# All-Electric Ship-Integrated Power Systems: Dependable Design Based on Fault Tree Analysis and Dynamic Modeling

A. Vicenzutti, *Member, IEEE*, R. Menis, *Member, IEEE*, and G. Sulligoi, *Senior Member, IEEE*

***Abstract*— The all-electric ship concept is becoming a standard for ships with large power requirements. At present, the design of the onboard power system [i.e., the integrated power system (IPS)] is done through a well-proven process. This process relies on historical data and trial-and-error procedures developed in nearly 30 years of design experience to address the ship's complexity. Nowadays, the evolution in IPSs is pushed forward by the introduction of more demanding requirements, which can be complied with only by using new power system architectures and introducing onboard innovative subsystems. However, introducing innovation by means of a design process defined on the basis of past experience is inefficient. Thus, new design paradigms are needed. In this regard, concepts and tools from other technical areas can be used to achieve a "dependable design process" able to ease the introduction of innovation in ships' IPSs. In this paper, after a brief presentation of the conventional process and the actual drivers pushing toward its revolution, the dependable design process is proposed. The latter integrates both dependability enforcing techniques and dynamic power system modeling. Insights about the process integration in the overall ship design process are given, while an application example is used to show the effectiveness of the proposed approach.**

***Index Terms*— All-electric ships (AESs), dependability, dynamic modeling, fault tree analysis (FTA), integrated power system (IPS).**

## NOMENCLATURE

| | |
|---|---|
| AES | All-electric ship. |
| AVR | Automatic voltage regulator. |
| BB | Birnbaum importance index. |
| DG | Diesel generator. |
| DP | Dynamic positioning. |
| FF | Failure frequency index. |
| FMEA | Failure modes and effects analysis. |
| FT | Failure tree |
| FTA | Fault tree analysis. |
| FV | Fussell–Vesely importance index. |
| IPS | Integrated power system. |
| KPI | Key performance indicator. |
| MTBF | Mean time between failures. |
| MTTF | Mean time to failure. |
| MTTM | Mean time to maintain. |
| MTTR | Mean time to repair. |
| MVZ | Main vertical zone. |
| OC | Operating condition. |
| QoS | Quality of service. |
| SG | Speed governor. |
| SWBD | Switchboard. |
| TE | Top event. |

Manuscript accepted May 24, 2019.

The authors are with the Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (e-mail: avicenzutti@units.it).

## I. INTRODUCTION

AT PRESENT, the AES concept is a standard for several vessel types [1], [2], but its application in the marine sector is steadily increasing. The peculiarity of an AES is its complex electrical system (the so-called IPS), which supplies all onboard loads, propulsion included. The IPS is equivalent to a large power microgrid operating in islanded configuration [3] (Fig. 1) and packs significant power levels (up to 100 MW) in a reduced extension system (common AESs length is lower than 300 m). An IPS is composed by several subsystems, dedicated to the generation, distribution, and usage of the electric power. Moreover, the system's control and protection functions are provided. These subsystems are strictly coupled and installed in a confined space (the ship's hull). Therefore, the IPS is a complex system with multiple interactions among its components, in which the simplification hypotheses used in designing and managing land power systems are not fully valid.

To correctly operate, an IPS must meet strict power quality and QoS requirements [2]–[4].

The compliancy with the requirements must be met despite the disadvantageous peculiarities of an IPS, which are as follows:

1) the islanded operation;
2) the presence of single loads whose power is comparable with single generators' one (e.g., propulsion);
3) the pervasive presence of power converters;
4) the presence of several control systems acting on a low decoupled power system.

The IPS can be considered as the core system of an AES, being all loads powered by electricity. In fact, losing power generation means losing the ship's control, which, in turn, can lead to harmful consequences (i.e., loss of life, significant property damage, or damage to the environment). In this context, designing an IPS is a complex task that is becoming

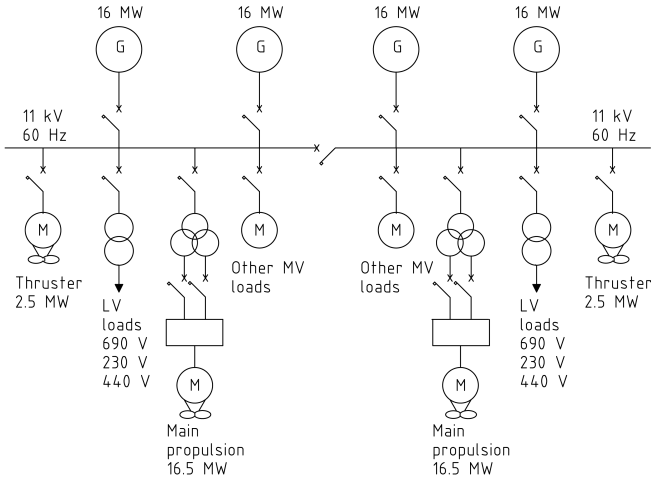


Fig. 1. Notional all electric cruise ship IPS [3].

more complicated as both the already present requirements became stricter and new ones are set. To face such an issue, this paper proposes a dependable design process integrating dependability theory and dynamic power system simulators.

The dependability theory comes from computer science technical area. It is focused on the service given by the system in favor of its users, which must be assured in spite of faults, errors, and failures. With respect to such topics, the importance of systems' correct behavior in fault conditions has always been capital for Oil & Gas marine applications, specifically in DP systems [4]. This is due to the significant level of risk related to the loss of power supply during operation (e.g., collision with other vessels, loss of payload, and so on) [5]. Likewise, similar considerations led to the birth of the survivability concept in the military area [6], [7], while in recent times, attention toward these topics has become common also in the cruise sector [3]. Consequently, several researchers are interested in the application of dependability on the design of AESs [10]–[15].

When considering the design of IPSs for ships with strict QoS requirements, the application of the conventional design approach may lead to several issues [16]–[18]. Thus, in the past, the regulatory bodies enforced specific rules to oblige the designers to find the "single point of failure" for the system [18], [19]. Such an action led to the widespread use of the FMEA in marine sector, as a mandatory requirement to attain ship classification (e.g., refer to [20]). The FMEA introduction significantly improved the ships' design. However, Phillips *et al.* [21] present some issues regarding the correct use of the FMEA by designers, questioning its ability in further improving system design above the actual level. Indeed, the FMEA lacks the ability to perform quantitative analysis, which is the capability of calculating numerical indexes about the system's dependability [22]. Such a capability is the enabler for further improvement in design efficiency and effectiveness. In fact, the evaluation of numerical indexes makes it possible to focus the design effort on the components with the highest effect on the system performance, while, at the same time, allowing to objectively compare different design solutions [19]. In this regard, quantitative analysis techniques are already used in some industry applications, like the fault tree analysis (FTA) [23], [24].

For what concerns software simulators, their use is a standard practice in the research area. However, nowadays, they are becoming more common also in industrial applications. As an example, in [25], a dedicated model has been built to test the power system protections onboard a ship, while, in [26], several different models have been interfaced together to evaluate the effect of sea state on the IPS operation. The use of systems' dynamic models can be beneficial to current design processes, thanks to the amount of information they provide about the system in the course of design.

Given these premises, this paper proposes a new design process, leveraging the capabilities of both dependability techniques and dynamic power system simulators. The proposed process has two objectives: the improvement of actual IPSs design and the correct design of innovative ones. Such goals are attained by means of integration between the two design tools, which is novel with respect to the actual state of the art found in the literature. In particular, the results obtained through a quantitative dependability analysis of the IPS are used to feed a dedicated power system simulator, aimed at assessing the IPS dynamic response to the most critical fault events. Along with the removal of the single points of failure (like conventional design process already do), the proposed process allows finding new design solutions that stop the failure process during its dynamic evolution from the basic faults. At present, such a result is achieved by exploiting the designers' experience during the FMEA process, which is clearly an unfeasible approach for designing innovative IPSs on which no previous experience is available. The proposed process is intended to be used throughout all the design of the system, from early-stage design to product engineering, by performing a new round each time new information is developed. This allows developing an initial design that is already focused on the QoS requirements, and to guide the designers up to the final design. The basic concepts of the proposed process have been briefly presented in [27]. Conversely, this paper presents the motivations pushing toward the conventional design process change, analyzes in depth each step of the proposed process, and validates it by means of an application example.

This paper is structured as follows. Section II presents a brief analysis of the conventional IPS design process and discusses the motivations pushing toward its revision. In Section III, the dependability techniques and the dynamic power system modeling approach are presented, focusing on their possible use in IPS design. The proposed dependable design process is then described in Section IV, including indications about its correct integration into the overall IPS design process. Finally, a validation through a simplified case study is given in Section V.

## II. Designing IPSs for AESs

### A. Conventional IPS Design Process

The IPS design is developed throughout the overall AES's design process, by means of a dedicated set of tasks starting

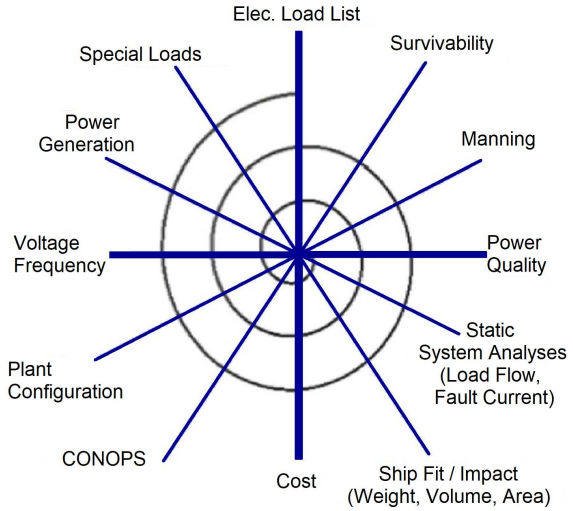


Fig. 2. IPS design spiral process [30].

during the ship's concept design and proceeding until functional design [28], [29].

During the first phases of ship design, the IPS base architecture is defined, while in the latter phases, the process ends with the definition of the electrical equipment to be acquired from external suppliers. Common inputs of the IPS design process are the loads to be supplied, the owner's requirements, and the relevant rules and regulations. The expected output data are the overall system design and the bills of materials, including specific details such as the power system architecture, the size and number of generators, and so on. The conventional representation of the IPS design process is a spiral, as shown in Fig. 2 [30]. Given the possibility of developing in parallel some design activities, the spiral design process is not perfectly representative of how a real IPS design works. However, it is commonly used to explain the basics of ship design.

