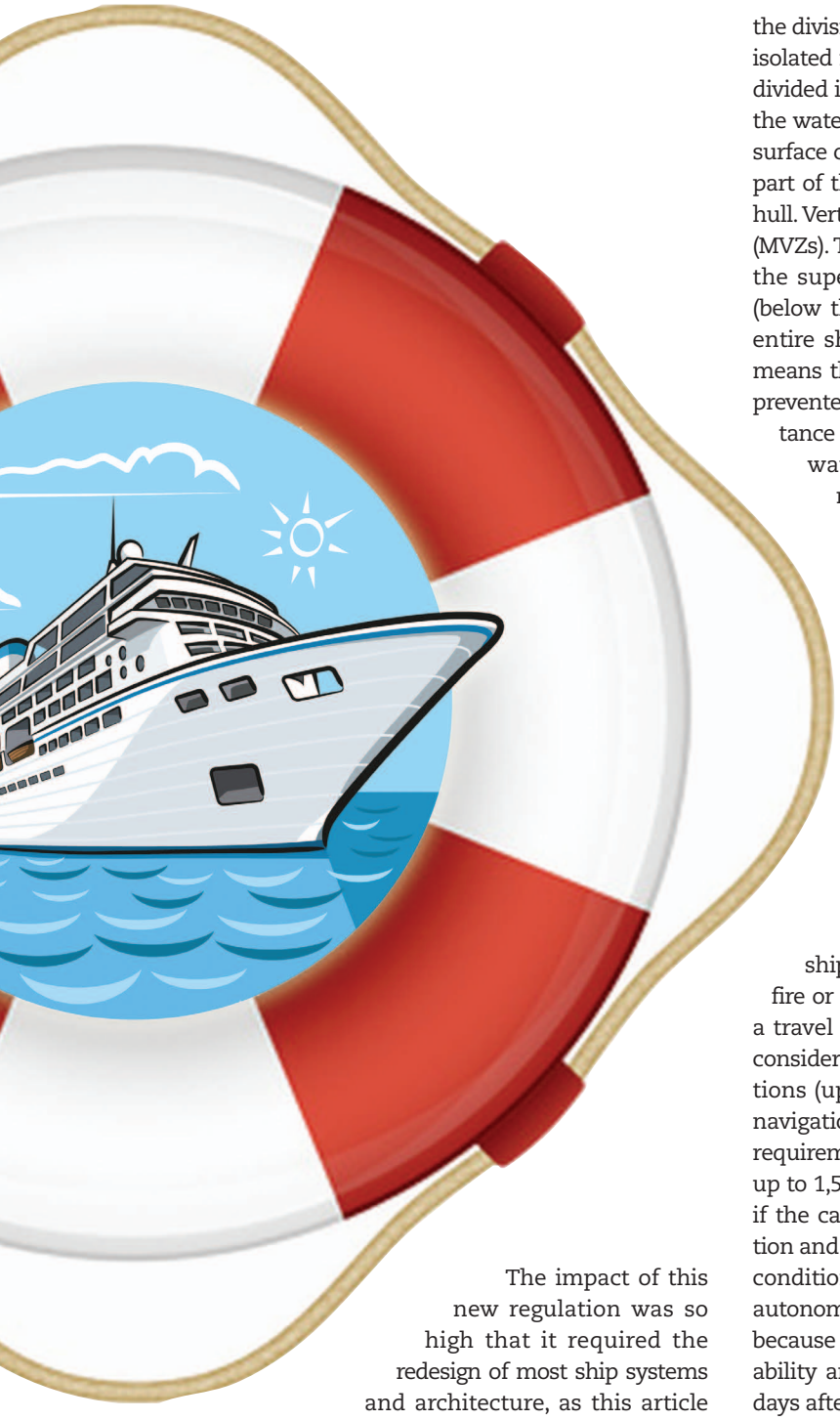
By Andrea Vicenzutti, Daniele Bosich, Roberto Pelaschiar, Roberto Menis, and Giorgio Sulligoi

Increasing the Safety of Modern Passenger Ships

A comprehensive approach for designing safe shipboard integrated electrical power systems.

OVER THE PAST DECADES, THE GROWTH OF international cruise tourism has been constant. The forecasts made by the Ships and Maritime Equipment Association indicates an annual growth rate of about 7%, leading to the triplication of global cruise passengers in the future (from 19 million passengers in 2010 to more than 54 million in 2035). To cover the future market needs, roughly six or eight new cruise ship buildings per year are planned until 2031, along with an increase in ship size (up to 8,000 persons accommodated onboard). These two facts have led to a growing interest in the passengers' safety, which has been addressed by the International Maritime Organization (IMO) Maritime Safety Committee (MSC) in 2000, with the launch of an initiative for adequate international safety regulation for large passenger ships. The first issue that emerged from such an initiative was the difficulty in safely evacuating passengers toward lifeboats during emergencies (in particular, during a fire or flooding). The solution proposed by the MSC requires that future passenger ships be designed to increase their intrinsic survivability, exploiting the concept that the ship is its own best lifeboat (thus avoiding abandoning the ship as much as possible). Such a solution was formalized in December 2006 through a package of amendments to regulations dedicated to large passenger ships and published in the 82nd session of the MSC, i.e., the Resolution MSC.216(82), commonly known as *safe return to port regulations (SRtP)*.



The impact of this new regulation was so high that it required the redesign of most ship systems and architecture, as this article will describe. Concerning the electrical power system, modern large passenger ships employ the all-electric ship (AES) concept; thus, they are endowed with a single integrated power system (IPS) (Figure 1) that supplies every onboard load, including propulsion. Therefore, the importance of the IPS in assuring the compliance with SRtP rules is significant, and its design must be conceived accordingly.

The safety of a ship is related to its overall design, so it is necessary to introduce some notions about the passenger ship's structure. In particular, it is important to highlight the division of the ship and to note how compartments are isolated from one another (Figure 2). Horizontally, a ship is divided into the hull and the superstructure. The former is the watertight lower body of the ship and meets the water surface on a line called the *waterline*, while the latter is the part of the ship that extends above the upper part of the hull. Vertically, a ship is separated into main vertical zones (MVZs). These are vertical sections into which the hull and the superstructure of a ship are divided by watertight (below the waterline) and fire resistant (throughout the entire ship) boundaries (A class boundaries). *Watertight* means that the passage of water through the structure is prevented in either direction with a proper margin of resistance under the pressure due to the maximum head of water that it might have to sustain. *Fire resistant* means that the spread of flames and smoke is prevented for at least one hour (tested with a standardized method) and designed so that the average temperature and the temperature of any single point of the unexposed side do not rise more than 140 °C and 180 °C, respectively, above the original temperature.

The SRtP Regulation

The Resolution MSC.216(82) made the new Regulations II-2/21-22 (namely, the SRtP regulation) compulsory for passenger ships constructed on or after 1 July 2010, having a length of 120 m or more or having three or more MVZs.

In particular, the SRtP rules aim to ensure a ship's safe return to port, by its own systems, after a fire or flooding casualty below a certain threshold. Such a travel must be performed at a minimum speed while considering an upper limit for weather and marine conditions (up to Beaufort force 8) and ensuring a minimum navigation autonomy depending on the ship's operative requirements (e.g., ocean sailing cruise ships must ensure up to 1,500 nmi of autonomy after a casualty). Conversely, if the casualty threshold is exceeded, an orderly evacuation and abandon ship shall be ensured. The return to port conditions (speed, weather and marine conditions, and autonomy) have a significant impact on the ship design, because they imply the need of assuring both the habitability and the minimum navigation services for several days after the casualty.

Beside the concept of "safe return to port," the Resolution MSC.216(82) introduced the fundamental concepts of casualty threshold, safe area(s), and essential systems.

