UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Sede Consorziata: Univeristà degli Studi di Trieste

Dipartimento di Ingegneria ed Architettura (DIA)

SCUOLA DI DOTTORATO DI RICERCA IN: Ingegneria Industriale
INDIRIZZO: Ingegneria dell'Energia
CICLO: XXVIII

INNOVATIVE INTEGRATED POWER SYSTEMS FOR ALL ELECTRIC SHIPS

Direttore della Scuola: Ch.mo Prof. Paolo Colombo

Coordinatore d'indirizzo: Ch.ma Prof.ssa Luisa Rossetto

Supervisore: Ch.mo Prof. Giorgio Sulligoi

Dottorando: Andrea Vicenzutti

If it can’t be expressed in figures, it is not science;

It is opinion.

Robert Heinlein

Abstract

Sommario

Oggigiorno, nelle grandi navi la propulsione elettrica è una valida alternativa a quella meccanica. Infatti, attualmente quest'ultima è limitata solo alle navi con requisiti particolari, quali la necessità di una elevata velocità di crociera o l'uso di combustibili specifici. L'uso della propulsione elettrica, in coppia con la progressiva elettrificazione dei carichi di bordo, ha portato alla nascita del concetto di All Electric Ship (AES). Una AES è una nave in cui tutti i carichi di bordo (propulsione inclusa) sono alimentati da un unico sistema elettrico, chiamato Sistema Elettrico Integrato (Integrated Power System - IPS). L'IPS è un sistema chiave in una AES, per cui richiede una progettazione ed una gestione accurata. In effetti, in una AES tale sistema alimenta quasi tutto, mettendo in evidenza il problema di garantire sia la corretta Power Quality, sia la continuità del servizio. La progettazione di un sistema così complesso viene convenzionalmente fatta considerando i singoli componenti separatamente, per semplificare il processo. Tuttavia tale pratica può portare a prestazioni ridotte, problemi di integrazione e sovradimensionamento. Come se non bastasse, la procedura di progettazione separata influisce pesantemente sull'affidabilità del sistema, a causa della difficoltà nel valutare l'effetto sulla nave di un guasto in un singolo sottosistema. Per questi motivi è necessario un nuovo processo di progettazione in grado di considerare l'effetto di tutti i componenti e sottosistemi del sistema, consentendo così di migliorare i più importanti driver applicati nella progettazione di una nave: efficienza, efficacia, affidabilità e riduzione dei costi.

Date queste premesse, l'obiettivo della ricerca era di ottenere una nuova metodologia di progettazione applicabile al sistema elettrico integrato delle AES, in grado di considerare il sistema nel suo insieme, comprese tutte le sue interdipendenze interne. Il risultato di tale ricerca è descritto in questo lavoro di tesi, e consiste in un sub-processo che dovrà essere integrato nel processo di progettazione convenzionale del sistema elettrico integrato.

In questa tesi viene effettuata un'ampia rassegna dello stato dell'arte, per consentire la comprensione del contesto, del perché tale processo innovativo è necessario e quali tecniche innovative possono essere utilizzate come un aiuto nella progettazione. Ogni punto è discusso concentrandosi sullo scopo di questa tesi, presentando così argomenti, bibliografia, e valutazioni personali volte ad indirizzare il lettore a comprendere l'impatto del processo di progettazione proposto.

In particolare, dopo un primo capitolo dedicato all'introduzione delle AES in cui sono descritte come tali navi si sono evolute e quali sono le applicazioni più impattanti, si effettua una discussione ragionata sul processo di progettazione convenzionale delle navi, contenuta nel secondo capitolo. In aggiunta a questo viene effettuata un'analisi approfondita del processi di

progettazione dell’IPS, per spiegare il contesto in cui il processo di progettazione innovativo deve essere integrato. Alcuni esempi di problemi derivanti dal processo di progettazione tradizionale sono dati, per motivare la proposta di un processo nuovo. In aggiunta ai problemi dovuti alla progettazione, altre motivazioni portano alla necessità di un rinnovato processo di progettazione, quali l'imminente introduzione di sistemi di distribuzione innovativi a bordo nave e la recente comparsa di nuovi requisiti il cui impatto sull’IPS è significativo. Per questo, un excursus su questi due temi è fatto nel terzo capitolo, con riferimento alle più recenti fonti letterarie e ricerche.

Il quarto capitolo è dedicato alla descrizione degli strumenti che verranno utilizzati per costruire l'innovativo processo di progettazione. La prima parte del capitolo è dedicata alla teoria della fidatezza (dependability), in grado di dare un approccio sistematico e coerente alla determinazione degli effetti guasti sui sistemi complessi. Attraverso la teoria della fidatezza e le sue tecniche è possibile: determinare l'effetto sul sistema dei guasti ai singoli componenti; valutare tutte le possibili cause di un dato evento di avaria; valutare alcuni indici matematici relativi al sistema, al fine di confrontare diverse soluzioni progettuali; definire dove e come il progettista deve intervenire per migliorare il sistema. La seconda parte del quarto capitolo è dedicata ai software per la simulazione del comportamento dell’IPS ed ai test hardware-in-the-loop. In particolare viene discusso l'uso di tali sistemi come aiuto nella progettazione di sistemi di potenza, per permettere di comprendere perché tali strumenti sono stati integrati nel processo di progettazione sviluppato.

Il quinto capitolo è dedicato al processo di progettazione sviluppato nel corso della ricerca. Viene discusso come tale processo funziona, come dovrebbe essere integrato nel processo di progettazione convenzionale, e qual è l'impatto che esso ha sulla progettazione. In particolare, la procedura sviluppata implica sia l'applicazione delle tecniche proprie della teoria della fidatezza (in particolare la Failure Tree Analysis), sia la simulazione del comportamento dinamico dell’IPS attraverso un modello matematico del sistema tarato sui transitori elettromeccanici.

Infine, per dimostrare l'applicabilità della procedura proposta, nel sesto capitolo viene analizzato un caso di studio: l'IPS di una nave da perforazione offshore oil & gas dotata di posizionamento dinamico. Questo caso di studio è stato scelto a causa dei requisiti molto stringenti di questa classe di navi, il cui impatto sul progetto dell’IPS è significativo. Viene presentata l'analisi dell’IPS tramite la tecnica di Fault Tree Analysis (anche se con un livello di dettaglio semplificato), seguita dal calcolo di diversi indici di affidabilità. Tali risultati, unitamente a norme e regolamenti vigenti, sono stati utilizzati per definire i dati di input per le simulazioni, effettuate utilizzando un modello matematico dell’IPS costruito appositamente. I risultati delle simulazioni hanno consentito di valutare come il sistema dinamicamente si porta all’avaria a partire dai guasti rilevanti, e pertanto di proporre soluzioni migliorative.

Summary

Nowadays, in the large ships the electric propulsion solution is a viable alternative to the mechanical one. In fact, at present the latter is limited only to ships with peculiar requirements, such as the need of a high cruise speed or use of specific fuels. The use of electric propulsion, paired with progressive electrification of onboard loads, led to the birth of the All Electric Ship (AES) concept. An AES is a ship where all onboard loads (propulsion included) are electrically powered by a single power system, called Integrated Power System (IPS). The IPS is a key system in an AES, thus requiring both accurate design and management. Indeed, in AES electricity powers almost everything, highlighting the issue of guaranteeing both the proper Power Quality and Continuity of Service. The design of such a complex system has been conventionally done considering all the single components separately, to simplify the process. However, such practice leads to poor performance, integration issues, and oversizing. Moreover, the separate design procedure affects heavily system's reliability, due to the difficulty in assessing the effect on the ship of a fault in a single subsystem. For these reasons, a new design process is needed, able to consider the effect of all components and subsystems on the system, thus improving the ship design's most important drivers: efficiency, effectiveness, reliability, and cost saving.

Therefore, the aim of the research has been to obtain a new design methodology, applicable to the AES' IPS, which is able to consider the systems as a whole, with all its internal interdependencies. The results of such research are depicted in this thesis work, as a sub-process to be integrated into IPS's design process.

In this thesis, a wide review of the state of the art is done, to allow understanding the context, why such innovative process is needed, and which innovative techniques can be used as an aid in design. Each point is discussed focusing on the aim of this thesis, thus presenting topics, bibliography, and personal evaluations tailored to direct the reader to comprehend the impact of the proposed design process.

In particular, after a first chapter dedicated to the introduction of All Electric Ships, in which are described how such ships have evolved, and what are the most impacting applications, a reasoned discussion on the conventional ship-design process is given in the second chapter. In addition to that, an in-depth analysis of the IPS design is done, to explain the context in which the proposed innovative design process has to be integrated. Several examples of issues coming from the conventional design process are given, to motivate the proposal of a new design process. Not only the above mentioned design issues, but also the upcoming introduction of innovative distribution systems onboard ships and the recent emergence of

new requirements, whose impact on IPS is significant, are motivations calling for a new design process. Due to that, an excursus of both these two topics is given in the third chapter, referring to recent literature and research activities.

Chapter four is dedicated to the description of the tools that will be used to build the innovative design process. The first part is dedicated to dependability theory, which is able to give a systematic and coherent approach to the determination of faults effects on complex systems. Through dependability theory and its techniques, it is possible: to assess the effect of single components faults on the overall system; to assess all the possible causes of a given system failure; to evaluate mathematical figures related to the system in order to compare different design solutions; and to define where the designer must intervene to improve the system. The second part of the fourth chapter is dedicated to power system's software simulators and hardware in the loop testing. In particular, the use of such systems as an aid in designing power systems is discussed, to allow comprehending why such tools have been integrated in the innovative design process developed.

The fifth chapter is dedicated to the developed design process. Discussion is presented on how such process work, how it should be integrated in ship design process, and which is the impact it have on the design. In particular, the developed procedure implies both the application of dependability theory techniques (in particular Failure Tree Analysis), and the simulation of the dynamic behavior of the power system through a mathematical model of the system tailored on electromechanical transients.