The spiral design process develops a feasible solution through an iterative sequence of design steps. At first, the designers use their knowledge to define the most suitable starting solution, able to comply with all the applicable requirements on the basis of their past experience. Then, they develop the solution and test whether it achieves the required level for a given set of KPIs or not. If the test is passed, the starting solution is fixed and the designers proceed to develop in detail all of its subsystems. Conversely, if the test is failed, the designers must propose and test a new design solution. During the first round, only the general design is defined, allowing easily proposing and testing new solutions. Afterward, consecutive rounds of the spiral allow developing more details, providing information to guide the designers' effort to a common target [29], [30].

It is relevant to note that ships have specific constraints in terms of space and weight (i.e., a common issue in transportation applications). Indeed, dedicating more space to a component implies reducing the available space for another one, given the limited amount of space onboard a ship. Due to these constraints, the designers must find a feasible balance among all the limiting factors, including requirements compliancy and considering also the nonelectrical components. Consequently, a correct IPS design cannot be achieved without considering its impact on the whole ship, which is commonly assessed through dedicated steps into the design process (some of them are visible in Fig. 2).

### *B. Need for Innovation in IPS Design Process*

The design of complex systems is commonly addressed by neglecting some of the interrelations among subsystems. Typically, this is done by considering only the most significant parameters affecting the design, which are identified through previous experiences. This is done also during the design of IPSs. As an example, the issue of keeping the THD within given bounds is commonly addressed by imposing separate limits on each component's harmonic injection content and then measuring the real value on the built system. Obviously, the forceful simplification of a complex system can lead to issues in the final product, which can be found only when the ship is already built. At that time, the range of possible corrective solutions is limited and the related costs are high.

Such an approach worked well until now, thanks to the significant knowledge base developed during the past 30 years through trial and error procedures. However, several changes in ship design are being promoted at present, both by the introduction of new requirements (e.g., the safe return to port regulation for passenger ships [3]) and by the owners' request to integrate onboard innovative subsystems. While the integration of electric weapons [31] and energy storage systems [32] is foreseen mostly for naval vessels, the increase in variable speed drive installation in new ships and the refitting of old ships with present-day technology are an actual trend [33]. Moreover, to address the needs of the future ships, new IPS architectures are being proposed, pointing toward the introduction of full dc power systems [34]. In this regard, the lack of prior knowledge about the correct design for these new IPSs can lead to suboptimal results when applying a conventional design approach. In particular, not knowing how these innovations affect the overall ship's KPI is one of the main concerns for ship designers. Indeed, the benefits of a new technology are usually assessed in terms of specific advancements with respect to its previous iterations by researchers. This approach makes it difficult for ship designers to infer how the innovation will affect their product, due to the complexity of a ship. As an example, at present, MVDC distribution has been mostly presented as advantageous with respect to conventional MVAC one in terms of electrical performance and survivability. However, most of the shipbuilders are not specifically interested in increasing electric power system performance or reconfigurability, being them satisfied by the levels achieved by actual ac IPSs. Conversely, they are interested in having proof of how MVDC distribution can improve their ship in terms of KPI, such as fuel consumption, available space for payload, ship weight, safety, and so on. The above-mentioned KPI depends on the overall ship's design; thus, their objective evaluation can be achieved only by designing a complete ship with the new

technologies, and by comparing it with the same ship built with conventional ones [35].

The issue of correctly integrate innovation onboard ships is worsened by the actual state of the marine market. In fact, nowadays, the profit margins for a shipyard are lower than those in the past, thus making real-scale prototypes costs unbearable by most of them. Therefore, while significant innovation can be exploited from academic and industrial research results, very few actors can thoroughly demonstrate on the field the effects of new technologies on a ship before putting it into the market. In fact, the most probable outcome of a bad design is the increase in both capital and operative expenditure. The former is caused by the increase in design times due to the lack of knowledge about its correct exploitation, while the possible happening of unforeseen issues during the ship operation leads to the latter.

Thus, a new design process needs to be applied, to lower the risks of integrating innovation into a product in the absence of a full-scale demonstrator. Such a new process cannot be the conventional one, because of the disruptiveness of most of the new technologies [36]. Thus, a change in design paradigms is needed, aimed at including into design processes tools able of preventing the appearance of issues, rather than addressing them after their appearance in the built system, as well as tools able of predicting the effect of innovation on the overall ship's KPI. In such a way, each ship design can exploit at its best the state-of-the-art technologies, thus assuring the maximization of the expected advantages for each specific application.

## III. Innovative Design Tools

The most effective way to improve the design process is to develop a new approach from scratch. In this regard, two promising proposals can be found in literature: the collaborative concurrent design and the design space exploration [29]. Their application can lead to significant improvement in ship design, at the price of placing a significant toll on designers. In fact, a complete design process overhaul implies not only changing software, work organization, and data flow, but also changing designers' way of thinking design. Instead, the adoption of a less invasive approach can be promoted to improve the actual design process while mitigating the burden placed on the designers. Such an approach can be focused on solving the conventional design defects through the introduction of steps dedicated to the exploitation of innovative design tools and methodologies. The goal is to develop new knowledge about the integration of new components and innovative system architectures and to attain an overall improvement of the final product and an increase in design effectiveness. Among the several proposals that can be found in literature, two tools have been considered as suitable: the enforcing techniques given by the dependability theory and the dynamic power system modeling.

### A. Dependability Theory and Techniques

The dependability theory provides a systematic approach to the analysis and management of the fault's origin, effect, and related countermeasures in complex systems. It was conceived as a general approach to the study of complex systems with high-QoS requirements [37]–[41]. One of its goals is to clarify ambiguities among the several previously developed concepts (e.g., safety, fault tolerance, reliability, and so on), by providing a set of widely applicable general concepts, aimed at improving cooperation among different scientific communities [42]. To this aim, Al-Kuwaiti *et al.* [43] provide an in-depth analysis of the commonalities and differences among dependability, fault tolerance, reliability, and survivability theories. Extensive explanations about dependability theory can be found in the literature, as well as discussion about its use in systems with high-QoS requirements [5], [12]–[14], [44]–[46]. Conversely, in this paper, only a brief explanation is given.

Dependability theory main concepts are threats (events menacing system's dependability: faults, errors, and failures), attributes (quantities or qualities measuring system's dependability level: reliability maintainability, availability, and safety), and enforcing techniques (techniques intended to improve system's dependability). Dependability attributes can be demonstrated through several different mathematical indexes, which are assessed by means of the fault-forecasting techniques. In particular, these techniques are the most suitable ones to improve system design. In the framework of fault-forecasting techniques, two classes of techniques can be found: qualitative and quantitative [47]. The former are aimed at identifying, locating, and classifying the faults that cause failures, and analyze the associated failure modes. The most widely known qualitative technique is FMEA [19], [48]. Conversely, quantitative techniques are aimed at assessing the dependability attributes of the system in terms of probability indexes. In this class, another well-known technique can be found: the Monte Carlo simulation [49].

Qualitative techniques can be applied without knowing historical/statistical data about system components (i.e., the failure data), and do not require any specific software/tool (being them document based). The qualitative analysis is usually a straightforward process that analyzes the relationship between the components of the system. Thus, the effect of design modification can be appreciated by comparing the presence or absence of causal links among components faults, before and after the designer intervention. The more complex the system is, the more difficult the analysis becomes due to the increase in the number of components and related interactions to be considered. Moreover, evaluating the effect of multiple concurrent components faults poses a significant burden on the analysts, thus being prone to human errors. Despite the disadvantages, qualitative techniques are widely used in the shipbuilding sector as a tool of verification. In fact, as already mentioned, FMEAs of onboard essential systems are required by classification societies to obtain ship's classification. In this regard, FMEAs led to significant improvement in ship design in the past, but the innovation in marine systems area is making them a tool that cannot fully respond to actual designers' needs.

Differently to qualitative techniques, quantitative ones rely on the failure data about the system components to be carried out. In this regard, the mathematical calculation needed for evaluating the probabilistic indexes that constitute the

dependability attributes are not manageable without using specific software tools. Luckily, the quantitative analysis process can be broken down in small blocks and done in parallel, easing the analysis of large systems. Indeed, it is possible to evaluate the indexes for single subsystems separately, and then using such data to evaluate the overall system performance. As an example, it is possible to calculate the probabilistic indexes for a diesel engine, for an alternator, for an SG, and for an AVR one at a time. Later on, the data about these subsystems can be used to evaluate the dependability indexes for a complete DG, and then, the results can be applied to an electrical system containing the generator along with several other components. The quantitative analysis process makes use of specific software that allows the analyst to build an easy to comprehend schematic of the case in study, while automatically building the related mathematical model on the background. In such a way, by modifying the scheme, it is possible to test the effects of different design solutions in systems with a high number of components. Finally, through the mathematical model, several scenarios can be tested, including ones in which multiple faults are present at the same time.

One of the most representative quantitative analysis techniques is the FTA, which was conceived in 1961 to study the Minuteman Missile launch control system [50]. Nowadays, its use has spread throughout several technical areas, from land power systems [51] to marine applications [52], [53]. The FTA has been selected in this paper as the most suitable technique. However, several other techniques are integrated into the dependability framework, thus making it possible for the designer to choose the most suited one for its goals.

### B. Dynamic Power Systems Modeling

Nowadays, the use of software simulators is a standard approach for testing and derisking new technologies in several applications. In fact, the proper software implementation of the mathematical model of a system allows evaluating its dynamic behavior in response to various events and the effect of the design choices before having built the real system [26]. This capability is significant when designing a new system because the attained information can partially substitute the field experience in the case of innovative systems. As an example, software simulators are useful to check the correct coordination between control systems and protections, define emergency actions, increase design flexibility, define control system's parameters, support crew training, and so on [54].

However, the usefulness of dynamic modeling during system design directly depends on the model's correct construction and use. Indeed, its scope has to be clearly defined *a priori*, to allow both the application of the suitable mathematical models and the correct interpretation of its outcomes. The hypotheses applied to simplify the mathematical models have to be carefully defined, because they affect the overall results, possibly impairing the tool effectiveness in the case of misuse. As an example, a model for evaluating the system's electromechanical transients is useful for assessing such transients only. Using it to evaluate higher dynamic transients provides results unrelated to reality, eventually leading to a system design unable to perform as intended.

### C. Reasons for Using Dependability Enforcing Techniques and Dynamic Power System Modeling as Design Tools

As above mentioned, dependability theory allows applying a systematic approach to the evaluation and improvement of the system's QoS and safety, providing techniques that are able to objectively assess and compare related attributes. The interest into introducing dependability theory in marine sector arises from the increasing attention given by regulatory bodies and ship owners to safety and QoS topics [15], which is happening also in other transportation systems applications [55], [56]. The dependability theory methodological approach can be used to assess the system's compliancy with safety and QoS requirements, and improve the system. In this regard, the integration of the dependability concepts and techniques in the IPS design process can be obtained with bearable effort, by exploiting an already present ship design substrate [45]. Such an evolutionary direction is already being followed for ships endowed with DP systems [18].