The threshold depends on both the casualty type (fire or flooding) and the presence of additional protection systems. Regarding the fire casualty threshold, it depends on the presence of a fixed fire-extinguishing system (represented as a V symbol in Figure 3) in the space of fire origin (represented as an O symbol in Figure 3). If the system is present, the casualty is represented by the loss of the only space corresponding to the origin, up to the nearest

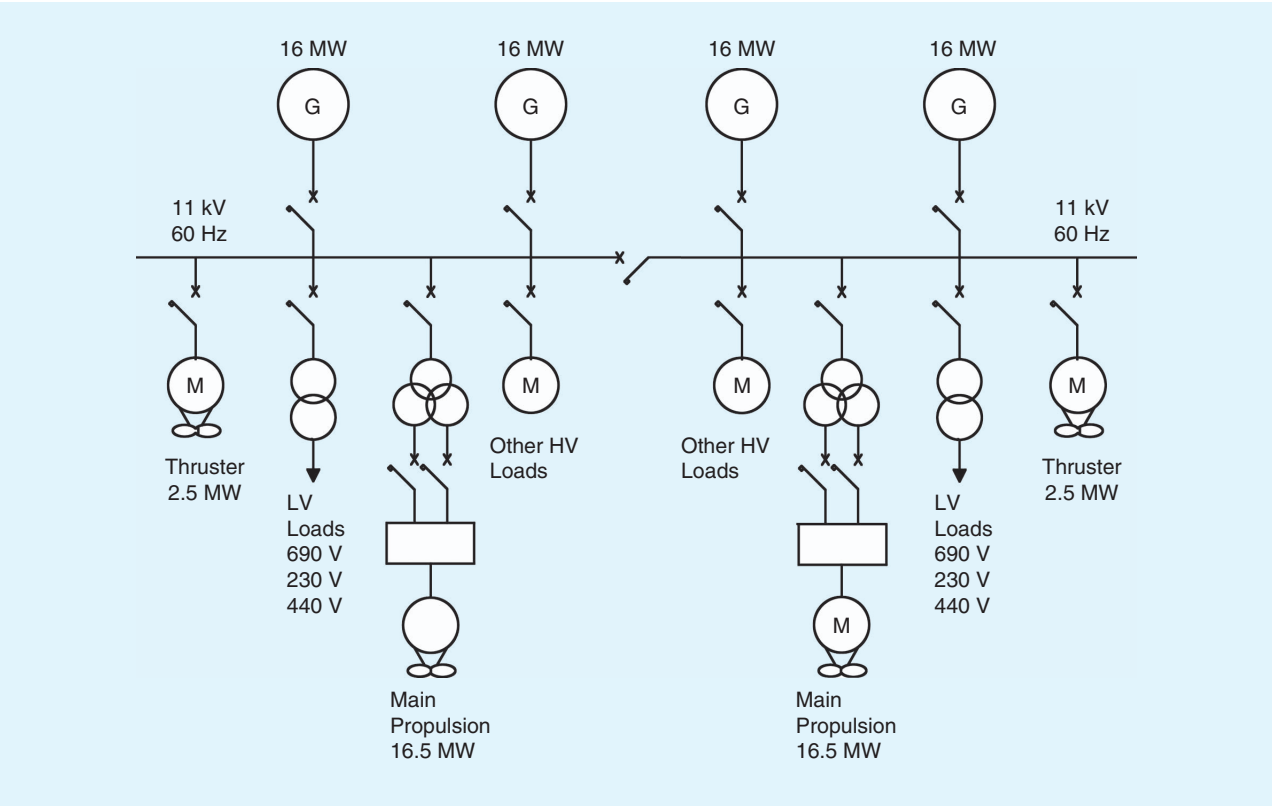


Figure 1. The typical all electric cruise ship IPS. LV: low voltage; HV: high voltage; G: generator; M: motor.

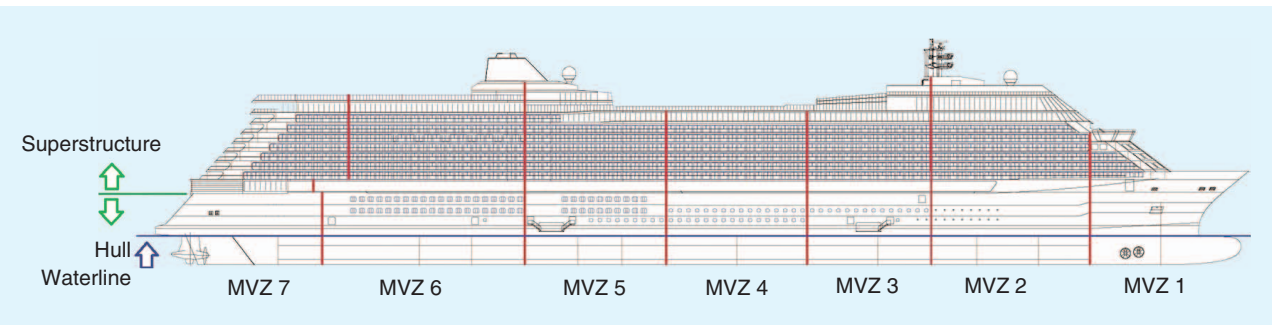


Figure 2. The typical passenger ship's structure subdivision.

A-class boundaries (both bulkheads and decks). If the system is not present, then the represented casualty also includes the adjacent spaces, as far as A-class boundaries are reached (Figure 3). Concerning flooding casualties, the threshold is determined by the loss of any single main watertight compartment. As a result, three possible scenarios shall be considered:

a) a safe return to port in the presence of flooding in one watertight compartment (Regulation II-1/8-1)
b) a safe return to port in the event of a fire in a limited space within an MVZ (Regulation II-2/21)
c) the need for evacuation and to abandon ship when a fire exceeds the casualty thresholds shown in Figure 3 (Regulation II-2/22).

In addition, in the SRtP perspective, casualties are to be considered as not occurring at the same time.

Regarding the essential systems, these shall remain operational after a fire or flooding casualty to allow a ship's safe return to port or to support an orderly evacuation and abandon ship if needed. In particular, the power supply to the essential systems must be guaranteed, as well as cooling and all the other accessory services needed to keep them operational. Examples of systems that are considered essential are as follows:

- propulsion, steering, and control systems
- navigational systems
- fuel oil systems
- internal and external communication
- fire main system, fixed fire-extinguishing systems, fire and smoke detection systems
- bilge and ballast systems
- power-operated watertight and semiwatertight doors

- systems intended to support safe areas
- flooding detection systems
- other systems determined to be vital for damage control effort.

In the case of a casualty not exceeding the thresholds, the essential systems that are needed to allow the ship to return to port with the performance stated by the regulation shall remain operational. Meanwhile, the accommodation of the passengers in the safe area(s) is required. The safe areas are the spaces in which the passengers must be recovered after a casualty. These must be outside the MVZ in which the casualty happened and must protect the passengers from hazards to life and provide the most basic habitability services (i.e., sanitation, water, food, space for medical care, shelter from the weather, means of preventing heat stress and hypothermia, lighting, and ventilation).

In contrast, if the casualty threshold is exceeded, a safe return to port can no longer be performed. In such a case, the essential systems required by the rules to be operational to allow an orderly evacuation and abandon ship must remain operational for at least 3 h (as stated in Regulation II-2/22).

The Impact of SRtP Rules on IPS Design

The drivers commonly affecting the IPS design are performance improvement, cost reduction, weight reduction, volume reduction, and rules and regulations compliance. Given the difficulty in predicting the long-term consequences of innovative design choices, designers tend to rely on well-proven solutions. It is a common belief that successful procedures should not be changed. However, the SRtP regulation led to a compulsory change in traditional design processes. Indeed, the financial consequences of a design that is not compliant with safety rules have proven to be several orders of magnitude greater than the cost given by the increase in design effort, thus leading to a fast shift toward safety in ship design paradigms.

In this regard, SRtP rules affect each ship system from sanitation to food preparation. A certain amount of systems can be made compliant with only a reduced effort (e.g., food supply for passengers during the return to port can be provided through dry food stowed in dedicated deposits in safe areas). In contrast, electrical power supply cannot be made compliant with a small amount of effort. The exploitation of the AES concept by modern large passenger ships means that electrical power is required to perform virtually each function, including SRtP related ones. Therefore, at present, the IPS is a critical system not only during normal ship operation but also during emergencies.

Consequently, SRtP regulation concepts heavily affect the perspective of electrical power system designers. Indeed, the need to assure correct operation of essential systems, not only during normal operation but also after a casualty in any space, led to a closer collaboration among all the designers involved in the shipbuilding process. The additional constraints placed on the IPS architecture and its spatial placements had to be introduced into a design process that was already full of other constraints (e.g., interfaces with other systems, ship balance, space