Finally, to demonstrate the applicability of the proposed procedure, in chapter six a case of study has been analyzed: the IPS of a Dynamic Positioned Offshore Oil & Gas drillship. This has been done due to the stringent requirements these ships have, whose impact on power system's design is significant. The analysis of the IPS done through the Fault Tree Analysis technique is presented (though using a simplified detail level), followed by the calculation of several dependability indexes. Such results, together with applicable rules and regulations, have been used to define the input data for simulations, carried out using a mathematical model of the IPS built on purpose. Simulations outcomes have been used in turn to evaluate the dynamic processes bringing the system from relevant faults to failure, in order to improve the system's response to the fault events.

Contents

List of figures

List of Tables

Glossary

AC: Alternating Current

AES: All Electric Ship

AN: author's note

AVR: Automatic Voltage Regulator

BB: Birnbaum importance index

CHIL: Control Hardware-In-the-Loop

DC: Direct Current

DG: Diesel Generator

DP: Dynamic Positioning *or* Dynamic Positioned *(referring to Ship/Vessel)*

FATs: Factory Acceptance Tests

FT: Failure Tree

FTA: Fault Tree Analysis

FMEA: Failure Modes and Effects Analysis

FV: Fussell-Vesely importance index

HAZOP: Hazard and Operability Analysis

HIL: Hardware-In-the-Loop

HVAC: Heating, Ventilation, and Air Conditioning

HVSC: High Voltage Shore Connection

IEEE: Institute of Electrical and Electronics Engineers

IEC: International Electrotechnical Commission

ILO: International Labour Organization

IMO: International Maritime Organization

IPS: Integrated Power System

LV: Low Voltage

LVDC: Low Voltage Direct Current

MV: Medium Voltage

MVAC: Medium Voltage Alternating Current

MVDC: Medium Voltage Direct Current

PHIL: Power Hardware-In-the-Loop

QoS: Quality of Service

RBD: Reliability Block Diagram

RCM: Reliability Centered Maintenance

SG: Speed Governor

SRtP: Safe Return to Port

SOLAS: international convention for the Safety Of Life At Sea

SWB: Switchboard

UPS: Uninterruptible Power Supply

VDL: Variable Deck Load

WCF: Worst Case Failure

WCFDI: Worst Case Failure Design Intent

ZEDS: Zonal Electrical Distribution System

Introduction

Objective

The aim of this thesis is to present an innovative design process, applicable to the All Electric Ships' (AESs) Integrated Power System (IPS), which considers the IPS as a single complex system with all its internal interdependencies.

Indeed, nowadays the design of such a complex system is done considering the single components separately. This leads to poor performance, integration issues (sometimes with dangerous outcomes), and oversizing. Moreover, the separate design procedure affects heavily on system's reliability. In fact, a fault in a single subsystem has an effect on the overall system that cannot be assessed easily, leading frequently to the adoption of ineffective countermeasures to that single fault. This usually cause a rise in costs, without bringing any improvement to the system.

For these reasons, a procedure capable of taking into account all the system's components behaviour is needed, to further improve the ship design's most important drivers, such as efficiency, effectiveness, reliability, and cost saving.

Outline of the thesis

The research work, developed during the PhD activity, has been performed at the Laboratory of Grid Connected and Marine Electric Power Generation and Control (EPGC Lab), in the University of Trieste. The development of the research has been made throughout several research projects and activities, which have contributed to achieve the necessary theoretical and practical bases to develop the innovative design process.

The first chapter is aimed at giving an overview on All Electric Ships (AESs). At first, the evolution in ship power systems that have led to the AESs birth is presented, followed by a concise state of the art of AESs' Integrated Power Systems (IPSs). The last section of the chapter analyze the most demanding applications of the AES concept, focusing on Dynamic Positioned (DP) vessels characteristics and requirements, in order to introduce the case study of Chapter 6.

The conventional ship design process is presented in first section of the second chapter, together with a discussion on the methodology currently used to design IPSs for AESs. The topic is discussed concisely, to allow comprehending how such processes work, but some considerations on possible pros and cons are given. Examples of issues and criticalities caused by the conventional design process are shown in the second section of the second chapter, to demonstrate the need to change such processes due to its inability to address the modern AES IPSs design issues.

Goal of the third chapter is to present some innovative distribution systems and new requirements. Indeed, onboard systems are evolving from conventional radial AC distributions to new systems, on which no previous design experience is available (such as Medium Voltage DC distribution, Mixed AC/DC distribution systems, etc.), and new requirements from owners (such as pulsed loads supply or feeding land systems from the ship) are creating new issues never faced before. The design of an IPS endowed with these new characteristics is difficult to face with common design process, pushing towards the need of a new methodology able to address the design of such innovative systems. Due to that, the chapter depict concisely the characteristics of these innovative distribution systems and possible new impacting requirements, thus allowing the comprehension of the problems the IPS designers are facing nowadays.

In the fourth chapter, some innovative theories and techniques are presented: dependability theory, software simulators, and Hardware-In-the-Loop (HIL) testing. Although being created for rather different applications, each of them can be successfully applied as an innovative tool to help in system's design (although HIL testing is more a verification tool than a design one). In particular, the ones shown in the chapter will be relevant for the definition of the new design process, goal of this PhD work. Due to that, these tools are described in this chapter, focusing on how they can be used as a design aid.

After having given all the information needed to comprehend why a new design is needed and which tools can be used to aid design process, it is possible to define the innovative design process. Goal of the fifth chapter is to present the design process developed during the research activity, which integrates the new design tools. These make it able to solve (or at least mitigate) the issues coming from conventional design and to aid in designing new generation integrated power systems. The design process is here focused on the IPS's design, but it is generally applicable to each sub-system's design, also outside shipboard applications.

The final chapter is focused on a case study, used to demonstrate the applicability of the proposed design process. After an outline about the system to be analyzed, the chapter proceeds presenting the parameters and the data about the case study. Following that, the application of the innovative design process steps is made, dicussing extensively each passage in order to clarify the achievable results and the possible outcomes of the analyses done.

1 All Electric Ships

1.1 Introduction

Goal of this chapter is to give an overview on All Electric Ships. At first, the evolution in ship power systems that have led to the All Electric Ships birth is presented. An overview on the state of the art of All Electric Ships Integrated Power Systems is then given, to allow comprehending their peculiarities and their operation. Finally, a discussion on the most demanding applications of All Electric Ship concept is given, focusing on Dynamic Positioned vessels characteristics and requirements. This to the aim of both introducing the case study of Chapter 6 and explaining why this thesis work has been focused on the design of such systems.

1.2 Ship's evolution: towards the All Electric Ship

In the last two centuries ships have evolved at a fast pace. The application of steam power to propulsion was the trigger to this evolution. In fact, steam was the first form of human generated power, easily controllable, and several times powerful than what previously used for ships propulsion (wind and human power). The introduction of internal combustion engines (mainly diesel engines, but also gas turbines) increased both performance and functionality of the ship, accelerating ship's development. Starting from early-1800 steam-powered ships, the improvements in shipboard systems were significant and increasingly rapid, up to the modern diesel-electric ships. In particular, the development occurred in the last 30 years has caused a huge step ahead in ship's design. Indeed, both the efficiency of the entire vessel and the new functions given to the owners have increased, thanks to the progressive electrification that has occurred.

Almost a century ago, there was a strong competition between electrical drives and the then-growing mechanical drives. At the time of the birth of the modern ship propulsion, the electrical solution was promising, up to the point to push the American Navy to the construction of an experimental electrically powered collier in 1912. Such experimental ship showed promising results, leading to the production of a series of electrically powered warships a few years later, whose field of test was the Second World War. These electric propelled warships have proved to consume 20% less fuel compared to conventional propelled vessels, which were using turbine engines at that time. The main issue, which caused the abandonment of such innovative idea, was the electric propulsion size and weight, much greater than conventional one. Indeed, at that time changing electric motors' speed and power was possible only through the variation of electric power supply frequency, achieved regulating from prime mover side the rotation speed of a steam powered electric generator.

Such system was complex and bulky, due to the presence of additional electrical machinery to conventional steam-turbine propulsion. However, performance and efficiency were in favor of electrical solution, hence electrical propulsion kept its estimators until the introduction of diesel engines. These new engines were easier to control and manage than both steam and turbo-electric propulsion ones, whereby diesel engines and pure mechanical propulsion became the standard solution until 1980. [1] [2] [3]

In the 1980s, the fast development in power electronics led to the construction of semiconductor switching devices capable of handling high currents. Thanks to these devices became possible to control electric variables (voltage and frequency) for high power applications. At the same time, the advancements in electrical machines design allowed producing smaller, torque denser and more robust motors. These two conditions together opened new ways of applying electric drives, thanks to the possibility to have variable speed control of motors independently from generators' supply without using cascaded electrical machines. All these advantages reduced the penalties associated to the old turbo-electric propulsion, thus allowing the re-introduction of electric powered propellers onboard ships [2]. In fact, one of the main reasons to prefer electric propulsion above mechanical one is the global system efficiency, exactly as happened with the first turbo-electric solutions. Although electric propulsion system efficiency drops below mechanical propulsion at the optimal operating point, having many more energy conversion stages and related losses, its efficiency remains practically constant on the overall operation field (from low speed/power to high speed/power). Conversely, mechanical propulsion have maximum efficiency only in a reduced operation area (near 80-90% of rated power), dropping considerably at low loads, and way below electrical one. Since a ship commonly sails at a speed lower than its maximum possible one, due to operating economy reasons, mechanical propulsion systems rarely works on maximum efficiency point, making it costly than electrical one. Indeed, sailing at max speed may be more efficient on the purely propulsion point of view, but hydrodynamic resistance causes a relevant increase in required propulsion power at high speeds (the relation can be roughly modeled as cubic), leading to an overall increase in fuel consumption.