Regarding the dynamic power system modeling, its application to system design is already in study by most advanced IPS's components suppliers, as well as by some ship designers [26]. Moreover, it is relevant to note that hardware-in-the-loop testing on selected shipboard control systems has been proposed for the integration in the IEC 61892-5 [57], thus pushing forward the application of new tools in IPS design.

Given these premises, dependability concepts and techniques and dynamic power system modeling have been selected as the most suitable tools to improve the conventional design process. While these two tools are already being used separately for similar goals, this paper proposes a new approach, capable of integrating both of them in a single design framework maximizing the achievable advantages.

## IV. Dependable Design Process

### A. Goals and Basic Concepts

The goal of this paper is to propose a dependable design process aimed at improving the design of the actual IPSs, as well as allowing the correct design of innovative power systems. Such aims are enabled by the increased level of knowledge achievable through the above-depicted innovative design tools, thus leading to an improvement in design effectiveness and a reduction in costs and risks.

The proposed design process integrates dependability fault-forecasting techniques and power system simulators, as shown in Fig. 3. The circular process depicted in the figure has been conceived specifically for improving the IPS design, but its approach is sufficiently general to be applied to other ship's subsystems. Obviously, in such a case, the specific characteristics and needs of the subsystem to be designed have to be considered. Similarly, designers can choose the ship's design stage in which this process is to be applied, as well as the depth of the analyses to be performed.

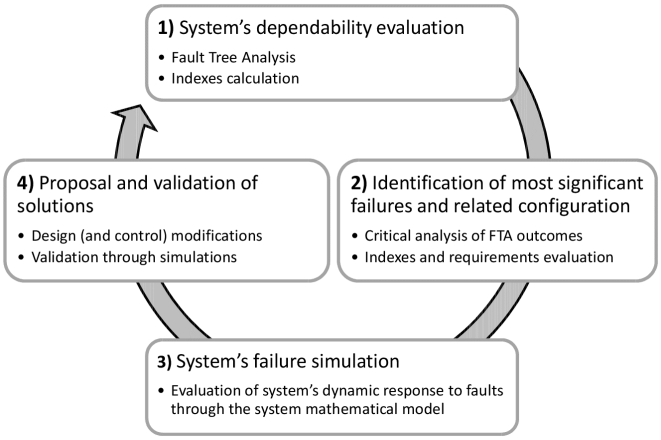


Fig. 3. Proposed dependable design process.

### *B. First Step: System's Dependability Evaluation*

The process starts with the system's dependability evaluation, obtained by means of a fault-forecasting technique.

In this regard, the FTA technique [23], [24] has been selected as the most suited one due to its capability of performing qualitative quantitative analysis [50], [56].

The FTA is a top-down analysis technique that is carried out to assess all the possible combinations of faults events leading to a given TE. The latter is a specific failure event, whose occurrence is considered critical to the system (e.g., the loss of power supply to essential users). For each TE, its immediate causes are defined, thus determining the first layer of events that are related to the TE by Boolean logic. The analysis proceeds by investigating the causes of the events collected in this first layer, building a newer layer on a lower level. The process is iterated until a given level of detail is reached (usually it is a fault in a single component acquired from an external supplier) [13]. The graphical representation of all the fault events, connected each other through logic ports (AND, OR, NOT, and so on), is the so-called failure tree (FT).

The qualitative analysis performed by the FTA leads to results that are similar to the ones achieved by means of an FMEA. However, the FTA is focused on finding all the combinations of faults that can lead to a specific failure (i.e., the TE), while the FMEA is aimed at assessing the causes and effects of single components faults on the system. In addition, the FTA results are graphically represented through the FT, which is easier to comprehend with respect to the documents collection produced by the FMEA. Conversely, the FMEA provides a deeper and wider analysis of the single faults. In addition to FTA and FMEA, many different fault-forecasting techniques are present in literature, thus making it possible for the designers to choose the most suited one depending on their specific goals.

Regarding quantitative analysis, some discussion is needed. In particular, the FTA allows performing easily such an analysis, because the cause–effect relationships depicted by the FT through Boolean logic gates can be expressed by means of mathematical relations. Thus, appropriate indexes can be calculated based on input failure data about the system's components. The main issue related to quantitative analysis techniques is their reliance on components' failure data. The latter needs reliable and coherent historical/statistical assessments on the system components to be determined. Indeed, obtaining accurate failure data has a significant cost, both in terms of time and resources needed, due to the need of performing measurement campaigns on a high number of components in controlled or well-known conditions. In this regard, several databases are present for components used in land applications, while the data about marine systems are scarce. The cause of the latter may be due to different issues. First, the ships are produced in small series, tailored on the owner needs, and sister ships frequently have modifications to some extent. Due to that, it is difficult to provide a sufficiently high number of equal components, used in the same conditions. Second, ship owners are reluctant to disclose information about onboard faults, for easily understandable reasons. Hopefully, a change in this regard will eventually happen, leading to great benefits for all the stakeholders.

Regarding specific failure data, the most used probabilistic indexes are the following, whose definitions are taken from the IEEE Std.493-2007 [58].

1) Failure Rate ($\lambda$): The mean number of failures of a component and/or system per unit exposure time.
2) MTBF: The mean exposure time between consecutive failures of a (repairable) component. It is an index equivalent to failure rate ($\lambda = 1/\text{MTBF}$).
3) MTTF: The mean exposure time between consecutive repairs (or installations) of a component and the next failure of that component. MTTF is commonly found for nonrepairable items.
4) MTTR: The mean time to replace or repair a failed component. Logistic times associated with the repair, such as part acquisitions and crew mobilization, are not included.

Among the several indexes that can be calculated by means of quantitative analysis, the following are to be highlighted.

1) FF: It is the number of failures per unit of time measurement.
2) FV importance: It is an index indicating the contribution of a single fault event to the overall system's dependability ($0 \leq \text{FV} \leq 1$).
3) BB: It is an index measuring the sensitivity of the system's dependability with respect to a change in a single component's data ($0 \leq \text{BB} \leq 1$).

These indexes can provide information aimed at improving the design. In fact, a high FF points out the components and subsystems that most likely will fail during the system's lifetime. On the contrary, FV highlights the impact of a single component or subsystem on the overall system dependability, therefore allowing to find the ones presenting dependability attributes with the highest effect on the system. Concerning the BB index, it evaluates the defense given by the system architecture with respect to a component or subsystem fault, making it possible to evaluate if the actual design is capable of compensating the loss of the component or subsystem in the study. The combination of FV and BB values allows

TABLE I
DETERMINATION OF POSSIBLE SYSTEM IMPROVEMENTS THROUGH FV AND BB EVALUATION [59]

| FV | BB | Possible System Improvements |
|---|---|---|
| High | High | Enhance component/subsystem dependability attributes or system architecture |
| High | Low | Enhance component/subsystem dependability attributes |
| Low | High | Avoid component/subsystem dependability attributes degradation over time |
| Low | Low | Weaken component/subsystem dependability attributes or system architecture |

pinpointing components and subsystems that need to be redesigned or upgraded, as shown in Table I [59].

Finally, during the first step of the proposed design process, an FTA has to be performed, building the FT (qualitative analysis), and suitable mathematical indexes are to be evaluated (quantitative analysis).

### C. Second Step: Identification of Most Significant Failures and Related System Configuration

This step is dedicated to the critical examination of the dependability analysis outcomes. The aim is the definition of both the components/subsystems on which the designer attention has to be focused and the specific combinations of faults to be evaluated by means of the dynamic system's simulations. By evaluating the FF, FV, and BB indexes, the components/subsystems most likely to fault can be identified (i.e., the ones with high FF), as well as their impact on the system's dependability. The enhancement opportunities for the system are assessed by comparing FV and BB, making it possible to focus the analysis on the most significant components in terms of overall system improvement. Thus, off-the-cuff interventions can be avoided, lowering the risk of proposing modifications leading to an increase in system complexity and costs with a possibly reduced effect. Concerning the dynamic simulations, the ones to be performed (and the related input data) can be defined by analyzing the system's FT, considering only the above-defined "most significant" elements. The aim is the determination of the system state before the failure and the set of faults to be applied. Then, the postfailure state is to be evaluated through the use of the dynamic model of the system, performed in the next step. Being simulations a time-consuming activity, an accurate selection among the failures to be analyzed is needed. If a complete dependability analysis is available (considering a wide range of TEs), the sum of all the most significant identified fault combinations is the set to be simulated. Otherwise, if a complete analysis is infeasible due to resources constrains, a reasoning activity by the analyst is needed. The latter process is more qualitative than quantitative and can be done with an approach similar to an FMEA.

### D. Third Step: System's Failure Simulation

In this step, the simulation of the system's dynamic transients for each relevant failure mode is to be performed, by using a mathematical model built accordingly and run in a proper software (i.e., the simulator). This step is useful for the designer because a failure in an electric power system is not a static event, but it is a dynamic one. Indeed, the failure starts from a steady-state equilibrium point before the fault (or faults). The latter event causes either a change in the system state variables, a change in system's configuration (i.e., a change in states' number and/or in their mathematical relationship), or both. After the initial fault perturbation, the system may or may not evolve toward a new stable steady-state condition. In the latter case, system failure is evident. In the former case, three subcases can occur.

1) The system reaches a stable equilibrium point that is not acceptable (output variables out of requirements range).
2) The system reaches a stable acceptable equilibrium point, but one or more of its output variables and/or states exceed their allowed transient limits.
3) The system reaches a stable and acceptable equilibrium point, without exceeding any transient limit for its output variables and states.

All cases except 3) are to be considered as the system's failures.

With regard to power system design, particular attention is to be given to the effects of frequency and voltage controls and their related components. Moreover, additional parameters are significant, such as the size and number of generators, the power system architecture, and so on. Thus, the mathematical model must consider the power system as a single complex entity, using proper models for its components and correctly addressing the relevant interrelations among them. The model detail level must be chosen carefully, to allow evaluating all the relevant dynamic transients for the system in design, at the same time lowering as much as possible simulation times. In this regard, during the IPS design, different models can be used, depending on the scope of the specific activity and on the progress of the IPS design process.