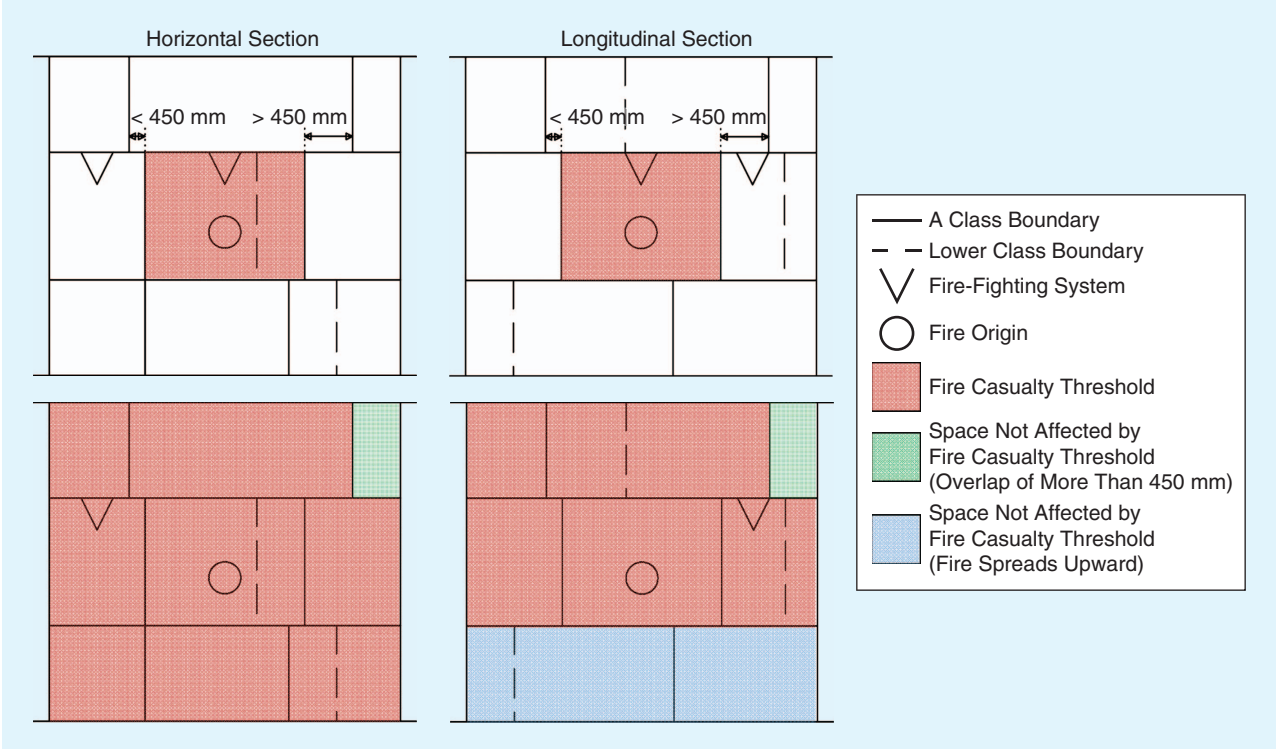


Figure 3. The fire casualty threshold example cases.

availability, and fixed systems placement). This, in turn, caused a rise in design complexity, which can be addressed with several different approaches.

To aid designers in producing a rule-compliant design, a set of criteria has been developed by the IMO MSC. In particular, the following criteria for designing the essential systems shall be used as either standalone or combined:

- separation: locate components of the system in different A-class spaces or watertight compartments
- duplication: replace a piece of equipment with two that are smaller in size (both necessary for the full service)
- redundancy: install more than one component that is independently able to fully perform the service
- protection: arrange adequate shields to protect the system (or any of its components) against fire/flooding
- manual actions: actions carried by the crew to restore the functionality of damaged systems (all the required actions must be performed within 1 h).

Although the combination of all criteria is effectively applied to produce a SRtP compliant design in a ship, the two most significant ones are separation and redundancy. Indeed, designers use such criteria as the basis for their overall essential systems design, while duplication and protection are commonly applied in the reduced sections in which peculiar situations arise. Concerning manual actions, these are used if deemed necessary, commonly to reduce the costs, weight, and volumes of possible automatic equipment. While it may be theoretically possible to build a ship that is completely automated with equipment that can reconfigure itself after a casualty without human intervention, in practice, it is not. Even apart from the problems inherent in the design and control of such a complex automated system, the issue is that the resulting vessel will have most of its internal volume occupied by these automated systems (e.g., sensors and automatic valves), thus limiting the volume for the payload. Therefore, manual actions are used for all of the systems that do not have the need for reconfiguration during the casualty, but the systems may need to be reconfigured after containment of the casualty. However, the limited period allowed for such operations implies the need for a careful design of the equipment concerned, and clear instructions specified for each possible casualty case must be provided through a dedicated manual.

The aforementioned two main design criteria (separation and redundancy) are conventionally exploited through the division of the ship into two subships in regards to the essential systems (Figure 4). The resulting two subships have essential services that are entirely separated and redundant, thus allowing their normal operation in case of casualty in the other ship section. Concerning nonessential systems, they can be managed with suitable criteria depending on other applicable rules and regulations.

Even though ship division seems to be an easy solution to achieve, the fixed placement of significant loads (e.g., propulsion) and equipment makes it a challenge. As a result, the two subships division is not as plain as shown in Figure 4, but their spaces interlock nonhomogeneously (refer to Figure 5). This means that sections of the IPS pertaining to one subship must pass through spaces

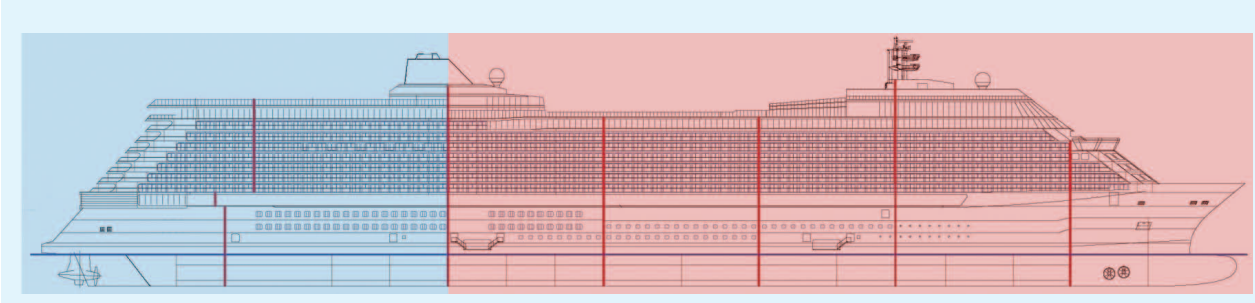


Figure 4. The ideal passenger ship's separation in subships. The blue sections are subship 1, and the red sections are subship 2.

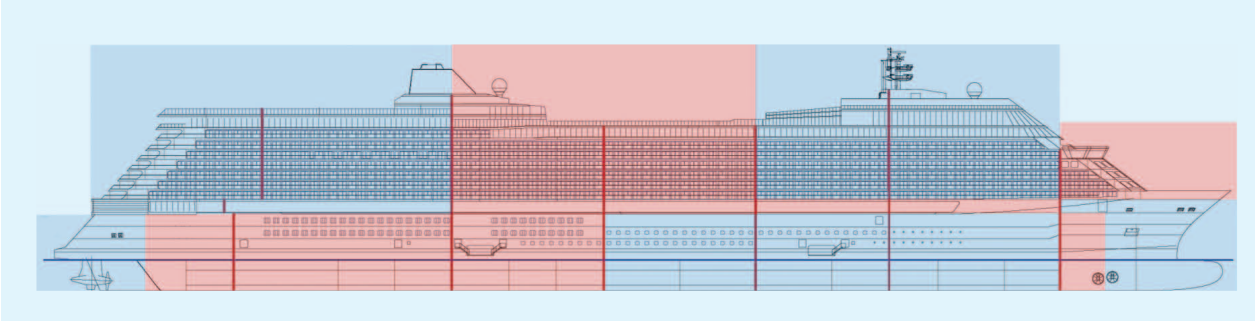


Figure 5. The real passenger ship's separation in subships. The blue sections are subship 1, and the red sections are subship 2.

pertaining to the other, thus leading to issues due to the resulting imperfect separation. In these cases, other design criteria are commonly applied (i.e., duplication, protection, and manual actions).

Redundancy is commonly applied to systems that must deliver the same performance level both before and after a casualty. An example of such a need is the fuel supply systems for a ship's diesel generators (Figure 6). The application of the redundancy concept assures the service continuation after a fault, guaranteeing the correct operation of the remaining generators at their maximum capability. Obviously, the exploitation of the redundancy concept also implies the application of the separation criteria to allow the complete independency among the redundant systems. Otherwise, a casualty affecting a system's section may also affect the redundant one, thus making the redundancy useless (such a practice was common in the past, as affirmed in the following paragraphs regarding the IPS). However, it is possible to design systems that are separated but not redundant, relying on automatic and/or manual actions to recover the system operation after a casualty. This is a common approach for systems that are spread throughout the ship (e.g., drinking water) that are not essential to function during the casualty event. Therefore, their operation can be recovered through reconfigurations after a casualty, separating the influenced sections from the unaffected ones, thus achieving a system that is still functioning even with reduced performance (as the spaces not affected by the casualty continue to operate).

Conversely, protection criteria are applied to the inevitable passages of cables and piping across spaces pertaining to the other subship. An example of such a case, specifically regarding the equipment cooling circuit of two subships, is depicted in Figure 7. Due to the need for cooled water to be distributed into the entire ship, such a system must continue to work despite having some of its sections crossing a space that could be the subject of a casualty. The only possible workaround is the application of protection criteria to the sole sections crossing spaces pertaining to the other subship, making these limited sections resistant to the casualty (e.g., reinforced piping, sealed and insulated cableways, or fire-resistant cables).

It is remarkable to notice that some electrical systems considered essential by SRtP have such a high power level that supplying power through separated emergency supplies is impossible (e.g., the propulsion system during a safe return to port can still absorb some megawatts despite being at a reduced power level due to the low-speed requirement in such a condition). Therefore, the onboard IPS operation must also be assured after a casualty. Consequently, the power system must be designed with the same criteria used for SRtP essential systems, although it not being considered an essential system. However, the application of the redundancy criterion is not possible in this case due to the significant increase in volumes and costs related to the installation of a fully redundant generation system. Therefore, the duplication criterion is applied, causing a reduction in power availability after a casualty that involves one subsection of the IPS, thus leading to the reduced speed requirement in SRtP operation.