On the other hand, electric equipment evolution had not stopped during the long diesel-mechanical propulsion parenthesis. The number of electric powered devices increased more and more, due to both the better performance, safety, and operation easiness of electrical powered devices in respect to mechanical and hydraulic powered ones, and the increase in functions to be integrated onboard. Moreover, electric devices allowed saving space and reducing noise and vibrations, relevant issues in shipboard applications. These reasons brought to the increasingly adoption of electric powered devices onboard, up to the point that, as an example, in a modern cruise liner mechanical operated devices are relegated only to emergency applications.

These two different evolutionary paths have crossed at the start of the 80s, resulting in a revolution in shipbuilding sector. The invasive adoption of electric powered equipment, both due to electric propulsion and electric devices, led to the birth of the so-called All Electric Ships (AESs). Such ships are endowed with a power system that supplies all shipboard loads, propulsion included, by means of a common set of generators. Due to that, and thanks to the possibility to reroute the power wherever is needed at the time, the power system has been called Integrated Power System (IPS).

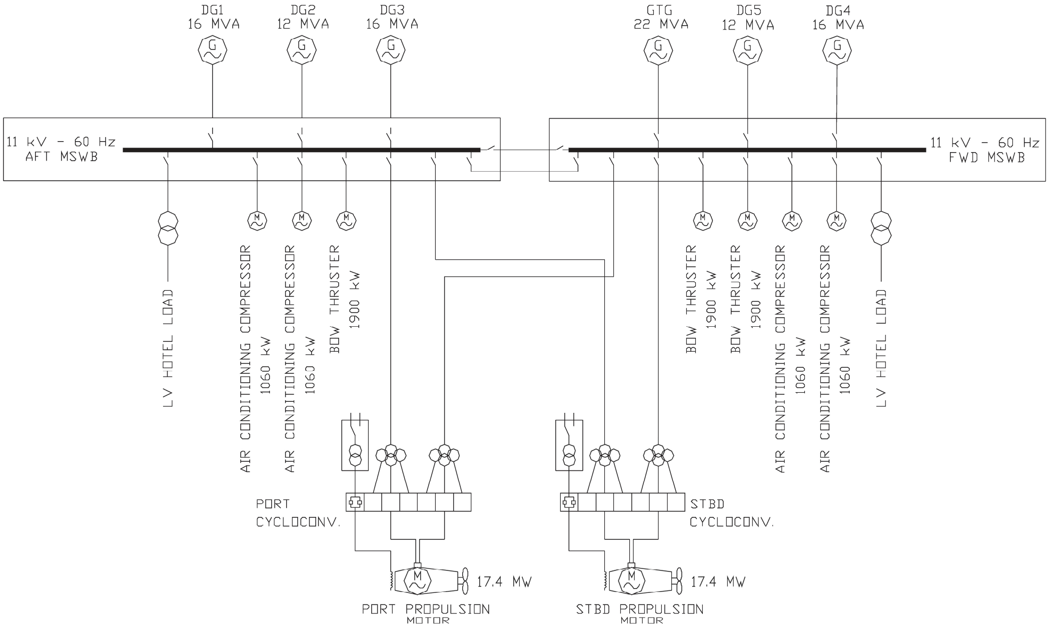
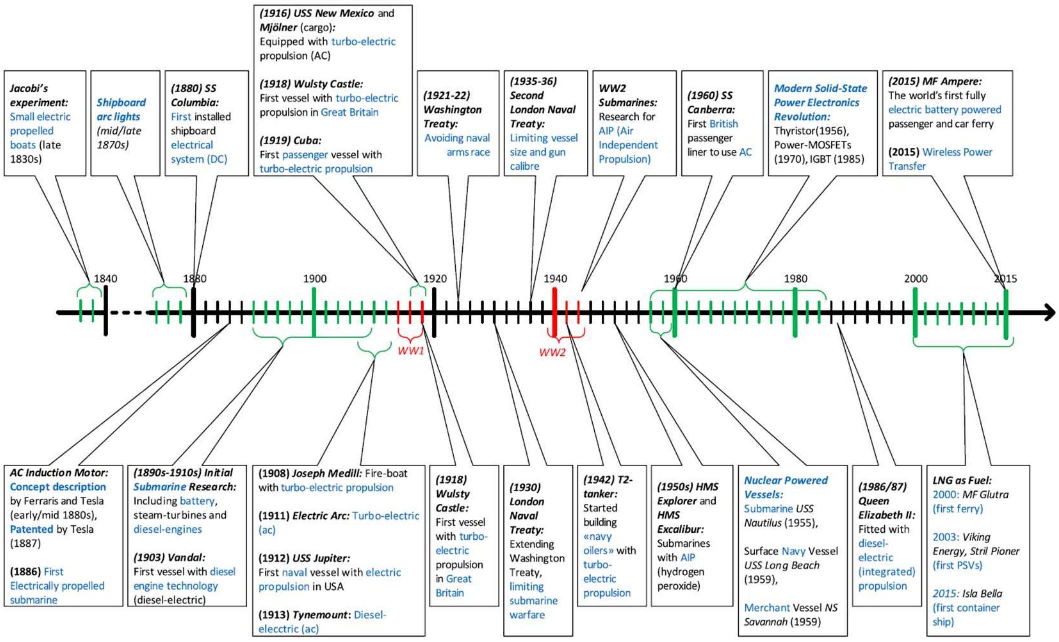


Figure 1 - Typical cruise all electric ship integrated power system [4].



Jacobi's experiment: Small electric propelled boats (late 1830s)

Shipboard arc lights *(mid/late 1870s)*

(1880) SS Columbia: First installed shipboard electrical system (DC)

(1916) USS New Mexico and ***Mjölner*** (cargo)***:*** Equipped with turbo-electric propulsion (AC)

(1918) Wulsty Castle: First vessel with turbo-electric propulsion in Great Britain

(1919) Cuba: First passenger vessel with turbo-electric propulsion

(1921-22) Washington Treaty: Avoiding naval arms race

(1935-36) Second London Naval Treaty: Limiting vessel size and gun calibre

WW2 Submarines: Research for AIP (Air Independent Propulsion)

(1960) SS Canberra: First British passenger liner to use AC

Modern Solid-State Power Electronics Revolution: Thyristor(1956), Power-MOSFETs (1970), IGBT (1985)

(2015) MF Ampere: The world's first fully electric battery powered passenger and car ferry

(2015) Wireless Power Transfer

AC Induction Motor: **Concept description** by Ferraris and Tesla (early/mid 1880s), **Patented** by Tesla (1887)

(1886) First Electrically propelled submarine

(1890s-1910s) Initial Submarine Research: Including battery, steam-turbines and diesel-engines

(1903) Vandal: First vessel with diesel engine technology (diesel-electric)

(1908) ***Joseph Medill:*** Fire-boat with turbo-electric propulsion

(1911) ***Electric Arc:*** Turbo-electric (ac)

(1912) ***USS Jupiter:*** First naval vessel with electric propulsion in USA

(1913) ***Tynemount*****:** Diesel-elecctric (ac)

(1918) Wulsty Castle: First vessel with turbo-electric propulsion in Great Britain

(1930) London Naval Treaty: Extending Washington Treaty, limiting submarine warfare

(1942) T2-tanker: Started building «navy oilers» with turbo-electric propulsion

(1950s) HMS Explorer and ***HMS Excalibur:*** Submarines with AIP (hydrogen peroxide)

Nuclear Powered Vessels: Submarine *USS Nautilus* (1955),

Surface Navy Vessel *USS Long Beach* (1959),

Merchant Vessel *NS Savannah* (1959)

(1986/87) Queen Elizabeth II: Fitted with diesel-electric (integrated) propulsion

LNG as Fuel: 2000: *MF Glutra* (first ferry)

2003: *Viking Energy, Stril Pioner* (first PSVs)

2015: Isla Bella (first container ship)

Figure 2 - Historical highlights of marine vessel's electrical power system's evolution: timeline [5].

The IPS removed the need of separated engines to generate electric power for onboard loads, necessary with diesel-mechanical propulsion, reducing total occupied size and increasing efficiency, (this is why it is called "integrated). In fact, an IPS can be considered equivalent to a land power grid, where generation, distribution, and utilization of the electric power coexists in a limited space (an example of a typical cruise ship IPS is shown in Figure 1). In an All Electric Ship, the IPS is the core system, being every load electrically powered. Losing power generation (blackout) means losing the ship control, which can lead to harmful consequences to people, things, and environment.

Nowadays the AES concept is widely applied on large ships: only ships with special requirements, such as high speed or peculiar fuel, still use mechanical propulsion (here small crafts are not considered, due to very different customer targets). As an example, in the field of the large cruise ships the AES concept has become a standard, covering the 100% of the constructions made by the major shipyards in the world. Other applications of AES concepts are: ferries, oceanographic ships, gas carriers, cable/pipe laying vessels, oil & gas dedicated vessels and platforms, icebreakers, mega-yachts. A separate mention deserves the military area, in which until now mechanical propulsion solution was the only one considered. This because of both high speed and reliability requirements of naval vessels, which led the designer to focus on well-proven technologies. However, in recent time a high attention is being paid to electric propulsion also in military area. This is clearly demonstrated by the growing number of research projects regarding this type of propulsion in all the most technologically advanced navies.

To conclude the discussion about ship's evolution, a timeline recalling the main milestones in marine vessel's power systems is shown in Figure 2, taken from [5].