### E. Fourth Step: Proposal and Validation of Solutions

At this point, the evaluation of all the previous steps' outcomes is to be performed, aimed at conceiving corrective solutions for either lowering the likelihood of occurrence of the analyzed TEs or interrupting the event chain that leads to the failure starting from the component faults. All the design modifications have to be validated through a simulation run to demonstrate their ability to solve the identified issue. Since more than one solution can result from the process, each has to be analyzed separately and the results have to be saved for the following studies. It is relevant to highlight that the proposed design modifications have to limit as much as possible their impact on the other functions of the ship, possibly avoiding to impair their operation. Preventing such an undesirable event is not a simple task, given the presence of several interactions among the onboard systems (e.g., fuel systems, cooling, and so on). Moreover, each modification has a cost that must be assessed at this step to properly compare all its pros and cons.

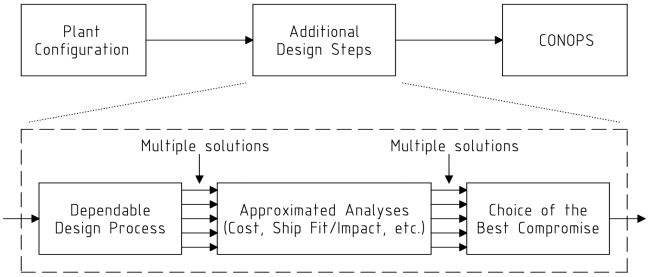


Fig. 4. Dependable design process, integration in conventional design process.

### *F. Return to First Step: Dependability Evaluation of the New Designs*

The circular process of Fig. 3 then returns to the first step, which is the assessment of the dependability attributes for the modified designs. The information developed throughout all the steps makes it possible to compare the modified design proposals. In such a way, it is possible to define the best one (or the set of the better ones) to be evaluated further in the IPS design process. To do that, the modifications leading to the lesser improvement or even to a reduction in system dependability attributes have to be discarded.

### *G. Integration Into the IPS Design Process*

As abovementioned, the goal of the approach proposed in this paper is the improvement of the conventional IPS design process (Fig. 2). To this aim, the dependable design process of Fig. 3 has to be integrated into the IPS design spiral as a subprocess. Referring to Fig. 2, the most suitable point in which performing the new process is right after the Plant Configuration step [Fig. 4 (top)]. In such a way, the information required to perform Fig. 3 design steps is available, and its outcomes can be used before time-consuming steps are made (e.g., Power Quality or Manning analyses). Moreover, the following IPS design steps can be used to compare the impact on the whole ship of multiple design solutions, if similar performance indexes result from the dependability analysis. If a detailed study for each modified design is deemed too resource-intensive, an approximated evaluation can be done. The latter makes it possible to highlight the pros and cons of each solution with respect to the overall ship design, thus allowing the selection of the best compromise [Fig. 4 (bottom)].

The integration of the proposed dependable design process into the conventional one allows finding nonevident issues in the IPS design and to advise suitable solutions, by considering the impact on the overall ship design. The application of Fig. 3 process during an advanced stage of the ship design (i.e., after having already performed some rounds of the conventional process) guarantees the most amount of input information. Thus, an in-depth analysis can be performed, at the price of limiting the range of feasible modifications applicable to solve the criticalities. On the contrary, by performing the process during the ship's early-stage design, the main design choices can be analyzed at the price of significant approximations because of the lack of data [36].

It is relevant to note that the application of the proposed process in the first design stages of the IPS can lead to significant advantages despite the low level of achievable accuracy with respect to its application during final design stages. In fact, during early-stage design, the architecture of the IPS and its main components are defined for the first time. Since changing these parameters in later design stages has a significant cost, their correct definition at the beginning of the design is capital.

The proposed process lowers the risk related to the need for changing these parameters on later design stages, by allowing the designers to make their choice based on an increased amount of knowledge. Conversely, in later design stages, it is possible to update both the dependability analysis and the simulations, exploiting the additional data developed during the IPS design. Therefore, the periodic iteration of the proposed process allows exploiting at best the capabilities of both dependability techniques and dynamic simulations.

A specific point can be made regarding dynamic simulations. In later design stages, new models can be used, to consider new information and evaluate more indexes and figures of merit (even nonelectrical ones, like fuel consumption, noise, and cooling requirements). The resulting data can be useful for all the ship designers, widening the information pool available for defining the final design. Finally, the integration of the proposed process in the ship design allows determining the impact of the IPS design choices on the ship's KPI, thanks to the additional evaluation steps (refer to Fig. 4).

## V. Application Example

### *A. Case Study and Goals Definition*

To test the applicability of the proposed dependable design process, a case study has been analyzed. In particular, the process in Fig. 3 has been tested on the IPS of an all-electric drillship, endowed with a DP system. The general IPS arrangement is shown in Fig. 5, while the one-line diagram of a single section is shown in Fig. 6. Three identical power system sections, powered by a total of six DGs, are installed in the ship's three MVZs. Proper cable ties interconnect the three sections at different voltage levels, to provide power supply to the loads in the case of faults on the main SWBDs. Such a complex power system architecture is needed to assure the compliancy with the highest level of DP classification notation (e.g., DPS-3 for American Bureau of Shipping [20]). To demonstrate the feasibility of the proposed approach, a single round of the process in Fig. 3 has been performed, with a limited level of detail. Specifically, the following elementary components have been considered: DG controls (AVRs and SGs), DG machines (including both the diesel prime mover and the alternator in a single element), circuit breakers, SWBDs, and transformers. It is clear that such a low level of detail cannot accurately represent the built system. However, such a detail level can be useful for defining the IPS during the early design stages. Indeed, at such a time, designers have to select the generators' number and size,

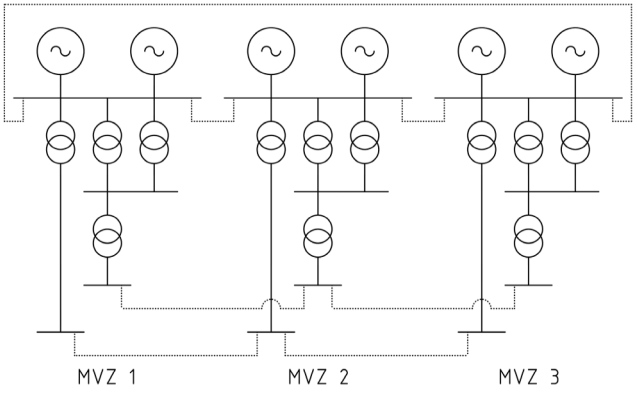


Fig. 5. Case Study: general IPS arrangement, three MVZs.

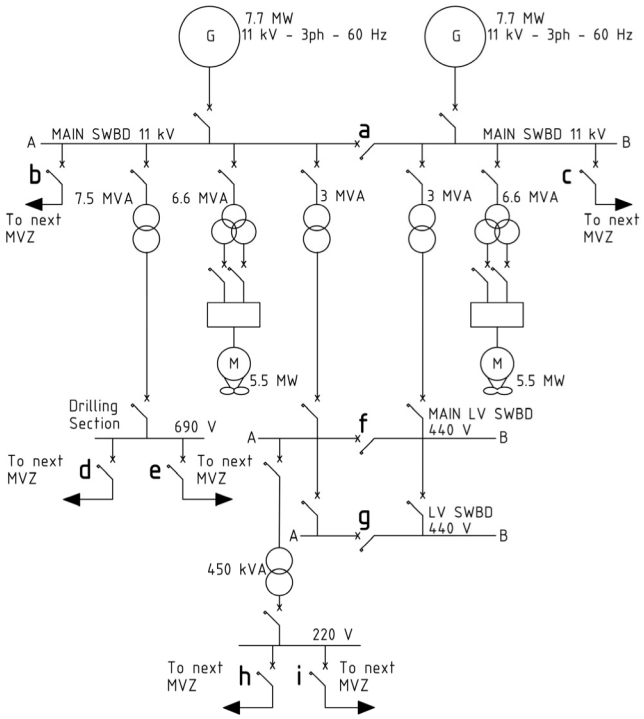


Fig. 6. Case Study: single line diagram of one MVZ IPS section.

and the size and architecture of main IPS elements (e.g., the propulsion system), and perform the calculation of the first approximated electric load balance. Such activities are made on the basis of standard requirements (both from regulations and owner) and designers' knowledge base.

Conversely, information that is more detailed is developed in later design stages (e.g., cable sizing, short-circuit calculations, and so on), requiring the periodic update and rerun of the process in Fig. 3. This update may also include new models and detailed analyses, depending on the designers' needs (e.g., sea state, mission requirements, new control algorithms, and so on). It has to be noted that the limited level of detail here used can be considered as representative of what a designer can achieve during the early-stage design, when the main IPS's characteristics are defined. Moreover, such a limited level of detail allows focusing on testing the dependable design process

TABLE II
DEPENDABILITY ANALYSIS, FAILURE DATA

| Fault event | Description | Failure rate [faults/y] | MTTR [h] |
|---|---|---|---|
| DG controls | Fault in AVR or SG | 0,03627 | 74,77 |
| DG machine | Diesel engine generator fault, 750 kW to 7 MW, continuous use | 1,81573 | 25,08 |
| LV circuit breaker, NC | Fault in LV circuit breaker, Drawout type, > 600 A, normally closed | 0,00185 | 4 |
| LV circuit breaker, NO | Fault in LV circuit breaker Drawout type, > 600A, normally open | 0,00553 | 4 |
| MV circuit breaker | Vacuum circuit breaker fault, Draw out, >600 A, normally closed | 0,02352 | 8 |
| LV Switchboard | LV SWBD fault, <600V, bare bus, circuit breakers not included | 0,00949 | 8 |
| MV Switchboard | MV SWBD fault >5kV, bare bus, circuit breakers not included | 0,01794 | 10 |
| MV/LV trs. | Fault in MV/LV transformer dry type 3MVA | 0,00061 | 8 |
| LV/LV trs. | Fault in LV/LV transformer, dry type <=500kVA | 0,00061 | 4 |

capabilities, rather than aiming to an in-depth analysis of the specific case study IPS. In this regard, the application example has been conceived to highlight some well-known issues and to validate a well-known solution, hence demonstrating the effectiveness of the proposed approach. In particular, the IPS is designed and operated in such a way to purposely generate a power supply issue in a given set of conditions. This is achieved by removing the load shedding function from the control systems, and by running the minimum number of generators required to supply the loads. In this perspective, obtaining well-known solutions through the process is the demonstration of its ability to develop information that is consistent and reliable, which is the scope of the application example.