While a certain level of duplication and redundancy was already implemented in modern IPS designs (refer to Figure 1, where the opening of the switchboards tiebreaker allows for two electrically independent power systems), until entry into force of SRtP regulation, the components were not separated. Such a lack of attention to the equipment's

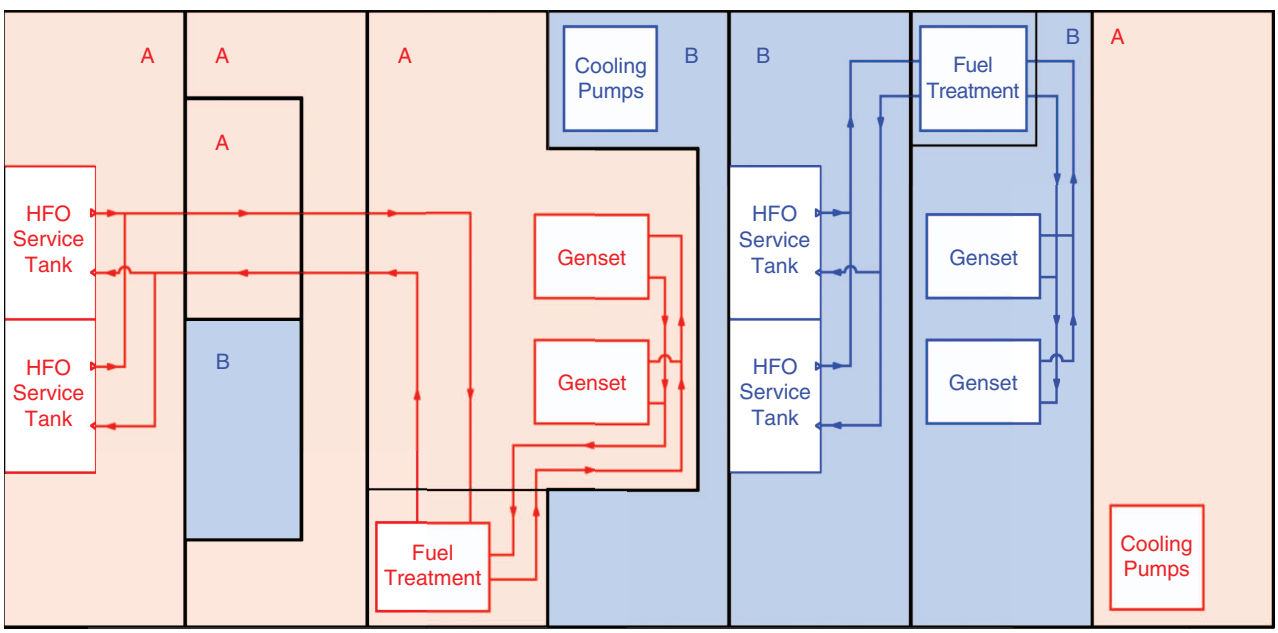


Figure 6. The fuel service, redundancy, and separation of the systems pertaining to the two subships (A and B, in red and blue, respectively). HFO: heavy fuel oil.

physical placement during the assessment of the system's response to faults led to several catastrophic failures in the past. As an example, the two main switchboards were installed in the same space but this caused several accidents in which a fire originated by a fault in one switchboard propagated to the other, thus causing an overall ship blackout. Currently, IPS designers have to address not only the power system architecture (auxiliaries included), but also its spatial placement onboard. This must be done while considering some peculiar loads whose position is fixed by their function and the ship's architecture (e.g., propulsion motors, thrusters, and rudders), thus leading to an increase in both design and building processes complexity.

To reach the building phase and deliver the ship, the compliancy with requirements must be verified and demonstrated to all the stakeholders.

Design Analysis and Verification

The increase in design burden is only part of the impact that SRtP regulation had on ship building processes. To reach the building phase and deliver the ship, the compliancy with requirements must be verified and demonstrated to all the stakeholders. This must be done for the overall vessel's design and for the IPS.

In the marine industry, the entity that oversees analyzing, verifying, and ultimately approving the final ship design is the classification society (CS). In particular, CSs establish technical standards and verify their correct application. Concerning SRtP regulation, the first duty of the CS is to translate its concepts into a set of technical requirements that is aimed at driving designers toward a result in accordance with MSC standards. The second duty of the CS is to analyze the design to verify its compliancy with the society's requirements. If the design is validated (i.e., it is fully compliant with all applicable rules and regulations), the ship can be built. Otherwise, appropriate modifications have to be made. Finally, the last duty of the CS regarding SRtP rules is to make periodic surveys during the ship construction with the aim of verifying that the shipyard proceeds as defined by designers. The latter task is as important as the other two, because issues requiring a design modification commonly arise during the building, thus requiring a further verification and validation by the CS.

Although the design analysis and verification burden seems to fall entirely on CSs, in reality, it is not. Indeed, ship designers must verify their work before consulting a CS to avoid costly and time-consuming validation failures and related design modifications. Such a process obviously increases the costs and time needed to design new SRtP-compliant ships in respect to old noncompliant ones.

Similar to what happened for design criteria, also for the verification process, the IMO MSC has suggested some criteria. In particular, one of the following two approaches must be used to demonstrate the design compliancy with SRtP regulation: a system-based approach and space-by-space approach.

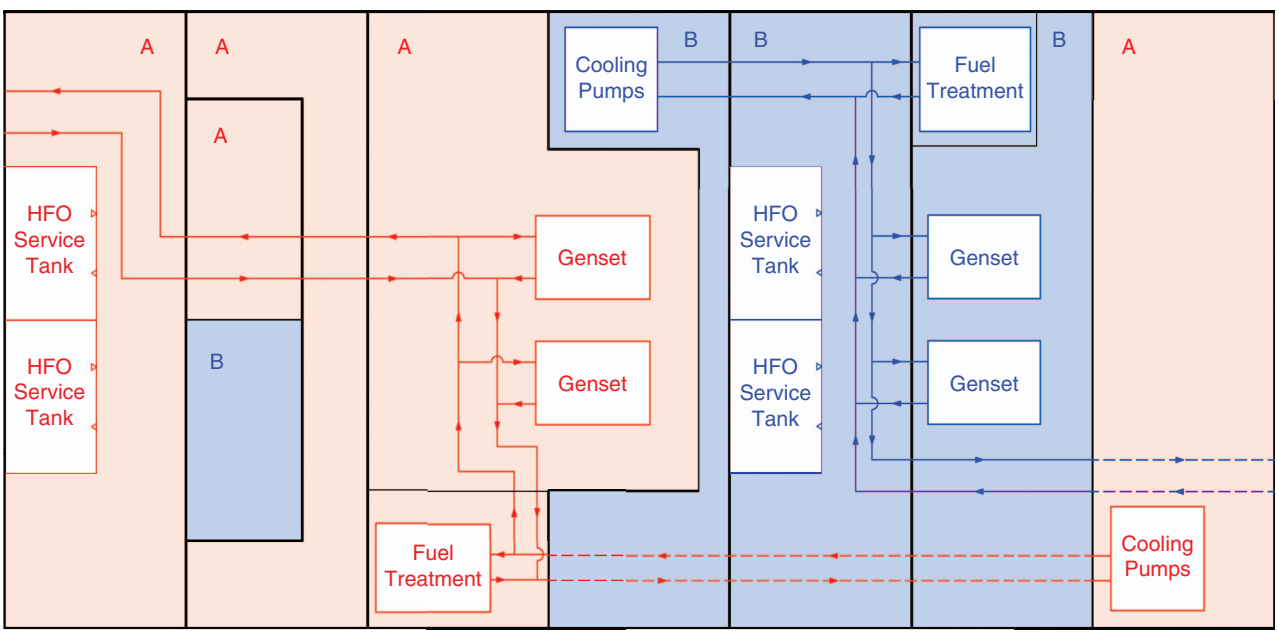


Figure 7. The cooling service with protection through reinforced tubing (dashed lines) of the sections of the redundant system that must cross into spaces pertaining to the other subship (A and B, in red and blue, respectively).

The system-based verification approach is a systematic and structured assessment of a ship's capabilities regarding SRtP requirements. It is focused on the ship as a whole complex system, considering all its internal systems' interrelations. The flowchart depicting all the steps needed to perform the assessment process is shown in Figure 8. It starts with a step dedicated to the collection of specific information, documents, and drawings about the ship design, as stated in the June 2010 IMO report MSC.1/Circ.1369 (i.e., the "ship's definition"). The second step is the overall assessment of essential systems, which is committed to examining essential systems to identify the possible presence of critical systems. These are systems that are classified as essential that may fail to operate adequately due to a casualty below the threshold. If no systems are found to be critical, then no further analysis is needed; thus, the design can be approved. Otherwise, all the identified critical systems must be analyzed in detail. If, and only if, the performance of all the critical systems is considered acceptable, then the design is compliant with SRtP regulation and approved for building. Conversely, a redesign activity must be performed to solve the issues identified during the assessment.