1.3 The All Electric Ship concept

The simplest definition of an "All Electric Ship" can be: a vessel endowed with electric propulsion, having all on-board loads electric powered, and having a single power system dedicated to supply both of them called Integrated Power System. The main benefits of the AES concept [6], made possible by both the electric propulsion and the integrated power system application, are:

- Better dynamic response;
- flexibility in space and weight allocation (propulsion motors and electric generators can be installed in different places, short shafts);
- more degrees of freedom in power system layout design;
- podded-drive solution availability (removal of shafts and rudders, increased maneuverability);

- enhanced control of electric propulsion systems (acceleration and maneuvering);
- increased overall efficiency (possibility to modulate the number of running generators to reach the optimal operating point, better management of Heating Ventilation and Air Conditioning systems - HVAC);
- noise and vibration attenuation (consequently increased comfort);
- advanced automation and reduction of the crew;
- increased survivability (generator sets distributed, better ship compartmentation);
- increased maintainability;
- enhanced operating life (less mechanical components, fewer stress on prime movers).

As stated before, electric propulsion allows an increase in efficiency at partial load operation, in respect to mechanical one (when comparing solely propulsion section efficiency). When considering the overall ship operation, the AES concept boosts this gain to a significant level, thanks to the modularization applied in IPS power stations. Indeed, an AES achieves its total generating power through at least two power stations, each consisting in two or more generators (as can be seen in IPS example, Figure 1). This allows splitting the maximum required power in several smaller (either equal or with different power levels) units instead of one big prime mover, ensuring a sufficiently high number of combinations of generators to keep their operating point near the maximum efficiency areas. Such concept can be illustrated through Figure 3, in which the total efficiency of the power system in respect to required propulsion power is shown, for both mechanical and electric propulsion.

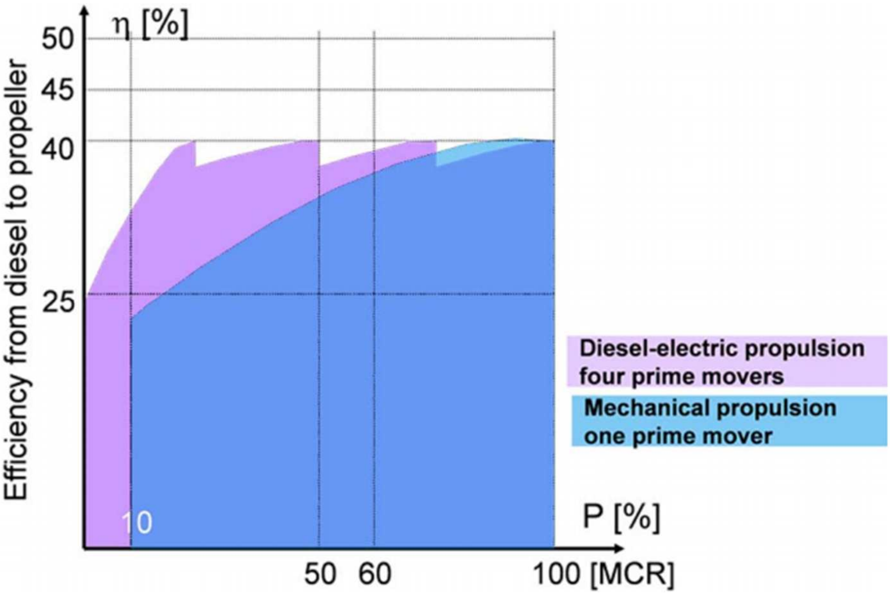


Figure 3 - AES, efficienciency of electric propulsion [2].

As can be seen, the possibility to start generators (thus their prime movers) only when the system required power overcomes the running generator's capabilities allows keeping the global efficiency at a high level also for low loads. This is true not only for propulsion, but also for onboard loads. In fact, supplying both trough the same power system allows rerouting power wherever needed, lowering total required power. As an example, cruise liners sails mostly by night, when passengers sleep. Due to that, during the night the electric load given by the hotel section of the ship drops, whereas the power required for propulsion increases. Conversely, during the day the ship usually it is moored in port, due to that propulsion load is absent; however, at the same time all the passengers are awake and use ship's commodities, increasing electric load required by the hotel section. The IPS allows supplying the ship in both of these situations, with an installed generation power way lower than the sum of the two. Moreover, in case of an emergency (like one or more generators faults), it is possible to balance the two loads actively, reducing propulsion power to ensure proper onboard loads supply, or reducing onboard commodities to ensure a minimum level of propulsion power.

Power supply in shipboard power systems is commonly achieved through diesel-generators, consisting in a marine diesel prime mover coupled with a wound-field synchronous alternator. For what concerns prime movers, other solutions are possible (and applied), such as gas turbines, while other types of electric generators are rarely used. Indeed, the robustness, ease of control, cheapness, and long-term experience on these machines make them the most reasonable choice for onboard installations. The brushless excitation configuration is the only viable solution in marine systems, due to its lower sensitivity to external ageing factors such as salt mist and humidity.

For what concerns loads, these are commonly formed by:

- Main propulsion system;

  Used to propel the ship forward and backward, main propulsion systems are the highest power single loads onboard (cruise ships nowadays commonly have 10÷20 MW for each propulsion axis, while other vessels can reach ever-higher power levels [1]). Power electronic converters, feeding variable speed electric motors directly connected to fixed pitch propellers, compose it. Variable pitch propellers can be used in high performance applications, but are not required due to the regulation capabilities of the electric propulsion system. Cycloconverters and synchroconverters coupled with synchronous machines are common onboard, but nowadays high power systems using PWM converters and induction motors are starting to be applied.

- Maneuvering propulsion systems (thrusters);

  Auxiliary propellers installed onboard, used to improve ship maneuvering capabilities during navigation, and to allow side movement (such as in berthing operation). The most common solution is a Direct On Line (DOL) induction motor coupled with a variable pitch propeller. However, PWM supplied motors coupled with fixed pitch propellers may be a future solution, when such systems will be able to achieve the same hydrodynamic performance of the conventional ones.

- HVAC systems;

  Set of subsystems needed to keep the ship in inhabitable conditions, through heating, cooling, and air exchange. Ventilation and heating subsystems are usually scattered throughout all the ship, being electrically powered, while air-cooling is usually achieved through a cold-water closed loop system. Heat exchangers and high power electrical compressors, directly connected to the main switchboard, provide cold water.

- Hotel loads;

  Such a name is used to classify the loads dedicated to provide accommodation to the ship's inhabitants, such as lighting systems, kitchens, waste management, entertainment, and so on. Hotel load can be a minimum quota of the total ship loads, as happens in most merchant and naval vessels, or can be the most relevant load onboard (either comparable or higher than main propulsion), as happens in cruise vessels.

- Navigation system loads;

  To keep the ship on the right route, and at the same time avoid dangerous collisions, a set of subsystems are needed. Radar systems, GPS, satellite and radio systems, all of them can be defined as navigation systems. Such loads commonly require high power quality, so they are fed through dedicated power converters.

- Other loads;

  All the loads not included in the above classification are here collected, such as firefighting pumps, fuel management, etc.

Power distribution onboard ships is very dependent on application. Different kind of vessels have different requirements, thus reflecting in different solutions for electric power distribution. Due to that, it is possible to state some common architectures applied in a single application area, but variations are possible. Some good descriptions and figures about AESs IPSs and propulsion systems can be found in [2] and [7]. Generally, when an architecture proves to be sufficiently reliable for an application, such a distribution system topology it is fixed and kept nearly untouched. This until a new requirement become conflicting with it. As an example, the Figure 1 power system is used for cruise liners from about thirty years, i.e. since the concept of AES has been adopted in this field. Such a structure have changed a little in the past, to integrate the basic level of fault resistance imposed by rules and regulations (mainly SRtP - Safe Return to Port regulation, part of requirements published by the SOLAS – Safety of Life at Sea convention [8]), with the goal to achieve the required redundancy at the lowest possible cost. Two main switchboards, connected through tie-breakers, supply all the ship's loads, either directly (for high power loads), or through lower voltage switchboards and onboard distribution. On such ships it is possible to have four or six generators, equally divided between the two switchboards, and the common ship operation is done in the so called closed bus condition. This means having the tie-breakers between switchboards closed, thus operating with a single power system. This allows achieving the efficiency goals above mentioned, keeping the possibility to separate the switchboards opening the tie-breakers in case of faults, thus achieving two separate power systems (the so called open bus operation). Other ships can have different layouts, such as the one depicted in Figure 4, used in Offshore Drillships [9]. Such a complex design comes from strict requirements on system's behavior in the event of faults. Indeed, such vessels have to keep a defined level of operating capability in spite of faults, to avoid damaging people, properties, or environment. Another different power system layout is the one depicted in Figure 5, installed onboard IT Navy aircraft carrier "Nave Cavour". Its ring structure, powered by several generators scattered onboard the ship hull, maximize ship's survivability, limiting the damage to the IPS in case of external menaces [10] [4].

Due to the high power levels of AES's IPS, tree-phase distribution is always applied for primary and secondary distribution, while some low voltage end-circuits can be single-phase. For what concerns voltage levels, such ships commonly require Medium Voltage primary distribution, spanning from 4.4 to 11 kV, while secondary Low Voltage distribution can span from 127 to 690 V, with exact values depending on the owner requirements and ship's area of operation. As an example, cruise liners use commonly 6.6 or 11 kV (depending on total ship power), with 120, 230 and 400 V Low Voltage sections. Standard voltage levels are identified in [11], [12], and other applicable standards. Frequencies, on the other hand, have two standardized values: 50 or 60 Hz. The choice between these two values is mainly due to owner requirement, being the difference non-influent by a purely technical point of view. However, it can be stated in general terms that the ship's that will operate in Europe are built with 50 Hz, while other use 60 Hz (mainly following land power system frequencies). Other frequencies can be used, but limited to small sections of the IPS, such as the 400 Hz distribution dedicated to aircraft supply in aircraft carriers, or other peculiar frequencies for military grade electronic warfare equipment. To give an idea of the power levels AES IPSs can reach, an example can be made: the cruise liner Queen Mary II, with 86 MW of total propulsion power and 112MVA of alternators, holds the record as total installed power of electrical drives and power plant on an AES now. However, nowadays some naval vessels are reaching similar levels, like the nearly ready HMS Queen Elizabeth. In fact, the UK Navy new aircraft carrier is an All Electric Ship, with a total installed electric power generation capability of 109MW, and will enter on duty in 2016. Such a ship, together with some lesser tonnage units, are examples of the worldwide Navies interest in the AES concept.

