AVR. ☐ d. Apply a voltage decrease to the generator by disconnection the AVR or by connecting a simulator/laptop.

Appendix F:
Enhanced blackout recovery test

1.	Key principles of blackout-recovery testing procedures
☐ a.	The main and emergency power systems can be tested once all the prerequisites are checked and the vessel is ready for the full blackout test.
☐ b.	A test is considered successful when all the equipment is recovered and healthy. Any recovery failures shall be investigated and once the fault is diagnosed and rectified, the test shall be performed again.
c.	A test should not be repeated before the roof cause of a failed test is rectified, as this will only show the random response to failure.
d.	Implement regular blackout tests, where the blackout incident is initiated by different conditions to verify system response triggered by different circumstances and to expose crew to various scenarios.
e.	Regular blackout testing can be combined with Redundant Propulsion – Failure mode and effect analysis (RP FMEA) tests or Safe Return to Port (SRtP) casualty threshold testing.
f.	Create trends to observe the power plant condition, timing between the interlocks and permission signals, and the exact time that the specific components need to recover and get ready for operation.

2.	Example of a simplified stepwise description of full blackout test
☐ 1.	**Close the switchboard into one common system.** All the thrusters (pods, conventional propulsion) shall be running.
☐ 2.	**Set all generating sets to remote control and ensure they are enabled for automatic start.** One diesel generator (DG) should be suppling all switchboards connected via bus-tie breakers.
☐ 3.	**Make the DG trip.** Good practice is to cause the trip by a different condition year by year, and use different generating set each year.
☐ 4.	**Verify that the power system split into independent power systems (typically on the undervoltage protection).** Verify that the power system detects the blackout.
☐ 5a	**Verify that the main power system starts the recovery process.** In the fully automated systems, the power generation shall start up automatically and connect to the main switchboards (power systems that recover on smaller sections are more efficient and quicker and are less probable to fail during recovery).
☐ 5b	**At the same time, verify that the emergency system detects the blackout and recovers in parallel to the main system.** The emergency system shall be free of any time delays that allow the main system to take over the emergency system (e.g. due operational reasons) and not reduce the time that is needed to energize the emergency services.
☐ 6.	**Once the main switchboard is energized, re-energize all the auxiliary systems and allow propulsion drives to recover.**
☐ 7.	**If manual actions are needed for main system restoration, ensure that they are part of the on-board procedure.** Ensure that on-board procedures are detailed and unambiguous. They should be supported with sketches and tags and location for circuit breakers or valves.

ABOUT DNV

We are the independent expert in risk management and quality assurance. Driven by our purpose, to safeguard life, property and the environment, we empower our customers and their stakeholders with facts and reliable insights so that critical decisions can be made with confidence. As a trusted voice for many of the world's most successful organizations, we use our knowledge to advance safety and performance, set industry benchmarks, and inspire and invent solutions to tackle global transformations.

Regional Maritime Offices

Americas
1400 Ravello Drive
Katy, TX 77449
USA
Phone +1 281 3961000
houston.maritime@dnv.com

Greater China
1591 Hong Qiao Road
House No. 9
200336 Shanghai
China
Phone +86 21 3279 9000
marketing.rgc@dnv.com

North Europe
Thormøhlensgt. 49A, 5006 Bergen
Postbox 7400
5020 Bergen
Norway
Phone +47 55943600
north-europe.maritime@dnv.com

South East Europe,
Middle East & Africa
5, Aitolikou Street
18545 Piraeus
Greece
Phone +30 210 4100200
piraeus@dnv.com

West Europe
Brooktorkai 18
20457 Hamburg
Germany
Phone +49 40 361495609
region.west-europe@dnv.com

Korea & Japan
8th Floor, Haeundae I-Park C1 Unit, 38, Marine city 2-ro, Haeundae-Gu 48120 Busan
Republic of Korea
Phone +82 51 6107700
busan.maritime.region@dnv.com

South East Asia, Pacific & India
16 Science Park Drive
118227 Singapore
Singapore
Phone +65 65 083750
singapore.maritime.fis@dnv.com

DNV
Brooktorkai 18
20457 Hamburg
Germany
Phone +49 40 361400
www.dnv.com

DNV AS
NO-1322 Høvik
Norway
Phone +47 67 57 99 00
www.dnv.com