Concerning the space-by-space approach, it involves building a spatial model of the ship with the essential systems allocated to their specific spaces onboard (related auxiliaries and supplies included). The resulting three-dimensional model of the overall ship is then used to verify the compliancy of the ship with SRtP rules by iteratively assuming the presence of the casualties in each onboard space and evaluating their effects. The final objective is to demonstrate that, for each possible casualty, the appropriate essential systems continue to operate despite the casualty presence. If this is true, the system design is considered to be compliant with SRtP requirements. Otherwise, it is not and must be redesigned. In practice, the space-by-space analysis process can be considered composed of two main steps: the first is dedicated to the verification of the compliancy of the single system's design with the chosen criteria, while the second is dedicated to the verification of the correct interrelations among all the essential systems.

The first step depends on the criteria used to design the specific system during the analysis. Concerning redundant systems, the verification is done by hypothesizing the presence of a casualty in the ship spaces to evaluate the cases in which the systems remain in operation and in which the systems fail. The correct application of the redundancy design criteria is verified if, and only if, for each possible casualty, a failure in an essential component is balanced by the operation of the redundant one. Conversely, for the systems designed using only the separation criteria, it must assess the possibility to reach an operative configuration after a casualty by separating parts of the system through automatic and/or manual actions (specified in the dedicated manual). Not only must the effectiveness of the specific

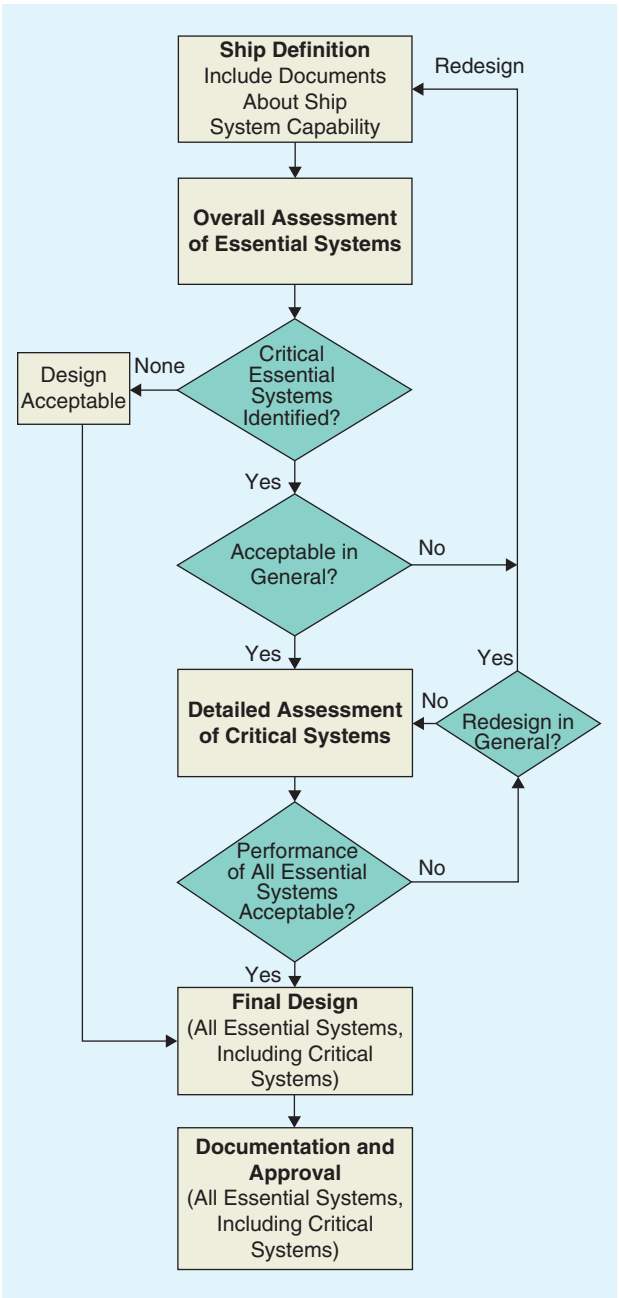


Figure 8. The system-based approach to the verification of SRtP compliancy for passenger ships.

set of operations be assessed, but the required execution time must also be analyzed, given the mandatory time limit set for performing the manual actions.

The second step implies the verification of the correctness of the relations between essential systems and between them and other systems. Each onboard system has a set of inputs (other systems that must be in operation to allow the correct operation of the system in analysis) and outputs (other systems that require the correct operation of the analyzed system to correctly operate themselves). These relationships must be mapped, and the impact of the casualties on each input and output system must be

assessed. The design is considered correct if, and only if, the inputs of a system in operation remain operational for each possible casualty and the operability of the required outputs is guaranteed.

The space-by-space approach is simpler than the former, since the verification process is merely a matter of removing a set of components from the system due to the casualty, and evaluating how their absence affects the system operation. Such an approach presents a significant advantage in respect to the system-based approach. It is possible to implement it through a software, using data coming from the conventional ship-design software and databases, making the verification task highly automated. Therefore, this is the approach currently preferred by most ship designers. Conversely, the system-based approach implies identifying possible critical systems and assessing the impact on the overall system caused by their performance level. It is a more detailed and effective assessment, but it requires more effort, a complex assessment of critical system performance, and a definition of the acceptable level of performance to be agreed with a CS.

Whatever the selected assessment process is, if all the steps are correctly documented (as per SRtP guidelines), then the results can be used as a universally recognized demonstration of the SRtP compliancy, thus ensuring to all stakeholders the final design's compliance with the requirements.

The design is considered correct if, and only if, the inputs of a system in operation remain operational for each possible casualty and the operability of the required outputs is guaranteed.

Existing Approaches to the Safe Design of Complex Systems

Besides the recent attention to safety given by the SRtP rule introduction in passenger ships, assuring a high system's safety standard has been a relevant issue for a long time in several technical areas and applications. Sectors such as aerospace, nuclear power systems, chemical plants, and military systems have developed, each separately, sets of concepts, definitions, and techniques dedicated to the analysis of the systems performance in case of faults. The ability to asses a system's performance level during non-normal operation (e.g., due to faults, errors, and casualties) through an analytical approach is paramount in such applications. These concepts and techniques analyze the possible outcomes of a system design before building it, thus making it possible to correct potential flaws and criticalities, thereby improving the system's safety by design. However, the separate development that occurs in each technical area makes it difficult to use these techniques and concepts in an integrated way, thus lowering the possibility for achievable advantages.

During the last 30 years, a unifying theory has been developed and is condensed in a single corpus with all the concepts and techniques previously developed separately. This approach is called *dependability theory*, and it can provide a standardized set of concepts and definitions with a comprehensive and systematic formulation containing all the past different approaches.

Dependability Base Concepts

Dependability theory relies on strict definitions and well-defined concepts. Because the lexicon itself is considered as a tool, it can be used to understand and manage the system. Indeed, correct lexicon leads to straightforward definitions and universal comprehension among the involved persons, while incorrect lexicon leaves space to ambiguity, thus possibly causing safety issues and related liabilities. Therefore, a short set of definitions must be given, allowing comprehension for the basic concepts of such a theory and its potentialities.

Dependability theory is based on the concept of service. The service is the set of operations performed by an entity in favor of its user(s). It is considered correct if the behavior (the set of operations users perceive as being done by the entity) is compliant with the user specification; otherwise, it is considered as incorrect (and this is caused by the failure in executing one or more operations). It is also possible to define a degraded level of service, which may be acceptable under specific circumstances but not in normal operation. Ultimately, the correct service is the user requirement, and designers must develop the entity (namely, the system) to be able to provide the required service. In addition, the system design must also present a set of qualities to assure the delivery of the expected service with a certain level of trust. Such qualities define the dependability of the system and are called *attributes* (Figure 9). Due to the dependability unifying approach, attributes have been chosen among the several concepts developed in the related past theories and are defined as follows:

- Reliability is the probability that a system performs the correct service at the time $t > 0$, provided that at the time $t_{0=0,}$ the service was correct.
- Maintainability is the probability that the system delivers the correct service at the time $t > 0$, provided that at the time $t_{0=0,}$ the service was not correct and that a repair process is in progress.
- Availability is the probability that a system delivers the correct service at the time $t > 0$ without specifying whether the service was correct at the time $t_{0=0}$.

- Safety is the ability of the system to show a safe behavior (which does not cause any damage) in the presence of a nonacceptable failure.

A system's dependability can be threatened by failures, errors, and faults. A failure is a deviation of the service from the correct one, and it occurs at the operational level. An error is a deviation of a state from its intended and correct value. It occurs at the processing level (e.g., control systems). Since the service is a sequence of system states, a failure means that at least one state deviates from its correct value (i.e., the presence of an error). A fault is the incorrect operation of a piece of equipment (a component) occurring on a physical level. It may cause an error or a failure or remain dormant. A causal link between those categories is present, as faults cause errors and errors cause failures. Moreover, a failure may generate a fault in another system, causing a consequent error in this system, which subsequently generates another failure. These relations are depicted in Figure 10.