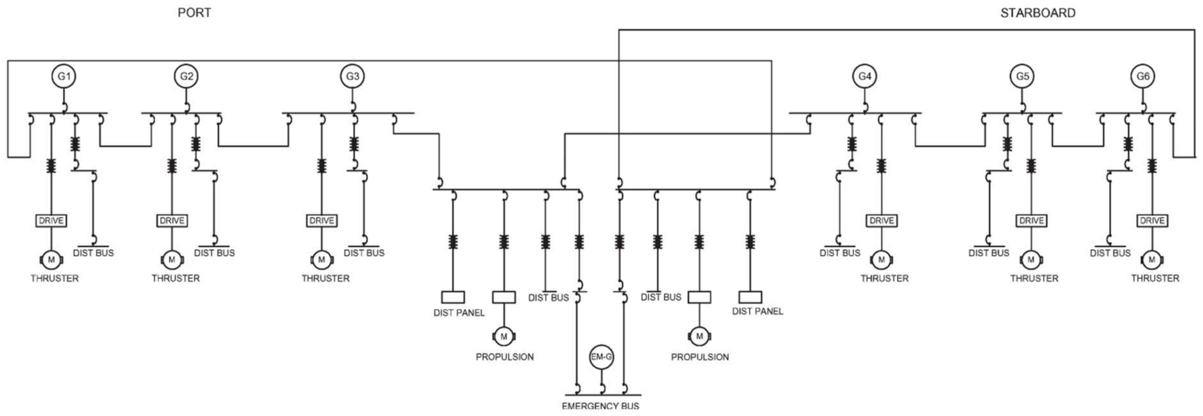


Figure 4 - Typical offshore drillship integrated power system [9].

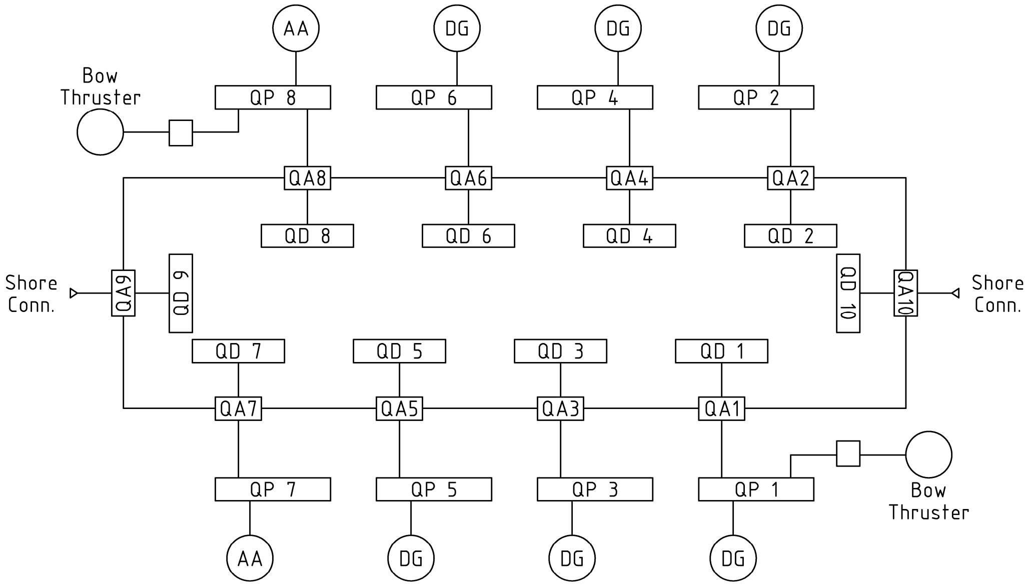


Figure 5 - IT Navy aircraft carrier "Nave Cavour" ring power system [4] [10].

The IPS is a rather complex system, and its function is to deliver electric power to the loads. To do that, proper control systems have to be installed, allowing keeping the power system variables into the correct operation limits. In a conventional IPS, most of the work is done through control systems acting on the generators, while protections are usually installed directly on the related subsystem. The most relevant control systems are the AVRs (Automatic Voltage Regulators) and the SGs (Speed Governors), acting respectively on generator's excitation and prime mover. Voltage and frequency real-time controls are the basic key controls in an islanded system, being in charge of keeping the IPS electric variables into the limits without the aid of a stabilizing source, such as an external power grid (as commonly happens in land power systems). Indeed, in an IPS the rated values of voltage and frequency have to be maintained constant as much as possible, exactly as in land power systems. However, the reduced extension of the IPS, together with the reduced number of running generators, leads to significant transients following perturbations in such systems, which must be controlled by AVRs and SGs. Due to the peculiar characteristics of shipboard power systems, it is evident that the limits imposed in land power systems cannot be respected. Therefore, the major regulatory bodies impose particular limits on both static and transient voltage and frequency deviations. In Table 1, an example of such limits is show, taken from Lloyd's Register of Shipping [13]. Although these limits seems quite wide in respect to the ones commonly imposed on land, complying with them may not be simple. In fact, a careful control design has to be done in IPSs, to ensure obtaining a fast and well-damped system's transient response.

Table 1 - Voltage and frequency limits onboard ships [13]

Variable		**Limit**	**Recovery time**
Voltage	Permanent	+6%, -10%	
	Transient	±20%	1.5 s
Frequency	Permanent	±5%	
	Transient	±10%	5 s

A peculiar control system installed onboard ships is the so-called Power Management System (PMS) [14] [15] [16] [17]. It is an automation layer set above the subsystems' control systems, dedicated to their coordinated management. Indeed, in a complex system like an IPS, each subsystem (such as propulsion drives, generators, HVAC systems, etc.) is managed by its own control system. However, each subsystem is interfaced with the power system, so single components operation affects not only themselves, but also the other components through the common power supply. The PMS allows a coordinated action of each subsystem, to allow the optimal operation for the overall IPS (thus trying to reach an optimal combination of some relevant drivers, such as minimum fuel consumption, fault resistance, etc.) [14] [15]. In fact, functions performed by a PMS can be grouped into three major areas:

- Power generation management – monitoring of voltage and frequency controls operation, monitoring and control of active and/or passive load sharing function (for both active and reactive power), start and stop of generators following load demand;
- Loads management – monitoring of load power consumption, power limitation for high power controllable loads based on available power, load shedding;
- Distribution system management – monitoring of distribution system protections, control of relevant breakers, management of the distribution system configuration.

The PMS allows managing all these functions by the crew, virtually from a single control station, thus removing the need to act directly on single subsystems' control systems. Another function, not related with IPS normal operation, is the recording of significant variables of onboard systems (such as voltages, currents, breakers states, temperatures, and so on). Such a function became significant in case of incidents, because recording are an aid in comprehending causes of relevant failures.

For what concerns protections, the same equipment installed on land power systems is usually applied: overload, overcurrent, under-frequency, reverse power, etc. Tripping levels are set following the same guidelines applied in common power systems, and their operation is trivial. However, some peculiar issues may arise, such as incorrect tripping of breakers despite correct selectivity setting [18]. Indeed, due to the small extension of shipboard power systems, low amount of series impedance is present in the system: apart for transformers between busbars at different voltage, cables impedance is negligible. This may cause an insufficient decoupling between system's sections, leading to issues in determining exact fault location, causing incorrect protection system intervention. Examples of such issues can be found in [18], where real system's fault causes are investigated. These commonly are the result of an insufficient power system analysis, which does not take into account the peculiarity of such systems.

Another issue, related to the presence of high power converters in IPSs (mainly propulsion ones, but power electronics drives are increasingly applied onboard ships), is the harmonic distortion. Indeed, the high amplitude distorted currents absorbed by such converters have a significant impact on power system's power quality, being both the system poorly decoupled and the distorting loads power comparable with generator's power. Harmonic distortion levels have to be kept under limits imposed by regulatory bodies. This because harmonic distortion has negative effects on system operation, such as anomalous heating of electrical machines, stress of insulation systems, and possible incorrect operation of measurement systems and protections. Classic solutions to lower the harmonic content in the IPS are: the installation of harmonic filters, or the use of multi-pulse configurations for the higher power converters. However, more advanced solutions could imply the installation of new converter topologies (Active Front End – AFE), or active filtering [3].

The IPS is one of the most relevant systems in an AES, since ship's operation relies totally on electric power. This highlights issues on IPS Power Quality, concerning not only harmonic distortion and voltage/frequency fluctuation, but also continuity of service. In fact, an AES IPS is an islanded power system, lacking the connection to a larger electrical system that would help in stabilizing voltage and frequency, and supply to transient unbalances. In such a system, all the components acting on it are relevant to ensure its correct operation. In fact, IPS Power Quality mainly relies on the controllers installed directly on the generators, such as voltage and frequency regulators, but also ship automation (in particular, the PMS) deeply affects it, due to the control it has on both loads connection/disconnection and system configuration. The correct coordination between generator control systems, ship automation, and protection must be sought, to avoid critical issues. However, this is a difficult task to accomplish, and incorrect design sometimes happens. Errors mostly goes unnoticed, but in some cases lead to unforeseen consequences, commonly dangerous for both the ship and those who inhabit it [18]. Such an issue is one of the drivers that led to the idea on which is based this thesis work.