### *B. First Step: System's Dependability Evaluation*

To perform the FTA of the case study IPS, a dedicated software has been used. The software allows building the FT through an easy to use graphical interface, and then automatically evaluates the quantitative indexes on the basis of proper input data for the single events. In particular, the failure data have been taken from the IEEE Std. 493-2007 [58], which addresses land-based power systems. In this regard, the failure rate has been considered acceptable also for marine applications because of the availability of data from the literature in the same order of magnitude [19]. Conversely, MTTR has been modified by using data taken directly from a shipyard. The complete set of failure data used in the example is shown in Table II. By examining the data in the table, it is clear that these indexes have a specific significance in probabilistic terms, but cannot be directly compared with data (and times) that are directly experienced by designers and service

technicians. As an example, the 1.81573 faults/year value for the DG machine does not mean that a DG will fail nearly twice a year. Instead, it means that a DG has an 83.73% probability of being faulted (the so-called "unavailability") at the end of the first year. Similarly, such a figure will reach the 99.93% probability value at the end of the fourth. Likewise, the MTTR values shown in Table II refer to the meantime to replace or repair a failed component, logistic times excluded (as defined in the IEEE Std. 493-2007 [58]). In this regard, it is clear that repairing a faulted transformer will take more than 8 h (value depicted in Table II) if the ship is sailing because the spare part is not available onboard. The real repair time depends on the ship's position, the supply chain, and several other factors that cannot be determined univocally. Moreover, most of the factors may vary several times during the ship's service life. To simplify the determination of the indexes, the standard excludes logistic times in the MTTR definition, thus enabling the comparison among results evaluated in different times, by different analysts, and on different applications. However, logistic times can be considered by means of the MTTM for defining preventive maintenance frequency and duration. The use of dependability rigorous lexicon, as well as the in-depth comprehension of statistical analysis concepts, allows using the proposed theory and techniques correctly, thus enabling the system improvement. Conversely, misused lexicon and/or poor comprehension of these concepts can lead to inconsistent results, or even to harmful consequences.

In order to carry out the FTA, one or more TEs have to be defined, as well as the OCs in which the ship will operate. In this paper, the loss of the capability of supplying all the loads from the loads balance (called "IPS failure") has been chosen as the TE. Concerning the OC, it defines both the IPS configuration (e.g., number of DGs online, breakers conditions, and so on) and the loads to be supplied. Here, the Navigation OC has been used (right column of Table III). The IPS breakers configuration is depicted in the right column of Table IV (refer Fig. 6 to locate the breakers), while a minimum of three DGs is needed to supply the loads in this OC. The FT built during the FTA is shown in Fig. 7. The size of the diagram is significant, despite the low level of details applied during analysis. Thus, it is difficult to appreciate in detail the overall FT on the available paper page size. To allow appreciating the structure of the resulting FT, a magnification of a single section (i.e., the failure of a running DG: the "DG Failure" gate) is shown in Fig. 8. In addition to that, only a selected number of the quantitative results of the FTA are depicted in this paper, given the number of the events analyzed and the Boolean logic gates in the FT. Regarding the TE in the study, the data are shown in the left column of Table V (heading: 3 *DG*). For the indexes that are not specified into the previous sections, refer to [58].

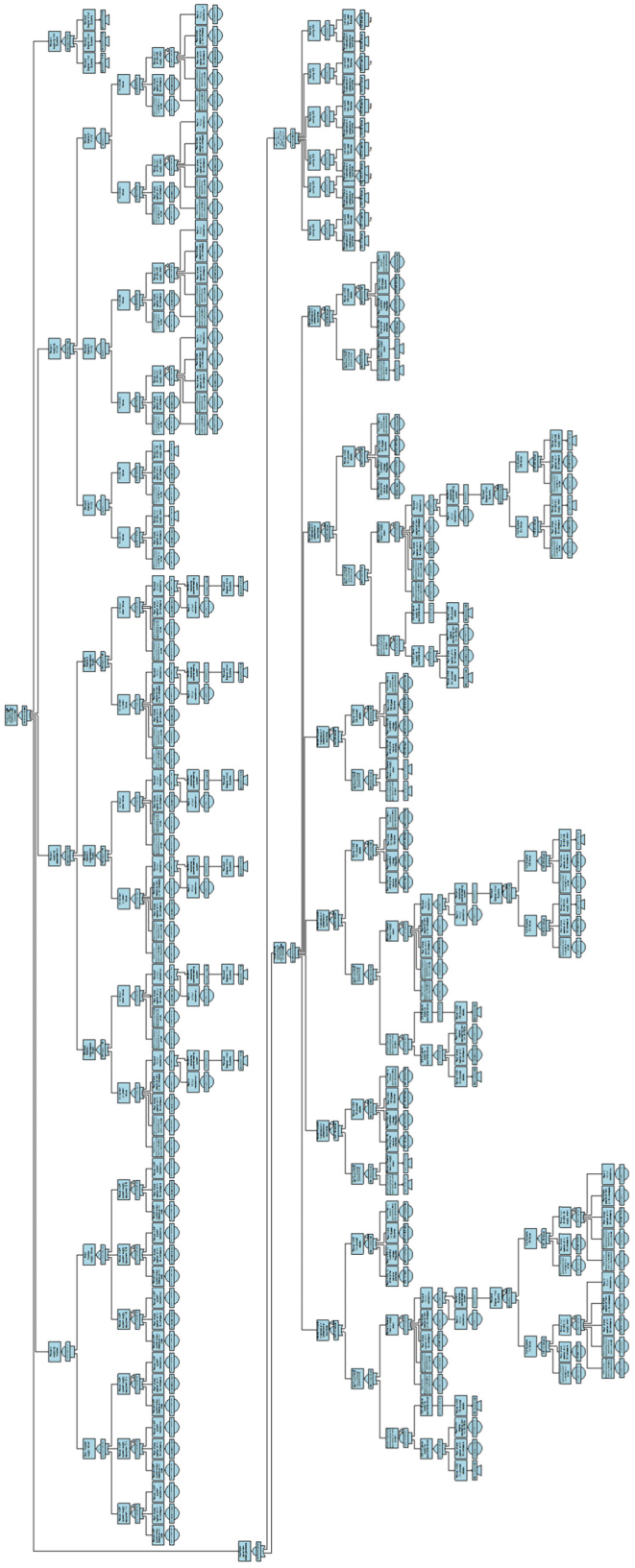

Fig. 7. Case Study FT, "IPS failure" TE in *Navigation* OC.

### *C. Second Step: Identification of Most Significant Failures and Related Configuration*

The critical examination of the FTA outcomes is aimed at identifying possible critical points for the current system design and/or OC. Moreover, it allows defining the dynamic simulations that are needed to assess the fault-to-failure dynamic process. As can be clearly seen from Table V, the case study IPS presents a rather low dependability level regarding the TE in the study. Indeed, circa 6 failures/year is

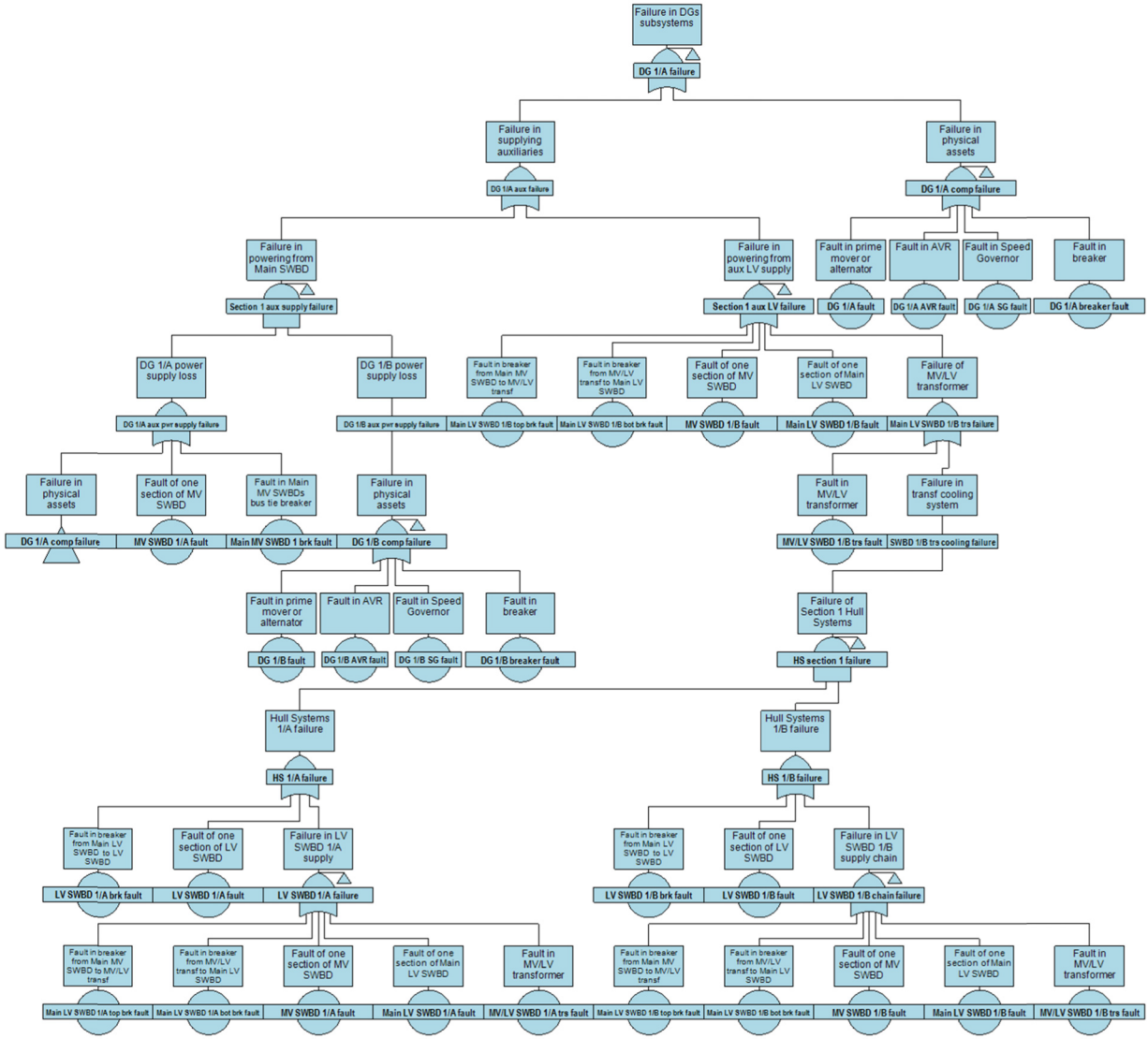


Fig. 8. Magnified FT section: failure of a single DG—"DG failure" gate.