Among the dependable attributes, safety is a peculiar one, employing a slightly different set of concepts and definitions. This is due to the different perspectives that must be applied in evaluating safety in the framework of dependability theory. While the other attributes are focused on the menaces to the correct service, safety evaluates the possible harmful consequences (to people, things, and the environment) of an incorrect service. Safety lexicon includes concepts such as *hazard* (the potential source of harmful consequences), *accident* (an unacceptable situation that compromises safety, caused by an unintentional hazard), and *risk* (the danger level of an accident). The base concepts of safety are described extensively in the International Electrotechnical Commission Standard 61508 (functional safety standard).

Regarding the SrTP regulation, its main aim is the reduction of the consequences of a given casualty (below a stated threshold) down to a level that allows the ship to autonomously return to port. Such an aim is achievable through the reduction of both the risk and frequency of casualty occurrences. These topics can be addressed through the dependability theory in its entirety thanks to its comprehensive and systematic approach.

Existing Techniques to Analyze and Verify System's Safe Design

As previously mentioned, along with different set of concepts, different techniques have also been developed in the past in each technical area. All these techniques can be collected in the main dependability theory but keep their individual aims and results, thus making it possible to select the one best suited for each application. These techniques are called *enforcing techniques* by dependability theory and are aimed at analyzing and possibly improving the system's dependability level, thus promoting a more dependable (and therefore safe) design.

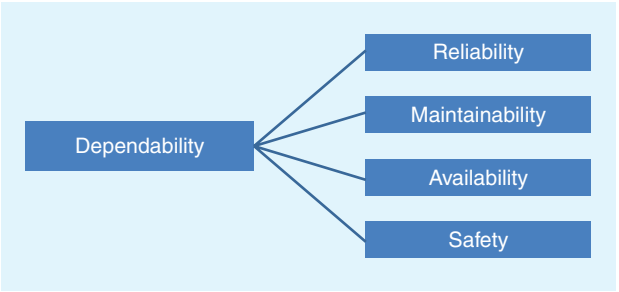


Figure 9. The dependability attributes.

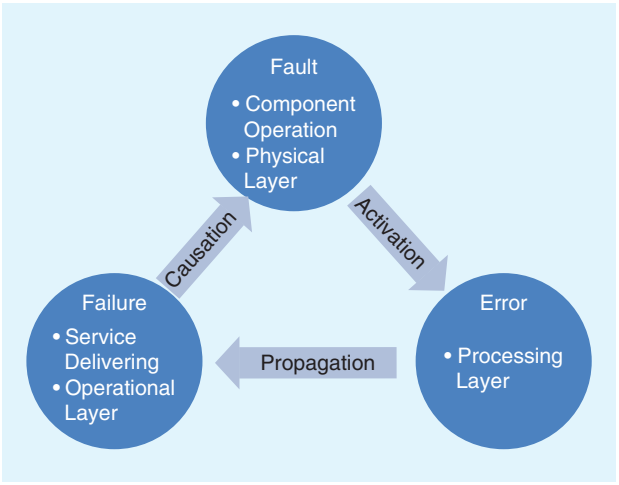


Figure 10. The relationship between fault, error, and failure concepts.

Among the several techniques that can be found in technical literature, some are worth mentioning: failure modes and effects analysis (FMEA); fault tree analysis (FTA); reliability block diagram (RBD); and hazard and operability analysis (HAZOP). Such techniques are well known and are currently used to design and analyze complex systems in mission-critical applications, thus making sufficient a brief explanation of their scope and use.

FMEA was one of the first analysis techniques dedicated to systematic failure analysis. It was developed in the military sector in the late 1950s with the aim to study possible malfunctions in essential systems. The objective of an FMEA is to provide a systematic, comprehensive, and documented analysis to determine the relevant failure modes for the system. In addition, the analysts review components and subsystems to identify failure modes, causes, and effects of the overall system. The analysis proceeds by examining single components to assess the whole system's behavior. For each component, all the relevant data (such as causes and possible solutions) is collected in dedicated worksheets (called *FMEA worksheets*). As a result, the analysts try to find the so-called single point of failure, which is the single component's fault that causes an overall system failure. This is the most common analysis performed in shipboard power systems, as it is required by CSs for mission-critical applications [e.g., dynamic positioning (DP) and naval vessels].

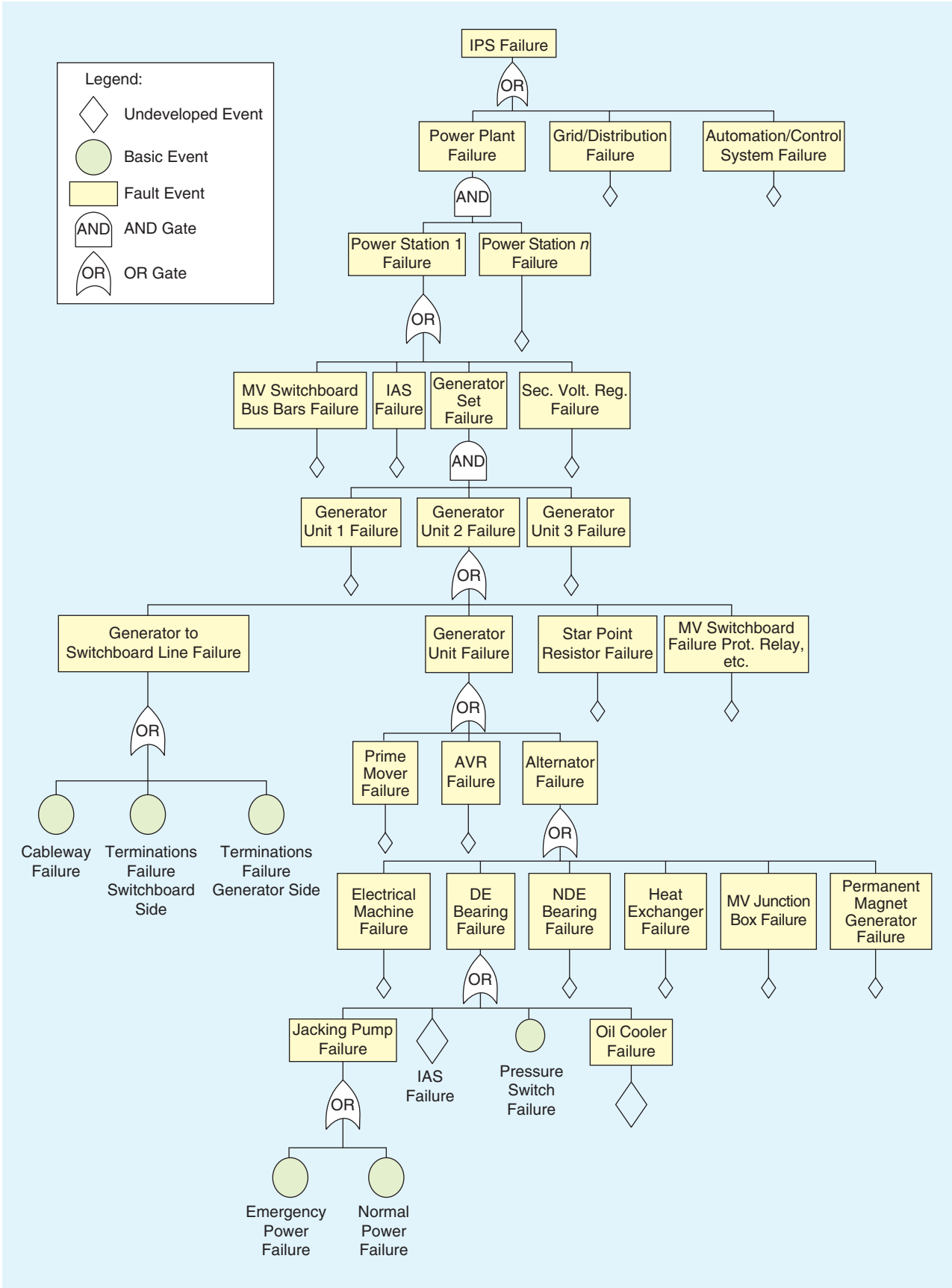


Figure 11. An example of a fault tree diagram built for a shipboard power system. IAS: integrated automation system; Sec. Volt. Reg.: secondary voltage regulator; Prot.: protection; AVR: automatic voltage regulator; DE: drive end; NDE: nondrive end.

The FTA technique was conceived in 1961 to study the Minuteman Missile launch control system for the U.S. Air Force. More recently, its use has spread abroad, and it is now commonly applied to assess the reliability of complex systems (such as nuclear and chemical plants). Consequently, the FTA methodology is described in several industry and government standards, and, regarding power systems, its use has been dedicated mostly to the reliability assessment of electric and electronic components and supervisory control and data acquisition. It is a top-down deductive failure analysis that is used to understand how a system can fail, the implied components, and the relations between them. Starting from an undesired state for the system (typically, a system's failure event, i.e., the "top event"), the analyst applies logic to deduce its causes, deepening the analysis to the identification of the base causes (the components' faults). During the investigation, a diagram is built, called the *failure tree* (see Figure 11), which maps the relationships between faults and components by Boolean logic.