1.4 Most demanding All Electric Ship application: Dynamic Positioning classification

1.4.1 Definition of the most demanding AES application

The definition of "most demanding" AES obviously depends on the evaluated ship's parameters and the related technical area. As an example, from a purely mechanical point of view, LNG (Liquefied Natural Gas) tankers can be seen as really demanding, due to the high pressure, low temperature, gas containment system. Indeed, in such ships the cargo containment section is complex, although nowadays uses well-proven technology. Conversely, from both naval building and electrical point of view, such ships are really simple and straightforward.

In this thesis work, the focus is given to the ship's IPS, and related components. Due to that, only the electrically propelled ships with a significant installed power will be considered. In relation to this, the possible interesting applications are reduced to: cruise ships, naval vessels (new ones, applying AES concept), Dynamic Positioned vessels (icebreakers will be not considered here, due to their extremely specialized function).

For what concerns cruise ships, they commonly use the IPS structure depicted above (Figure 1). Such a structure is the result of about 30 years of continuous development based on the same drivers: ensuring the compliancy with both regulatory bodies and owners, limiting at the same time the costs as much as possible. The most significant revolution happened in this sector was the SOLAS SRtP regulation adoption [8]. SRtP imposes some minimum requirements on ship's redundancy levels and onboard technical systems location, to lower the hazard posed to people in case of a fault onboard. The requirements most impacting on the power system oblige the designers ensuring a minimum level of propulsion following fire or flooding, when limited to a single fire-zone or watertight compartment respectively. The IPS structure depicted above allows complying with SRtP requirements at the lowest possible cost, thus becoming the standard IPS structure on cruise vessels. Due to that, cruise ships cannot be addressed as demanding applications from a purely power system point of view.

Naval vessels are applying AES concept only recently, mainly due to the progressive electrification of onboard loads and the increase in military equipment required power. The former is happening with a relevant delay in respect to merchant area, because in military area well-proven technologies are preferred for common equipment. This allows finding and solving all the major fault of a technology, before installing it onboard a naval vessel, to the aim of limiting the variables that can impair ship's mission. The latter is due to both improved performance of military equipment, and the installation of new weapon systems, such as new radars, FELs (free electron lasers), electromagnetic launchers, etc. [19]. In naval AESs the focus is given to IPS redundancy and reconfiguration, to allow concluding the mission in spite of external menaces. Complex architectures are proposed and applied, such as the ring bus of IT Navy aircraft carrier "Nave Cavour", shown in Figure 5, or the mixed MVAC/LVDC (Medium Voltage Alternate Current / Low Voltage Direct Current) zonal distribution system of the innovative US Navy destroyer "U.S.S. Zumwalt" (class DDG-1000) [19].

Although naval vessels may seem the most demanding application in marine power systems, due to their military grade requirements, other vessels are in competition with them in terms of requirements: the ships endowed with Dynamic Positioning (DP) classification. Actually, the military application of the AES concept is recent, while DP all electric ships are nowadays common in merchant area (mostly in Oil & Gas applications, but not only limited to these). Indeed, the first application of a DP system onboard an electric propelled ship was in 1961 on the ship *Eureka* (Figure 6), built by Shell to drill ocean floor core samples [20]. From that time, significant improvements have been done, and nowadays DP classified ships are endowed with rather complex power systems, as can be seen in the example of Figure 4. Dynamic Positioned ships are commonly used to perform operations such as seabed drilling, cable/pipe laying, and so on. Such operations are capital intensive, and an interruption in the workflow can case damages spanning from simple money losses to damages to people, things, and environment. Due to that, DP ships have strict requirements on system redundancy, to avoid as much as possible the loss of the DP operation, thus the work interruption, leading to complex redundant IPS architecture (Figure 4). These ships have the strictest requirement on IPS operation in case of fault of the overall marine industry sector; therefore can be defined as the most demanding all electric ship application, from the integrated power system point of view [21].

The above-mentioned motivations led to the choice of a Dynamic Positioned Drillship as the case study in this thesis work. Due to that, some indications on requirements and operation of such ships are given in the following, to allow comprehending the relevance of the proposed innovative design process, core of this thesis.

Figure 6 - Ship "Eureka", the first dynamic positioned vessel [20].

1.4.2 Dynamic Positioning classification for ships

Dynamic Positioning classification is applied to ships which are able to keep their position only by means of their propulsion system, in spite of wind, waves, and faults (under certain fixed limits). Such ships are endowed with a complex control system, able to assess absolute or relative ship position, and to control propellers to the aim of keeping the error between reference and real position under a certain acceptable value.

Some basic definitions and concepts of the DP systems are given in the following, as stated in the Guide for Dynamic Positioning Systems, published by the American Bureau of Shipping (ABS) [22]. Other references can be given, from other regulatory bodies, such as Det Norske Veritas (DNV) [23]. Each different regulatory body apply its own classification, but base concepts and definitions are equivalent, at the point that the different classifications can be compared and a certain level of equivalence can be found (as shown in Table 2). This happens because each particular implementation of these rules by a classification society originates from a common source, which is the Document MSC/Circ. 645, emitted by the International Maritime Organization (IMO) [24]. Due to that, in this thesis work reference will be done to only the ABS guide, to ease the discussion. Accordingly, following definitions are taken from such a document:

Dynamic Positioned Vessel (DP Vessel): A unit or a vessel that automatically maintains its position (fixed location or predetermined track) by means of thruster force.

Specified Maximum Environmental Conditions: The specified maximum environmental conditions are the specified wind speed, current and wave height under which the vessel is designed to carry out intended operations.

Specified Operating Envelope: The specified envelope is the area within which the vessel is required to stay in order to satisfactorily perform the intended operations under the specified maximum environmental conditions.

Active component: Active components or systems are in particular: generators, thrusters, switchboards, DP control computers, sensors, remote controlled valves, compensators, etc.

Static component: Static components are in particular: cables, pipes, manual valves, etc.

Dynamic Positioning System (DP System): The complete installation necessary for dynamically positioning a vessel comprises the following subsystems

i) Power system,
ii) Thruster system,
iii) DP control system.

Power system: All components necessary to supply the DP system with power, the power system includes:

i) Prime movers with necessary auxiliary systems including piping,
ii) Generators,
iii) Switchboards,
iv) Electrical distribution system (cabling and cable routing),
v) Power management if applicable.

Thruster System: All components and systems necessary to supply the DP system with thrust force and direction. The thruster system includes:

i) Thrusters with drive units and necessary auxiliary system including piping,
ii) Main propellers and rudders if these are under the control of the DP system,
iii) Thruster control electronics,
iv) Manual thruster controls,
v) Associated cabling and cable routing.

DP Control System: All control components and systems, hardware and software necessary to dynamically position the vessel. The DP control system consists of the following:

i) Computer system/joystick systems,
ii) Position reference systems,
iii) DP sensor system,
iv) Display system (operator panels),
v) Associated cabling and routing.

Worst Case Failure (WCF): The identified single fault in the DP system resulting in maximum effect on DP capability as determined through the FMEA (Failure Modes and Effects Analysis, see section 4.2.3 of this thesis work, at page 74). This worst case failure is to be used in the consequence analysis.

Worst Case Failure Design Intent (WCFDI): The worst case failure design intent describes the minimum amount of propulsion and control equipment remaining operational following the worst case failure. The worst case failure design intent is used as the basis of design. This usually relates with the number of thrusters and generators that can simultaneously fail.

Redundancy: Ability of a component or system to maintain or restore its function, when a single fault has occurred. Redundancy can be achieved for instance by installation of multiple components, systems or alternative means of performing a function.

Redundancy concept: The means by which the worst case failure design intent is achieved. It is to be documented as a part of the preliminary design process.

Single fault: The single fault is an occurrence of the termination of the ability to perform a required function of a component or a subsystem in the DP system. For vessels with DPS-3 notation, the loss of any single compartment is also to be considered as a single fault.

Single fault tolerance: The ability of a system to continue its function, following a single fault, without unacceptable interruption.

The class of the DP system, therefore the class of the ship, is defined according to the following:

DPS-0 For vessels, which are fitted with centralized manual position control and automatic heading control system to maintain the position and heading under the specified maximum environmental conditions.

DPS-1 For vessels, which are fitted with a dynamic positioning system which is capable of automatically maintain the position and heading of the vessel under specified maximum environmental conditions having a manual position control system.

DPS-2 For vessels, which are fitted with a dynamic positioning system which is capable of automatically maintain the position and heading of the vessel within a specified operating envelope under specified maximum environmental conditions during and following any single fault, excluding loss of compartment or compartments.

DPS-3 For vessels, which are fitted with dynamic positioning system that is capable of automatically maintaining the position and heading of the vessel within a specified operating envelope under specified maximum environmental conditions during and following any single fault, including complete loss of a compartment due to fire or flood.

American Bureau of Shipping structures DPS-1, DPS-2 and DPS-3 classification notation following the guidelines of the IMO MSC/Cir.645 "Guidelines for Vessels with Dynamic Positioning Systems" [24], as previously stated, as well as all the other Classification Societies. In particular, such notations are in line with IMO equipment class 1, 2 and 3, respectively.

Table 2 – Class Notation equivalence between major Classification Societies [25]

DNV **Det Norske Veritas**	**ABS** **American Bureau of Shipping**	**LRS** **Lloyd's Register of Shipping**
DYNPOS T	DPS-0	DP (CM)
DYNPOS AUTS	Not applicable	Not applicable
DYNPOS AUT	DPS-1	DP (AM)
DYNPOS AUTR	DPS-2	DP (AA)
DYNPOS AUTRO	DPS-3	DP (AAA)

1.4.3 Specific Requirements

The technical requirements of DP vessels, imposed by classification society, are related to their ability to keep position in spite of adverse events. Indeed, a DP vessel has to be designed to have a defined level of position keeping capability and related reliability. The classification of DP systems made by regulatory bodies addresses the reliability of the DP system installed onboard, thus assessing minimum levels of fault tolerance and redundancy.