TABLE III
CASE STUDY IPS, ELECTRIC LOADS BALANCE

| Subsystem \ OC | Drilling [kW] | Navigation [kW] |
|---|---|---|
| Thrusters | 17710 | 15890 |
| Drilling systems | 15400 | 0 |
| DG auxiliaries | 450 | 410 |
| Hull Systems | 240 | 210 |
| HVAC | 2440 | 2100 |
| Accommodation | 240 | 240 |
| **Total** | **36480** | **18850** |

TABLE IV
CASE STUDY IPS, BREAKERS CONFIGURATION

| Breakers \ OC | Drilling | Navigation |
|---|---|---|
| **a** | CLOSED (open in emergency) | CLOSED (open in emergency) |
| **b, c** | OPEN | CLOSED |
| **d, e, h, i** | OPEN (closed in emergency) | OPEN (closed in emergency) |
| **f, g** | OPEN | OPEN |

a significantly high FF, thus highlighting the expected issue in the present design. The examination can be deepened by evaluating the indexes calculated for each gate in the FT. In particular, the gate "Insufficient Power" presents a set of indexes that are nearly equal to the TE ones, as can be seen comparing the left columns of Tables V and VI (heading: 3 *DG*). Such a logic gate collects all the fault events that are able to lower the maximum generable power under the amount of power required by the loads. The indexes comparison makes it possible to infer that the "Insufficient Power" event is the main culprit of the low dependability level of the overall IPS. This conclusion is supported by the high levels of the FV and BB importance indexes for the "DG Failure" gate (left

TABLE V
QUANTITATIVE ANALYSIS RESULTS, TE: "IPS FAILURE"

| Index \ System Configuration | 3 DG | 4 DG | L-Shed |
|---|---|---|---|
| Unavailability = (1 - Availability) | 1.77 E-2 | 4.44 E-4 | 2.91 E-4 |
| Failure Frequency [failures/y] | 5.99 E0 | 3.90 E-1 | 2.70 E-1 |
| Expected failures in lifetime (20 years) | 1.20 E2 | 7.80 E0 | 5.41 E0 |
| Total downtime in lifetime (20 years) [y] | 3.53 E-1 | 8.89 E-3 | 5.82 E-3 |

TABLE VI
QUANTITATIVE ANALYSIS RESULTS, "INSUFFICIENT POWER" GATE

| Index \ System Configuration | 3 DG | 4 DG | L-Shed |
|---|---|---|---|
| Unavailability | 1.75 E-2 | 2.57 E-4 | 1.03 E-4 |
| Failure frequency [failures/year] | 5.79 E0 | 1.89 E-1 | 6.87 E-2 |
| Expected failures in lifetime (20 y) | 1.16 E2 | 3.77 E0 | 1.37 E0 |
| Total downtime in lifetime (20 y) [y] | 3.50 E-1 | 5.13 E-3 | 2.06 E-3 |

column of Table VII; Fig. 8), which is one of the subevents causing the "Insufficient Power" event. The resulting high FV value for the "DG failure" gate indicates that such an event has a significant effect on the overall system's attributes in the considered TE. Conversely, the high BB value highlights a design flaw in the case study IPS, which is not able to compensate for the fault presence. By applying the approach depicted in Table I, it is possible to affirm that an improvement in the system design can be achieved by either substituting the DGs with more reliable ones or by modifying the system architecture (which also includes the OCs). Thus, the process starting from the "DG Failure" event (i.e., the loss of a running DG) and leading to the "IPS failure" is the one that has to be dynamically simulated.

### *D. Third Step: System's Failure Simulation*

To evaluate the dynamic evolution of the system main variables following the "DG failure" event, a mathematical model of the IPS has been built in MATLAB Simulink environment, by applying the electromechanical transients simplifying hypothesis. The model includes the six synchronous generators, represented through a sixth-order mathematical model with saturations [60], and PID AVRs and SGs. The DG models incorporate both the excitation system (actuator and rotating exciter model) and a simplified first-order model of the diesel engine prime mover (with an additional fuel injection delay) with proper saturation limits. The ship's power distribution system has been modeled through an admittance matrix, thanks to the electromechanical transient simplification hypothesis, and allows separating and reconnecting (after a synchronization process) the three main MV SWBDs. Finally, the loads models are simple equivalent admittances, directly connected to the SWBDs for the MV loads, and connected through a simplified transformer model (an admittance with

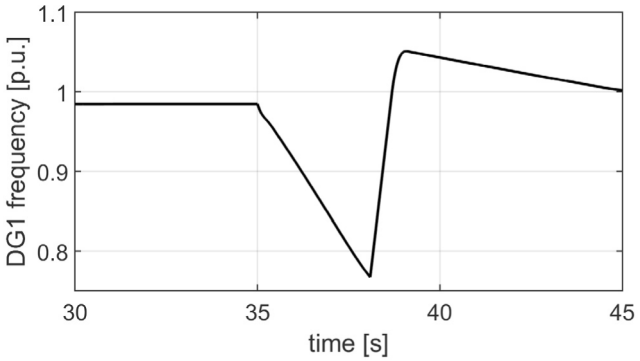


Fig. 9. Frequency of a running generator, 3 DG.

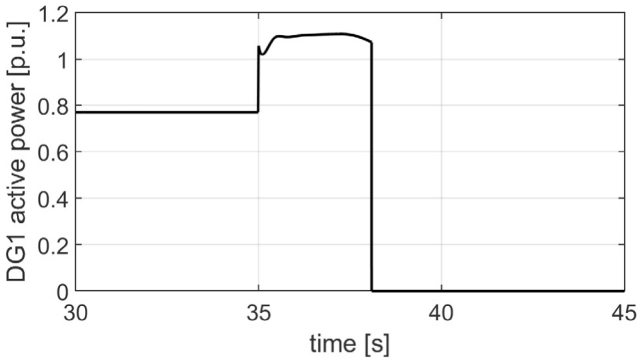


Fig. 10. Power of a running generator, 3 DG.

proper per-unit representation base changes) in the case of the LV loads. The resulting software simulator is based on well proven mathematical models, being it an upgraded and expanded version of a previous simulator built for a naval vessel, whose correct behavior was already validated in [54]. Regarding the case study results, Figs. 9 and 10 show the frequency and active power output of one surviving DG after the disconnection of one running DG at $t = 35$ s. By examining the figures, it is clear that the blackout happening at $t = 37$ s is caused by the overload of the DGs remaining online, which in turn leads to the intervention of the underfrequency protection. Thus, the analysis of the dynamic process leading to the failure points toward the frequency and active power regulation functions. As above mentioned, such a condition has been forced to happen in this case study by removing load-shedding and by running the minimum number of DGs required to supply the loads for the sake of validating the proposed process only.

### *E. Fourth Step: Proposal and Validation of Solutions*

The proposal of design modification to avoid the occurrence of the failure in the study (i.e., the TE) starts from the FV and BB indexes evaluation, carried out in the second step. In particular, the possible improvement actions depicted in Table I are aimed at lowering the likelihood of occurrence of the fault events originating the failure, or at modifying the system design to either prevent the start of the failure dynamic process or to stop it during its evolution. The first

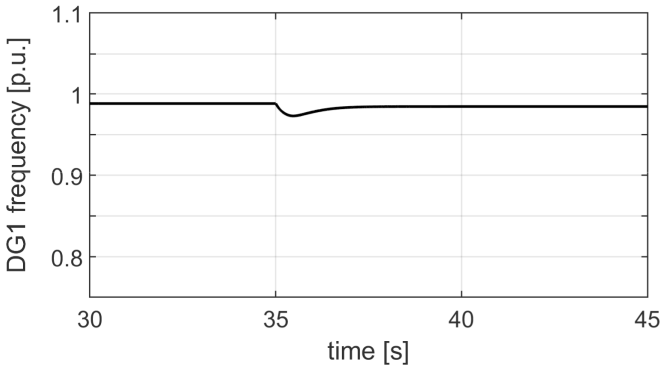


Fig. 11. Frequency of a running generator, 4 DG.

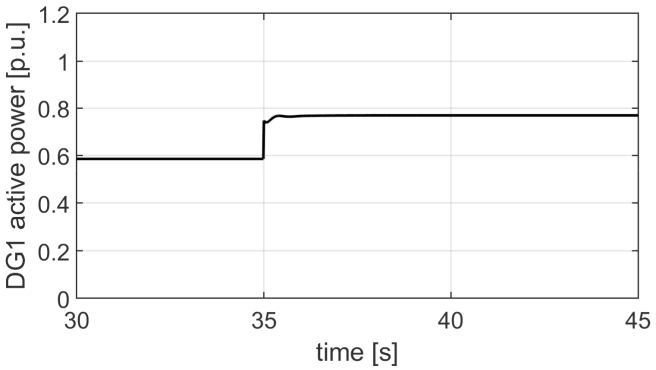


Fig. 12. Power of a running generator, 4 DG.

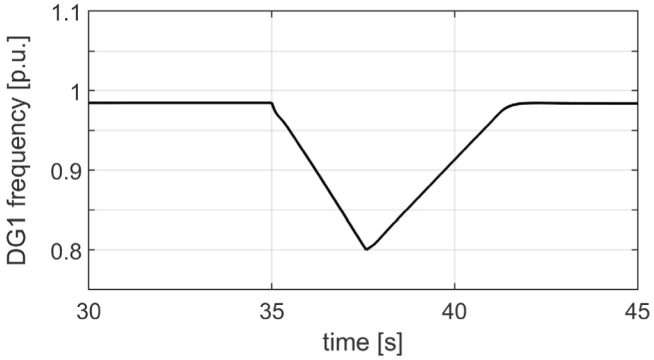


Fig. 13. Frequency of a running generator, L-Shed.