The RBD is a diagrammatic system modeling technique aimed at showing how a single component's reliability contributes to the success of a complex system. It implies building a diagram in which each component is connected (in a series or parallel) with the others, following dependability relations (Figure 12). A parallel connection implies redundancy, because all of the elements must fail for the paralleled section to fail. However, in series-connected components, the fault of one leads to the loss of the entire section. Failed components are considered as *open paths*; therefore, the system operation is guaranteed only if there is a continuous path connecting one side of the diagram with the other. The RBD provides an easy-to-read and understand representation of the system that is mission success oriented.

The HAZOP technique was developed in the 1960s for the chemical industry. Currently, HAZOPs are considered a safety/legal requirement in that industry, and any findings become legal requirements with costly implications and on-going controls. An HAZOP is a structured analysis of a process, operation, or system performed by a multidisciplinary team. The team examines, node by node, the design of a system to identify possible flaws and safety hazards. This is achieved through the combination of a set of guidewords (adjectives) with the system's parameters and used to seek deviations from the design intent and to evaluate whether such deviations are meaningful (the former are the ones physically possible; thus, they are retained, while meaningless associations between attributes and parameters, such as "no-temperature," are discarded). Afterward, the team concentrates on those that could lead to potential health, safety, or environment hazards. For each hazard, the likelihood of a specific undesirable event occurrence within a specific period

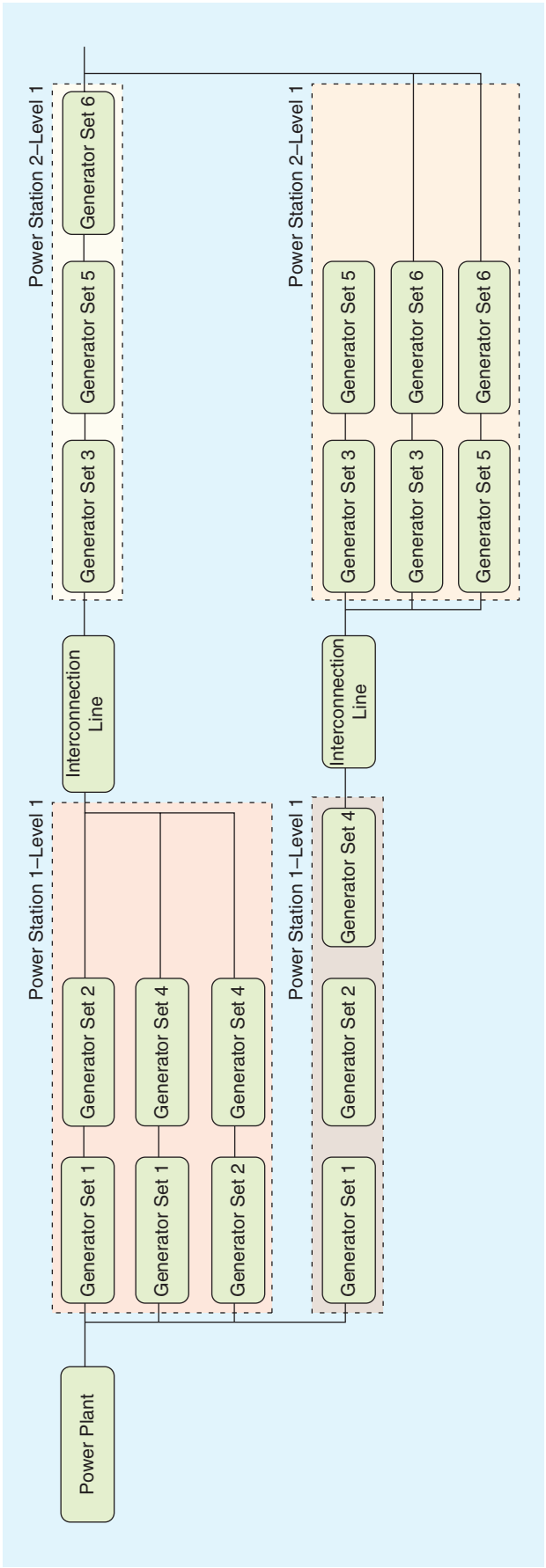


Figure 12. An example of an RBD for a shipboard power system.

TABLE 1. The risk assessment matrix.

0–5 = Low Risk 6–10 = Moderate Risk 11–15 = High Risk 16–25 = Extremely High Unacceptable Risk	Severity of the Potential Injury/Damage				
Likelihood of the Hazard Happening	Insignificant damage to property or equipment, or a minor injury Risk level: 1	Nonreportable inquiry, minor loss of process or slight damage to property Risk level: 2	Reportable inquiry, moderate loss of process or limited damage to property Risk level: 3	Major inquiry, single fatality critical loss of process/damage to property Risk level: 4	Multiple fatalities catastrophic loss of business Risk level: 5
Almost certain 5	5	10	15	20	25
Will probably occur 4	4	8	12	16	20
Possible occur 3	3	6	9	12	15
Remote possibility 2	2	4	6	8	10
Extremely unlikely 1	1	2	3	4	5

or under specific circumstances is determined. The combination of hazard severity and its probability defines the risk related to the specified deviation (as shown in Table 1). Where deviation causes are found, the team evaluates their consequences, taking into account existing safeguards and using experience and judgment. Each identified deviation that falls into the high-risk area must be addressed and solutions proposed to lower its occurrence likelihood, its hazard, or both. Due to its focus on risks and potential hazards, the HAZOP technique is extensively used in functional safety related analyses.

Facing the SRtP New Issues Using Existing Tools

The introduction of the SRtP regulation created several issues to designers, and its impact has not been trivial. At present, the designers rely mainly on the MSC suggestions to achieve the required level of safety. Although the results appear to be good, a hoped enhancement can be pursued. The correct balance of all the ship design drivers (performance improvement, cost reduction, weight reduction, and volume reduction) with the requirements' compliancy is difficult. The possibility of exploiting the same result (rules' compliancy) with several possible system designs leads not only to the issue of correctly evaluating the degree of closeness of each driver to its target levels, but also to the issue of correctly setting such targets a priori. This is true for areas that can be evaluated using well known and fully recognized indexes, such as costs and weights, but this becomes paramount for safety related ones, whose analysis is commonly based on several different concepts, which are often not representable by numerical indexes. Indeed, the marine sector currently lacks fixed numerical targets for several relevant concepts related to safety and, in general, the system's response to faults. While land power systems have well-defined numerical requirements (e.g., the System Average Interruption Frequency Index and System Average Interruption Duration Index described in IEEE Standard 1366), the marine sector still mostly relies on verbal requirements.

In this context, the dependability theory can be the enabling tool that allows a step forward in the design processes of ship systems. Such a theory can give a universally recognized framework for the analysis of SRtP requirements and related design issues, also providing numerical indexes that can objectively exploit concepts that normally are not exploited. Using the techniques given by dependability theory, these indexes can be calculated, compared, improved, and ultimately optimized along with the other design indexes. Both the design and verification processes discussed in this article are based on a set of numerical indexes and coupled with a set of verbal requirements, which both come from multiple sources. At present, the latter must be interpreted by designers to be introduced into the design process, and this must equally be done by analysts to proceed with the verification process (Figure 13).

It is clear that the expertise of both these professional figures can deeply affect the overall process. This is because different levels of knowledge about the system in the course of design and different points of view about how a design must be done may lead to different interpretations of the same requirement. Therefore, misunderstandings may arise, causing possible costs and time increase due to the involved redesign process. From this perspective, the functional safety branch of the dependability theory can be used as a tool to translate the actual set of verbal requirements in proper numerical requirements, thus leading to a clear and universally recognized interpretation (Figure 14). Indeed, its strict lexicon allows

removing the potential misinterpretations among designers and analysts, making it possible to apply a unique reading of the verbal requirements. Moreover, through its concepts and techniques, functional safety at first enables the definition of an acceptable level of safety for the system in the course of design, based on historical data and systems already approved, and then it allows evaluation of the degree of closeness of all the possible design solutions to the defined target.

Along with the significant improvements to safety that could be reached by using functional safety, the application of dependability theory can provide several other advantages. Indeed, dependability techniques can be used to perform optimization and refinement both in design and verification processes, along with common design drivers' evaluations. In the following, some examples of such capabilities are given.

Regarding the aforementioned space-by-space verification approach, its base concept is similar to the FMEA process. Indeed, both are aimed at assessing the effects on the overall system of an event: a single component fault in FMEA, a single space, or an entire MVZ in a space-by-space approach. Moreover, both imply evaluating the inputs and outputs of the system in the course of study, trying to find possible causes and effects of faults in FMEA, or assessing functional relationships in SRtP verification. Due to such a similarity, it may be possible/useful to introduce into the SRtP verification process tools originally developed for the FMEA (e.g., software and modeling) to take advantage of what has been already developed for such a technique.