DP classes fault tolerance basic requirements are specified in Section 2 of [22], Rule 3.1:

a. For a vessel with the notation DPS-0, or DPS-1, a loss of position may occur in the event of a single fault;
b. For a vessel with the notation DPS-2, a loss of position may not occur in the event of a single fault in any active component or system, excluding a loss of compartment or compartments;

c. For a vessel with the notation DPS-3, a loss of position may not occur in the event of a single fault in any active or static component or system, including complete loss of a compartment due to fire and flood;

d. The redundant components and systems are to be immediately available and with such capacity that the DP operation can continue for such a period that the work in progress can be terminated safely;

e. The period for safely terminating a work in progress is to be specified by the Owner.

As can be easily seen from such basic requirements, the DPS-3 class notation is the most demanding from a fault tolerance point of view. The case study, which will be presented in Chapter 6 (page 117), has been chosen accordingly (DPS-3 classified drillship). This has been done with the aim of showing the impact of the new design methodology on the IPSs which mostly will benefit from it.

The requirements with the higher impact on the IPS will be given in the following. These will be generally limited to the DPS-3 notation, but also lower classes requirements will be considered when relevant.

The next requirements can be found in "ABS Guide for DP Systems" [22], in the November 2013 edition (with July 2014 updates). To correctly identify the rules reference, the following notation is applied:

A/X.Y.Z

where *A* is the section number, *X* the rule number, *Y* the number of the paragraph, *Z* the sub-paragraph number.

2/3.3.1 […]

> For the DPS-2 or DPS-3 notation is required to have an automatic dynamic positioning system, manual position control system and to be single fault tolerant.
>
> The single fault tolerance is to be achieved by the design of redundant systems. The station keeping capability after a single fault is to be achieved by providing control, electric power and thrust.
>
> […]
>
> For DPS-3 notation, a single fault includes:
>
> i) any active component or system […] and any normally static component is assumed to fail;
> ii) any component in any one watertight compartment from flooding;
> iii) any components in any one fire subdivision from fire.

2/3.3.2 Considerations on redundancy:

i) The redundancy is to have two or more items of equipment or system required to perform a function so that the redundant unit can take over from the failed unit without unacceptable interruption of function.

ii) Redundancy is to be based on systems which are immediately available for use, namely on running machinery. In general, full stop and restart of the system do not comply.

iii) Automatic start of equipment may be accepted as contributing to redundancy only if they can be tested to prove that they can be brought into operation before position and heading keeping performance is degraded.

iv) […] Independence of redundancy groups is to take into account all technical functions.

v) The redundancy design can consist of two fully redundant power and thruster systems each capable of maintaining position and heading if the other fails. The design can also make use of multiple systems each providing partial redundancy such that the vessel can maintain position with all combinations of independent systems that survive any defined fault. The redundancy design is to provide suitable combinations of available systems following any defined fault.

vi) The transfer of failures between redundant subsystems is to be prevented by separation of the redundant systems.

vii) […]

2/3.7 To meet the requirements for a DPS-series notation, the minimum number of subsystems and components and the redundancy for: power system, thruster system and DP control system are provided in Table 3. […]

2/5.1 The essential non-DP systems, such as common fire suppression systems, engine ventilation systems, emergency shutdown systems, etc., may interference with the DP system.

The redundancy concept for the DP system is to be followed through to these systems so that actions or failures initiated by these systems do not cause consequences that exceed the worst case failure design intent. […]

2/11.1 FMEA (Failure Modes and Effects Analysis, see Chapter 4.2.3, at page 76, of this thesis work) is only applicable to DPS-2 and DPS-3 notations. In general, two FMEAs are to be considered, one covering the main DP control systems and the other for all other systems onboard related to DP operations.

The purpose of the FMEA is to indicate whether or not the DP system meets the requirements of the relevant DP notation and complies with the vessel's WCFDI.

[…]

The objective of the DP FMEA is to at least include the following:

i) Identify and provide recommendations to eliminate or mitigate the effects of all single faults and common mode failures in the vessel DP equipment, which, if any occurs, would cause total or partial loss of station keeping capability.
ii) Demonstrate effective redundancy.
iii) Identify potential "hidden" failures and determine the effects of a second failure.

[…]

2/11.3 Failure Mode Analysis.

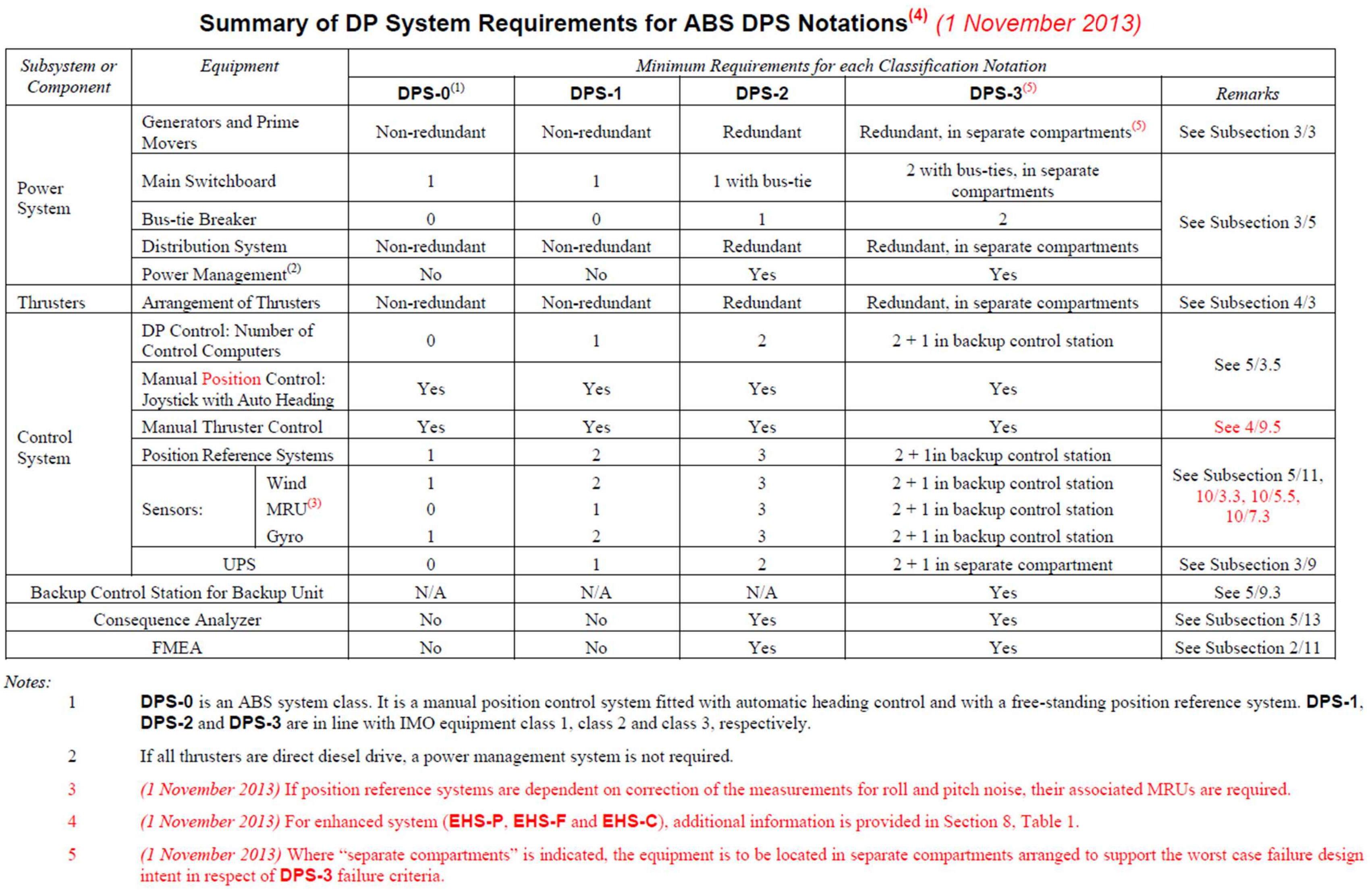
For a DPS-2 or a DPS-3 notation, loss of position is not allowed to occur in the event of a single fault. Single fault includes, but is not limited to following:

i) All redundant components, systems or subsystems
ii) A single inadvertent act of operation (ventilation, fire suppression, etc.) where applicable and if such an act is reasonably probable
iii) Hidden failures (such as protective functions on which redundancy depends) where applicable
iv) Common mode failures
v) Governor and AVR failure modes where applicable
vi) Main switchboard control power failure modes
vii) Bus-tie protection where applicable
viii) Power management system
ix) DP control system input and output arrangement
x) Position reference processing
xi) Networks
xii) Communication failure
xiii) Automatic interventions caused by external events, when found relevant (e.g. automatic action upon detection of gas)

[…]

When there are more configurations for the diesel electric plant design to cope with equipment unavailability (e.g. failures or equipment taken down for maintenance), it is important that all configurations that are possible to be included in DP operations are to be analyzed in the vessel's DP system FMEA to prove that the DP system remains redundant. Fault tolerance of the configurations is to be made visible and understood by the crew.

Table 3 – DP system requirements for ABS Notations [22].