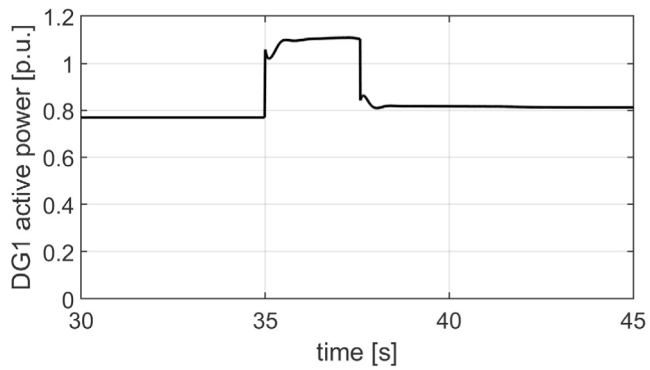


Fig. 14. Power of a running generator, L-Shed.

option is usually the most difficult to carry out, due to the need of deeply intervening onto single components (e.g., generators, control systems, and so on) whose manufacturing is commonly not controlled by the IPS designer. Conversely, the designer can apply the second option by using the information resulting from the previous steps. In this case study, the overload and consequent underfrequency protection intervention can be avoided by either running an additional generator (i.e., the solution called 4 DG) or by implementing a load-shedding algorithm (i.e., the solution called L-Shed). These two solutions act on the dynamic process that leads to the failure and not on the root cause (the fault of one DG), thus representing the implementation of the second possible improvement action mentioned above. Both the solutions are here defined. For the 4 DG solution, one of the shutdown DGs is selected to be powered on, while in the L-Shed one, the loads to be shed are chosen. In particular, in the latter, the shedding algorithm cuts the propulsion power by 25% and the heating, ventilation, and air conditioning (HVAC) power by 75% when system frequency falls below 80% of its rated value. As affirmed in the previous section, the effectiveness of the proposed modifications must be demonstrated through another simulation before proceeding further with the process. The results are shown in Figs. 11 and 12 for the 4 DG solution, and in Figs. 13 and 14 for the L-Shed one. As can be clearly seen from the figures, both solutions allow avoiding the IPS blackout after the loss of one running DG (at $t = 35$ s). However, both the power system variables transient behavior and the final steady-state level of service delivered by the two solutions are different.

TABLE VII
FV AND BB IMPORTANCE INDEXES, "DG FAILURE" GATE

| Index \ System Configuration | 3 DG | 4 DG | L-Shed |
|---|---|---|---|
| Fussell-Vesely Importance | 0.3269 | 0.2294 | 0.2339 |
| Birnbaum Importance | 1 | 0.0176 | 0.0117 |

### *F. Return to the First Step: Dependability Evaluation of the Proposed Solutions*

The final step implies performing a dependability evaluation of the two proposed solutions in order to verify their effectiveness in term of system's dependability attributes. Therefore, two new FTAs have been performed, by using the same TE as before. The quantitative analysis outcomes are shown in the second and third columns of Tables V–VII. The comparison among the dependability indexes makes it possible to appreciate the positive effect of the proposed solutions. In fact, both of them improve the system's dependability to an acceptable level: the FF falls well below 1 failure per year, while both FV and BB indexes are significantly reduced. Such a result was expected, being them the most common solutions applied to solve power system's blackout issues. Having the two solutions passed the dependability improvement test, it is possible to proceed with further evaluations about their overall

impact on the ship (as shown in Fig. 4). As a closing remark, it can be highlighted that the results of the FT gate "Insufficient Power" finally differ from the TE ones. In fact, the two solutions led to a change in the combination of faults causing the "IPS failure" TE, thus making the effect of the former most significant faults comparable with other ones.

### G. Integration Into the Overall Design Process and Remarks

The application of the circular process shown in Fig. 3 to the case study led to two solutions, both able to solve the issue highlighted in steps one and two, and both presenting comparable dependability indexes. Consequently, the IPS design process can proceed further with the conventional approach, with steps aimed at evaluating the solutions' impact overall the ship design to select the best compromise (Fig. 4).

These analyses have not been performed for this case study. Still, some insights about the expected impact on the ship can be given. In particular, L-Shed solution presents better dependability results than 4 DG one, with the additional benefit of avoiding the increase in fuel consumption caused by running another DG. However, it implies shedding HVAC (lesser impact) and propulsion power (major impact), which is viable only in Navigation OC. In fact, in other OCs, it may be required to retain the full propulsion power (e.g., in Drilling OC, the propulsion power needs to be prioritized to avoid harmful consequences), thus limiting the shedding effect to a level that may be insufficient to guarantee frequency stability after a DG fault. As a consequence, the best solution from a dependability point of view in one OC (i.e., Load Shedding in Navigation) may not be the best one in other OCs. Consequently, during Drilling OC, running an additional DG becomes the best solution for the IPS in the study. It is relevant to note that, in all OCs including DP operations, the rules and regulations oblige to separate the main SWBDs of the MVZs if Class 3 equipment is used [20]. This is enforced to remove the possibility of a fault in one section affecting the rest of the IPS. In such a case, the L-Shed solution results not applicable outside of Navigation OC, being the reduction of power not sufficient to avoid a blackout in the single isolated MVZ affected by the fault. Owing to that, running an additional DG in each section is commonly applied in vessels with DP systems, in the relevant OCs. Obviously, with separated IPS sections, the other two MVZs will continue to operate without issues after the considered fault.

Finally, the application example highlighted a well-known issue, which is the possible blackout of the IPS after the loss of one DG. By using the proposed process, two well-known solutions to the blackout issue have been found. In this perspective, the validation of these commonly applied solutions through the proposed process shows that the developed information is consistent and reliable, which was the scope of the case study. Moreover, while these solutions are commonly applied as a standard and have been demonstrated in the past through the field practice, a quantitative evaluation of their real impact on the terms of dependability is rarely assessed. In this regard, the proposed process allowed developing a deeper knowledge about the effect of these solutions on the system in terms of numerical indexes.

## VI. Conclusion

In this paper, a new design process has been presented, integrating quantitative dependability analysis and dynamic power system modeling. The aim of the proposal is to provide designers with a design methodology for addressing the incoming needs in AESs IPSs design area, by means of a circular process divided into sequential steps. The novelty in the approach proposed here is the integration among the two "innovative design tools." Indeed, the dependability attributes of the IPS are assessed through a fault-forecasting technique (quantitative dependability analysis). The results are then used not only to identify critical points (i.e., the so-called "single point of failure") but also to provide data for defining the dynamic system simulations to be run. The latter makes it possible to assess the dynamic process leading to a failure, which starts with the single components faults. Then, corrective solutions can be applied (i.e., design modifications) to either reduce the likelihood of occurrence of the single faults at the root of the failure or to stop the dynamic process leading to the failure. The proposed process applies an iterative approach to evaluate the pros and cons of the proposed design modifications. This is achieved not only in terms of IPS dependability but also in terms of their effect on the ship. The proposed process is useful for designing innovative IPS architectures, by reducing as much as possible the "trial and error" procedure commonly used to find solutions when unforeseen issues arise. Moreover, also well-proven power systems can benefit from the proposed design, thanks to an increased system design optimization.

In order to clarify both how the process is supposed to be applied and which are the activities on which the designers' attention needs to be focused during the process, a simplified application example has been here shown. The case study analysis allowed performing a first validation of the proposed process, by analyzing a design in which a set of common critical flaws were purposely added. In addition to validation, the case study developed additional information about dependability performance levels of the case study IPS.

Finally, it has to be noted that this specific process has been conceived for the IPS design, but its base approach can be applied to all ship subsystems. However, the modification will be needed to consider the specific characteristics of other subsystems and the needs of their designers.

## References


[1] J. F. Hansen and F. Wendt, "History and state of the art in commercial electric ship propulsion, integrated power systems, and future trends," *Proc. IEEE*, vol. 103, no. 12, pp. 2229–2242, Dec. 2015.

[2] A. Vicenzutti, D. Bosich, 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, Jun. 2015.

[3] A. Vicenzutti, D. Bosich, R. Pelaschiar, R. Menis, and G. Sulligoi, "Increasing the safety of modern passenger ships: A comprehensive approach for designing safe shipboard integrated electrical power systems," *IEEE Electrific. Mag.*, vol. 5, no. 3, pp. 40–54, Sep. 2017.

[4] *Guidelines for Vessels With Dynamic Positioning Systems*, document MSC/Circulation 645, International Maritime Organization, Jun. 1994.

[5] E. O. S. Hansen, "DP dependability," in *Proc. MTS Dyn. Positioning Conf.*, Oct. 2011, pp. 11–12.

[6] E. L. Zivi, "Integrated shipboard power and automation control challenge problem," in *Proc. IEEE Power Eng. Soc. Summer Meeting*, vol. 1, Jul. 2002, pp. 325–330.

[7] I. Jackson and I. Milne, "Safety justification of the complex electronic elements used in the power and propulsion control of the queen Elizabeth class aircraft carrier," in *Proc. IMarEST Mar. Elect. Control Syst. Saf. Conf. (MECSS)*, Amsterdam, The Netherlands, Oct. 2013, pp. 1–10.

[8] A. M. Cramer, X. Liu, Y. Zhang, J. D. Stevens, and E. L. Zivi, "Early-stage shipboard power system simulation of operational vignettes for dependability assessment," in *Proc. IEEE Electr. Ship Technol. Symp. (ESTS)*, Alexandria, VA, USA, Jun. 2015, pp. 382–387.

[9] A. Dubey and S. Santoso, "Availability-based distribution circuit design for shipboard power system," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1599–1608, Jul. 2017.

[10] A. Dubey and S. Santoso, "Designing electric distribution circuits for improved system reliability," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Boston, MA, USA, Jul. 2016, pp. 1–5.

[11] A. Dubey, S. Santoso, and A. Arapostathis, "Reliability analysis of three-dimensional shipboard electrical power distribution systems," in *Proc. IEEE Electr. Ship Technol. Symp. (ESTS)*, Alexandria, VA, USA, Jun. 2015, pp. 93–98.

[12] G. Buja, A. da Rin, R. Menis, and G. Sulligoi, "Dependable design assessment of integrated power systems for all electric ships," in *Proc. Elect. Syst. Aircr., Railway Ship Propuls.*, Bologna, Italy, Oct. 2010, pp. 1–8.

[13] R. Menis, A. da Rin, A. Vicenzutti, and G. Sulligoi, "Dependable design of all electric ships integrated power system: Guidelines for system decomposition and analysis," in *Proc. Elect. Syst. Aircr., Railway Ship Propuls.*, Bologna, Italy, Oct. 2012, pp. 1–6.

[14] M. Chiandone, A. da Rin, R. Menis, G. Sulligoi, and A. Vicenzutti, "Dependable oriented design of complex integrated power systems on ships," in *Proc. Int. Conf. Elect. Syst. Aircr., Railway, Ship Propuls. Road Veh. (ESARS)*, Aachen, Germany, Mar. 2015, pp. 1–6.

[15] J. Lampe, E. Rüde, Y. Papadopoulos, and S. Kabir, "Model-based assessment of energy-efficiency, dependability, and cost-effectiveness of waste heat recovery systems onboard ship," *Ocean Eng.*, vol. 157, pp. 234–250, Jun. 2018.

[16] D. F. Phillips, "Classic single point failures of redundant DP systems," in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Oct. 1998, pp. 1–9.

[17] D. E. Wilkes, "Dynamic positioning incidents resulting from inadequate power systems analysis," in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Sep. 2002, pp. 1–11.