In addition, the input–output relationships assessed by the space-by-space verification can be used to execute an FTA or an RBD, with a reduced effort with respect to a standalone analysis. Conversely, such techniques may also be employed during design, thus allowing an easy final verification to be performed. Both techniques can conveniently identify the single points of failure in the system, which are solvable through the application of proper design criteria. Moreover, the excessive application of redundancy criterion can also be indicated (redundant components whose effect on the overall system's dependability level is risible, but they have a relevant effect on weights, volumes, and costs) and are thus removed. In addition, it is possible to find components that may be either improved, to enhance the whole ship's dependability (by substituting them with more dependable but costly ones), or worsened, if their impact on global indexes is risible (by installing less dependable but cheaper ones).

Finally, it is remarkable that some marine applications that use concepts similar to the ones already present in SRtP exist. The ships endowed with DP systems must comply with several requirements concerning their response to faults and possible accidents. Such requirements are significantly stricter than the SRtP ones, especially for the higher DP classification levels. Indeed, the DP systems with the highest performance (e.g., the American Bureau of Shipping DPS-3 class) shall continue to operate after a given casualty (fire and flooding, equally to SRtP), assuring the same performance level as before the event (delivery of the correct service). In contrast, SRtP regulation allows a certain degradation of the service, given that it is

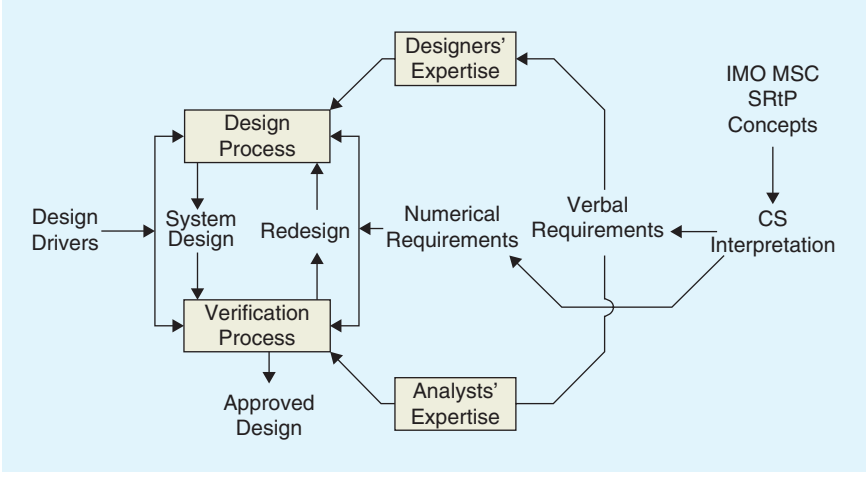


Figure 13. The current state of the relationships among design/verification processes and SRtP requirements.

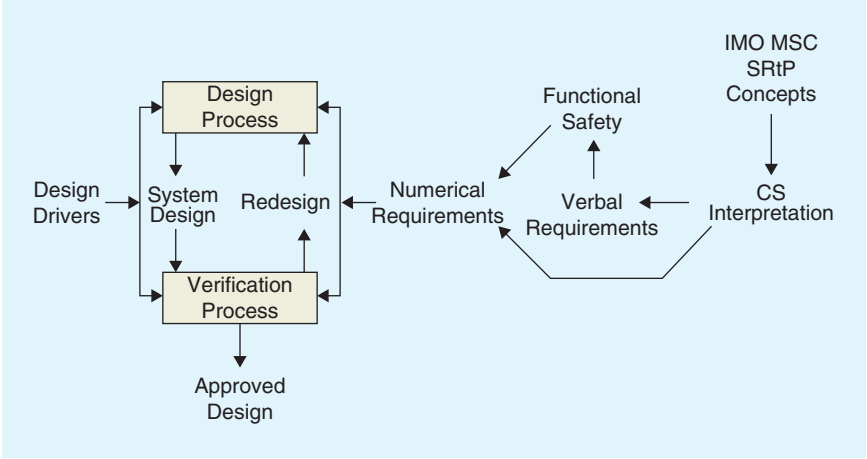


Figure 14. The state of relationships among design/verification processes and SRtP requirements after dependability theory application.

acceptable (e.g., a slower ship, but one that is able to return to port; a lower comfort level for passengers, but they are alive). It is important to note that, when designing vessels endowed with DP systems, some shipbuilders apply the HAZOP technique to foresee possible harmful consequences caused by faults and thus reduce them by modifying the design. Consequently, it may be possible to gather competences from the DP systems design sector by using such an expertise to improve the passenger ships.

Conclusions

In recent years, a new set of mandatory rules has been presented, aimed at increasing the safety of modern passenger ships (namely the SRtP regulation). Given the foreseen rise in passenger ship numbers and sizes in the near future, such a regulation has been proposed by the IMO to improve the intrinsic survivability of large passenger ships, exploiting the concept that the ship is its own best lifeboat. Therefore, SRtP regulation is aimed at increasing the resilience of ships with respect to the two most common accidents onboard, fire and flooding, assuring at the same time passenger safety and reducing the need of abandoning the ship. However, such a growing attention to the safety topic led to the issue of changing both the design processes and the designers' perspectives toward a more safety-oriented vision without impairing the achievement of the conventional ship design drivers (such as performance improvement, cost reduction, weight reduction, and volume reduction).

Although a generally accepted solution has been found by designers, by exploiting redundancy and separation as the main design criteria and applying a space-by-space verification approach, the issue of producing a design that is both compliant with the regulations and competitive on the market is still present. In this regard, concepts and techniques developed in other mission-critical areas (e.g., nuclear power and chemical plants) can be used as tools to improve the ship design given their well proven capabilities, which have been demonstrated through several decades of utilization. Their implementation can pass through the unifying approach given by dependability theory, which allows the handling of all these different concepts and techniques through a systematic and comprehensive approach, thus simplifying the designer's work. Such a theory allows not only removing the misunderstandings caused by the possible varied interpretations of verbal requirements by system designers and design analysts, but also evaluating safety as a set of numerical indexes, in contrast to the actual verbal approach. Moreover, the representation of safety through numerical indexes allows including it in the design process at the same level as the other design drivers, thus enabling evaluation, comparison, and optimization of the overall design.

Through the application of dependability, the foreseen result is an integrated ship design process that can receive several different requirements, each defined by a set of parameters, and produce a compliant design optimized with respect to all the design drivers, including safety.

For Further Reading

International Maritime Organization. (2006, Dec. 8). Amendments to the international convention for the safety of life at sea, 1974, as amended. Int. Maritime Organization. London. Tech. Rep. MSC.216(82). [Online]. Available: http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-(MSC)/Documents/MSC.216(82).pdf

International Maritime Organization. (2010, June 22). Interim explanatory notes for the assessment of passenger ship system's capabilities after a fire or flooding casualty. Int. Maritime Organization. London. Tech. Rep. MSC.1/Circ.1369. [Online]. Available: http://imo.udhb.gov.tr/dosyam/EKLER/MSC.1-Circ.1369.pdf

D. B. Vicenzutti, G. Giadrossi, and G. Sulligoi, "The role of voltage controls in modern all-electric ships: Toward the all-electric ship," *IEEE Electrific. Mag.*, vol. 3, no. 2, pp. 49–65, June 2015.

V. Bucci and A. Marinò, "Influence of the 'safe return to port' standards on the integrated design and arrangements of small passenger ships," in *Proc. 17th Int. Conf. Ships and Shipping Research NAV 2012*, Naples, 2012, pp. 1–10.

G. Buja, A. da Rin, R. Menis, and G. Sulligoi, "Dependable design assessment of integrated power systems for all electric ships," in *Proc. Electrical Systems for Aircraft, Railway, and Ship Propulsion*, Bologna, 2010, pp. 1–8.

R. M. Vicenzutti and G. Sulligoi, "Dependable design of all electric ships integrated power system: New design process," in *Proc. 2016 Int. Conf. Electrical Systems for Aircraft, Railway, Ship Propulsion, and Road Vehicles and Int. Transportation Electrification Conf. (ESARS-ITEC)*, Toulouse, France, 2016, pp. 1–6.

Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC Standard 61508, 2010.

IEEE Guide for Electric Power Distribution Reliability Indices—Redline, IEEE Std 1366-2012 (revision of IEEE Std 1366-2003), 2012.

Biographies

Andrea Vicenzutti (avicenzutti@units.it) is with the Department of Engineering and Architecture, University of Trieste, Italy.

Daniele Bosich (dbosich@units.it) is with the Department of Engineering and Architecture, University of Trieste, Italy.

Roberto Pelaschiar (roberto.pelaschiar@fIncantieri.it) is the head of the Electric Power Systems Office at Fincantieri Italian Shipyards, Trieste, Italy.

Roberto Menis (menis@units.it) is with the Department of Engineering and Architecture, University of Trieste, Italy.

Giorgio Sulligoi (gsulligoi@units.it) is with the Department of Engineering and Architecture, University of Trieste, Italy.