[18] R. Cornes and T. R. Stockton, "FMEA as an integral part of vessel design and construction: Producing a fault tolerant DP vessel," in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Oct. 1998, pp. 1–9.

[19] H. Shatto and D. Phillips, "Reliability and risk analysis—Failure modes and effects analysis (FMEAs)," in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Oct. 1997, pp. 1–13.

[20] *Guide for Dynamic Positioning Systems*, Amer. Bureau Shipping, Houston, TX, USA, Jul. 2014.

[21] D. Phillips, B. Haycock, and S. Cargill, "FMEA failed to meet expectations again (again)?" in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Oct. 2010, pp. 1–17.

[22] R. Eriksen, J. Harms, and R. McDonnell, "Assessing the reliability of dynamic positioning systems for deepwater drilling vessels," in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Oct. 1999, pp. 1–12.

[23] S. Kabir, "An overview of fault tree analysis and its application in model based dependability analysis," *Expert Syst. Appl.*, vol. 77, pp. 114–135, Jul. 2017.

[24] *Fault Tree Analysis (FTA)*, Standard IEC 61025, Dec. 2006.

[25] A. Boveri, F. D'Agostino, A. Fidigatti, E. Ragaini, and F. Silvestro, "Dynamic modeling of a supply vessel power system for DP3 protection system," *IEEE Trans. Transp. Electrific.*, vol. 2, no. 4, pp. 570–579, Dec. 2016.

[26] T. Lauvdal, "Optimizing and evaluating the performance of power and thruster plant in DP vessels with an integrated vessel simulator," in *Proc. MTS Dyn. Positioning Conf.*, Houston, TX, USA, Oct. 2000, pp. 1–7.

[27] A. Vicenzutti, R. Menis, and G. Sulligoi, "Dependable design of all electric ships integrated power system: New design process," in *Proc. Int. Conf. Elect. Syst. Aircr., Railway, Ship Propuls. Road Veh. Int. Transp. Electrific. Conf. (ESARS-ITEC)*, Toulouse, 2016, pp. 1–6.

[28] V. Bucci, A. Marinò, and I. Juricic, "Integrated ship design: Automated generation of production deliverables with new generation shipbuilding CAD systems," in *Proc. 12th Int. Conf. Comput. Appl. Maritime Ind.*, Hamburg, Germany, Apr. 2013, pp. 15–17.

[29] J. Chalfant, "Early-stage design for electric ship," *Proc. IEEE*, vol. 103, no. 12, pp. 2252–2266, Dec. 2015.

[30] T. McCoy, "Integrated power systems—An outline of requirements and functionalities for ships," *Proc. IEEE*, vol. 103, no. 12, pp. 2276–2284, Dec. 2015.

[31] J. Neely, L. Rashkin, M. Cook, D. Wilson, and S. Glover, "Evaluation of power flow control for an all-electric warship power system with pulsed load applications," in *Proc. IEEE Appl. Power Electron. Conf. Expo. (APEC)*, Long Beach, CA, USA, Mar. 2016, pp. 3537–3544.

[32] R. E. Hebner *et al.*, "Dynamic load and storage integration," *Proc. IEEE*, vol. 103, no. 12, pp. 2344–2354, Dec. 2015.

[33] M. Baret *et al.*, "Amerigo vespucci: Retrofitting of propulsion and generation systems on the italian training's tall ship," in *Proc. Int. Symp. Power Electron., Elect. Drives, Automat. Motion*, Jun. 2014, pp. 319–326.

[34] *IEEE Recommended Practice for 1 kV to 35 kV Medium-Voltage DC Power Systems on Ships*, IEEE Stdandard 1709-2010, 2010.

[35] G. Sulligoi, A. Vicenzutti, V. Arcidiacono, and Y. Khersonsky, "Voltage stability in large marine-integrated electrical and electronic power systems," *IEEE Trans. Ind. Appl.*, vol. 52, no. 4, pp. 3584–3594, Jul/Aug. 2016.

[36] G. Sulligoi, A. Vicenzutti, and R. Menis, "All-electric ship design: From electrical propulsion to integrated electrical and electronic power systems," *IEEE Trans. Transport. Electrific.*, vol. 2, no. 4, pp. 507–521, Dec. 2016.

[37] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 1, pp. 11–33, Jan./Mar. 2004.

[38] A. Avižienis, "Document faults: An extension of the taxonomy of dependable and secure computing," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Denver, CO, USA, Jun. 2017, pp. 113–114.

[39] V. Basili, P. Donzelli, and S. Asgari, "A unified model of dependability: Capturing dependability in context," *IEEE Softw.*, vol. 21, no. 6, pp. 19–25, Nov. 2004.

[40] W. Zamojski and D. Caban, "Introduction to the dependability modeling of computer systems," in *Proc. Int. Conf. Dependable Comput. Syst.*, Szklarska Poreba, Poland, May 2006, pp. 100–109.

[41] L. Bukowski, "System of systems dependability–Theoretical models and applications examples," *Rel. Eng. Syst. Saf.*, vol. 151, pp. 76–92, Jul. 2016.

[42] R. K. Kaur, B. Pandey, and L. K. Singh, "Dependability analysis of safety critical systems: Issues and challenges," *Ann. Nucl. Energy*, vol. 120, pp. 127–154, Oct. 2018.

[43] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 106–124, 2nd Quart., 2009.

[44] A. Wakankar, A. Kabra, A. K. Bhattacharjee, and G. Karmakar, "Architectural model driven dependability analysis of computer based safety system in nuclear power plant," *Nucl. Eng. Technol.*, vol. 51, no. 2, pp. 463–478, 2018.

[45] R. Menis, A. da Rin, G. Sulligoi, and A. Vicenzutti, "All electric ships dependable design: Implications on project management," in *Proc. AEIT Annu. Conf.-Res. Ind., Need More Effective Technol. Transf. (AEIT)*, Trieste, Italy, Sep. 2014, pp. 1–6.

[46] E. Schnieder, L. Schnieder, and J. R. Müller, "Conceptual foundation of dependable systems modelling," *IFAC Proc. Volumes*, vol. 42, no. 5, pp. 198–202, 2009.

[47] M. D. Quilici, "DP system reliability-quantitative vs. qualitative analysis," in *Proc. MTS Dyn. Positioning Conf.*, Oct. 1999, pp. 12–13.

[48] *Guidance on Failure Modes & Effects Analyses (FMEAs)*, IMCA, London, U.K., Apr. 2002.

[49] R. Y. Rubinstein and S. P. Kroese, *Simulation and the Monte Carlo Method*, 3rd ed. Hoboken, NJ, USA: Wiley, 2017.

[50] W. S. Lee, D. L. Grosh, F. A. Tillman, and C. H. Lie, "Fault tree analysis, methods, and applications—A review," *IEEE Trans. Rel.*, vol. R-34, no. 3, pp. 194–203, Aug. 1985.

[51] Y.-Y. Hong, L.-H. Lee, and H.-H. Cheng, "Reliability assessment of protection system for switchyard using fault-tree analysis," in *Proc. Int. Conf. Power Syst. Technol.*, Chongqing, China, Oct. 2006, pp. 1–8.

[52] C. Dong, C. Yuan, Z. Liu, and X. Yan, "Marine propulsion system reliability research based on fault tree analysis," *Adv. Shipping Ocean Eng.*, vol. 2, no. 1, pp. 27–33, Mar. 2013.
[53] A. M. Yasa and H. Akyildiz, "Formal safety assessment of offshore support vessels," in *Proc. GiDB|DERGi*, vol. 6, 2016, pp. 34–49.
[54] G. Sulligoi, D. Bosich, A. Vicenzutti, L. Piva, G. Lipardi, and T. Mazzuca, "Studies of electromechanical transients in FREMM frigates integrated power system using a time-domain simulator," in *Proc. IEEE Electr. Ship Technol. Symp. (ESTS)*, Arlington, VA, USA, Apr. 2013, pp. 429–433.
[55] H. Song and E. Schnieder, "Evaluating fault tree by means of colored Petri nets to analyze the railway system dependability," *Saf. Sci.*, vol. 110, pp. 313–323, Dec. 2018.
[56] A. Abdulkhaleq *et al.*, "A systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles," *Procedia Eng.*, vol. 179, pp. 41–51, Jan. 2017.
[57] *Mobile and Fixed Offshore Units—Electrical Installations—Part 5: Mobile Units*, Standard IEC 61892-5, 2010.
[58] *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, IEEE Stdandard 493-2007, Jun. 2007.
[59] M. van der Borst and H. Schoonakker, "An overview of PSA importance measures," *Rel. Eng. Syst. Saf.*, vol. 72, no. 3, pp. 241–245, 2001.
[60] R. Marconato, *Electric Power Systems*, vol. 1. Chennai, Tamil Nadu: CEI, 2004.

**A. Vicenzutti** (M'13) received the M.Sc. degree (Hons.) in electrical engineering from the University of Trieste, Trieste, Italy, in 2012, and the Ph.D. degree in industrial engineering from the University of Padova, Padua, Italy, in 2016.

He is currently an Assistant Professor with the University of Trieste, where he is involved in design and dependability of power systems, concerning both land and transportation applications at the Electric Power Generation and Control Laboratory (EPGC Lab), Department of Engineering and Architecture (DIA), University of Trieste.

Dr. Vicenzutti is an IEEE Member, registered with IAS and PES societies.

**R. Menis** (M'92) is currently an Associate Professor of electric drives with the Department of Engineering and Architecture, University of Trieste, Trieste, Italy, where he is also the Head of the Electric Drives Laboratory. His current research interests include the field of the electrical machines and drives: modeling, identification, and control of ac and dc machines; industry and transport applications of the electrical drives; and dependability and functional safety applied to the electrical systems for transportations (automotive and naval areas).

**G. Sulligoi** (M'87–SM'02) received the M.Sc. degree (*summa cum laude*) in electrical engineering from the University of Trieste, Trieste, Italy, in 2001, and the Ph.D. degree in electrical engineering from the University of Padua, Padua, Italy, in 2005.

In 2007, he joined the University of Trieste, where he is currently an Associate Professor of electric power generation and control and appointed as an Associate Professor of shipboard electrical power systems. He is also the Founder and the Director of the Grid Connected & Marine Electric Power Generation and Control Laboratory (EPGC Lab), Department of Engineering and Architecture, University of Trieste. He has authored more than 100 scientific papers in the fields of shipboard power systems, all-electric ships, generators modeling, and voltage control, where he also has received some scientific awards.

Dr. Sulligoi received the national qualification for the level of Full Professor in electrical energy engineering. He is the Deputy Rector for Community Affairs and Business Relations of the University of Trieste.