Summary of DP System Requirements for ABS DPS Notations[4] *(1 November 2013)*

Subsystem or Component	*Equipment*		*Minimum Requirements for each Classification Notation*				
			DPS-0[1]	**DPS-1**	**DPS-2**	**DPS-3**[5]	*Remarks*
Power System	Generators and Prime Movers		Non-redundant	Non-redundant	Redundant	Redundant, in separate compartments[5]	See Subsection 3/3
	Main Switchboard		1	1	1 with bus-tie	2 with bus-ties, in separate compartments	See Subsection 3/5
	Bus-tie Breaker		0	0	1	2	
	Distribution System		Non-redundant	Non-redundant	Redundant	Redundant, in separate compartments	
	Power Management[2]		No	No	Yes	Yes	
Thrusters	Arrangement of Thrusters		Non-redundant	Non-redundant	Redundant	Redundant, in separate compartments	See Subsection 4/3
Control System	DP Control: Number of Control Computers		0	1	2	2 + 1 in backup control station	See 5/3.5
	Manual Position Control: Joystick with Auto Heading		Yes	Yes	Yes	Yes	
	Manual Thruster Control		Yes	Yes	Yes	Yes	See 4/9.5
	Position Reference Systems		1	2	3	2 + 1in backup control station	See Subsection 5/11, 10/3.3, 10/5.5, 10/7.3
	Sensors:	Wind	1	2	3	2 + 1 in backup control station	
		MRU[3]	0	1	3	2 + 1 in backup control station	
		Gyro	1	2	3	2 + 1 in backup control station	
	UPS		0	1	2	2 + 1 in separate compartment	See Subsection 3/9
Backup Control Station for Backup Unit			N/A	N/A	N/A	Yes	See 5/9.3
Consequence Analyzer			No	No	Yes	Yes	See Subsection 5/13
FMEA			No	No	Yes	Yes	See Subsection 2/11

Notes:

1 **DPS-0** is an ABS system class. It is a manual position control system fitted with automatic heading control and with a free-standing position reference system. **DPS-1**, **DPS-2** and **DPS-3** are in line with IMO equipment class 1, class 2 and class 3, respectively.

2 If all thrusters are direct diesel drive, a power management system is not required.

3 *(1 November 2013)* If position reference systems are dependent on correction of the measurements for roll and pitch noise, their associated MRUs are required.

4 *(1 November 2013)* For enhanced system (**EHS-P**, **EHS-F** and **EHS-C**), additional information is provided in Section 8, Table 1.

5 *(1 November 2013)* Where "separate compartments" is indicated, the equipment is to be located in separate compartments arranged to support the worst case failure design intent in respect of **DPS-3** failure criteria.

Apart from the general requirements above mentioned, the ABS Guide for DP systems has sections dedicated to each essential DP system: Power Systems, Thruster System, Control System, and Auxiliary Systems. Given the focus given to IPS in this thesis work, only the Power System requirements are here shown, if these have significant impact on system design.

3/1 The power systems are to be in compliance with the relevant Rules for vessel's mandatory classification notations (*AN: in this case, the ABS Rules for Building and classing Mobile Offshore Drilling Units apply* [26]). This Guide provides additional requirements for DPS-2 and DPS-3 notations in regard to redundancy and with respect to maximum single failure, as specified for each notation.

IMO MSC/Circ. 645 states:

- […]
- For equipment class 3 (*AN: equivalent to ABS DPS-3 classification*), the power system is to be divisible into two or more systems such that in the event of failure of one system, at least one other system will remain in operation. The divided power system is to be located in different spaces separated by A-60 class division. Where the power system are located below the operational waterline, the separation is also to be watertight. Bus-tie breakers are to be open during operations, unless equivalent integrity of power operation can be accepted.

The above criteria from IMO MSC/Circ. 645 are to be followed in the design of the power system for DPS-2 and DPS-3 systems.

3/3.1 Vessels with DPS-1 Notation

Generators and their distribution systems are, as minimum, to have the capacity to supply sufficient power to thrusters to maintain vessel's position within the specified operating envelope in addition to supplying industrial activities and essential ship service loads.

When power is shared, power supply to industrial activities and essential ship service loads is not to affect DP operations.

3/3.3 Vessels with DPS-2 Notation

In addition to the criteria above for DPS-1, generators and their distribution systems are to be sized and arranged for Worst Case Failure of any bus section. Sufficient power is to remain available to supply essential ship service loads, critical operational loads and maintain the vessel's position within the specified post failure operating envelope.

The post failure remaining power plant is to be able to start any non-running load without the associated voltage dip causing any motor to stall or its control equipment to drop out.

Essential services for generators and their prime movers, such as cooling water and fuel oil systems, are to be arranged such that, with any single fault, sufficient power remains available to supply the essential loads and to maintain position within the specified post failure operating envelope.

3/3.5 Vessels with DPS-3 Notation

In addition to the criteria above for DPS-2, generator and their distribution systems are to be sized and arranged in at least two compartments with a-60 and watertight boundaries so that, if any compartment is lost due to fire or flood, sufficient power is available to maintain position within the specified post failure operating envelope, and to start any non-running load without the associated voltage dip causing any running motor to stall or control equipment to drop out.

Essential services for generators and their prime movers, such as cooling water and fuel oil systems, are to be arranged such that, with any single fault in the systems or the loss of any single compartment, sufficient power remains available to supply the essential loads, the critical operational load, and to maintain position within the specified post failure operating envelope.

3/5.1 The switchboard is to be arranged for manual and automatic remote controls and be provided with all necessary alarms, controls and indications to allow local manual control of the power plant.

The distribution system at the main power generation level is to be arranged to reflect the split in the redundancy concept.

The split in the auxiliary power system is to follow the split in the main power generation system to match the worst case failure design intent.

[…]

3/5.3 For DPS-2 or DPS-3, the switchboard is to be designed such that no single fault will result in a total black-out, including failure of all equipment in any fire and/or watertight subdivision for DPS-3.

For DPS-2, a main bus bar system consisting of at least two sections, with at least one bus-tie breaker between any two bus sections, is to be arranged.

For DPS-3, each switchboard room is to be separated by watertight A-60 partitions. A bus-tie breaker on each side of the partition is to be arranged.

Bus-ties are to be designed to prevent a fault from propagating from one bus section to another.

When the DP system is designed including the configuration of closed bus-tie breaker, this breaker is to be:

i) A circuit breaker capable of breaking the maximum short circuit current in the connected system

ii) Coordinated in relation to generator breakers to avoid total loss of main power (black-out)

Minimum of two bus-tie breakers are to be provided and to be arranged such that a failure of one bus-tie breaker is not to result in a total blackout. […]

Consideration is to be given to effective intelligent detecting and executing methods featuring ultra-fast acting actions by the devices, including rapid communication to other protective systems under the coordination scheme, to prevent and/or mitigate the detected fault being migrating to other parts of the switchboard.

Bus bar control and protection systems are to be designed to work with both open and closed bus-tie breakers.

For DPS-3, in addition to the above requirements, the closed bus design is to include following

i) Power system protection as in 8/3.1.2(c) of this Guide

ii) Fault ride through capability. All equipment essential for dynamically positioning system are to have fault ride through capability, allowing for a short circuit condition to clear before under voltage protection is actuated. Low voltage transients during a short circuit condition are not to cause the motor starter to drop out, or other drives to fail.

3/7 The power management system is to be capable of operating with both open and closed bus-tie breakers where applicable. For a DPS-2 or a DPS-3 notation, where DP operations are configured with diesel electric driven thrusters, power management systems are to be provided. Power management systems may be of an individual designed type or integrated with other switchboard/generator control systems.

i) Power management system is to be capable of providing sufficient power for essential operations, and to prevent loads from starting while there is insufficient generator capacity. […].

ii) Consideration is to be given to techniques such as power limiting of heavy consumers, shedding of non-essential loads and temporary thrust reduction to maintain the availability of power. Total failure of the power management system is not to produce failure effects exceeding the worst case failure design intent and to be demonstrated through FMEA.

iii) Power management system is to be supplied with an uninterruptible power supply system (UPS).

iv) A failure in the power management system is to initiate an alarm in the DP control station. When the power management is disconnected, manual operation of the switchboard, […], is to be provided.

v) Loss of an online generator is not to result in the sustained overloading of the generators remaining on line. If sufficient power is not available, the power management system in conjunction with "controls" of consumers is to reduce system load in a coordinated fashion to restore power balance. The restoration of power balance may be accomplished by load reduction of specific consumers, load shedding and sectionalization of the electrical network.

vi) […]

vii) When the DP system is designed with a closed bus-tie configuration for DPS-2 or DPS-3, the power management system is to have protective measures implemented in order to provide the required integrity between the redundancy groups. The power management system is also to be able to communicate with other alternate protection systems if applicable. Analysis of relevant failure modes are to be addressed in the FMEA.

viii) For DPS-3 notation, the power management system is to be arranged such that no single fault, including fire or flood in one compartment, will render the power management system inoperable.

[…]

Analyzing the power system requirements, the design complexity of DP ship's IPSs is evident. The common practice until now was to rely on a well-proven design of a single power system section, and then apply redundancy at power system level, multiplying the same identical section two or more times. An example is shown in Figure 4 at page 9, where the connection of more equal power system sections to achieve a completely redundant power system is evident. Nowadays, the major driver is the improvement in vessel's efficiency, because the complete redundant power system concept applied until now implies excessive fuel costs. Indeed, to comply with rules and regulations the most common solution was the already mentioned division of the system in independent subsystems, to be used completely separated each other. Such a practice ensures high levels of fault resistance, but imposes to keep a number of active generators higher than the required. Moreover, this causes also an increase in the working hours for all the generators, which have to be kept running also when it is not necessary from the whole ship power balance point of view. This in turns increases maintenance costs, in addition to increased fuel costs. Due to that, major DP vessels shipbuilders and power system suppliers are starting to propose on the market new architectures, such as the Wartsila Low Loss Concept (LLC) [27] [28].

This thesis work does not propose system architectures or solutions able to improve IPS's fault resistance, or efficiency, but tries to give a methodology to improve system design. This can be seen as a tool to refine a ship's IPS design, whatever is the chosen design, to ensure its correct operation, and to remove unnecessary redundant components.

2 Conventional design process and its issues

2.1 Introduction

In this chapter, the conventional ship design process will be presented, together with a discussion on the design of Integrated Power Systems for All Electric Ships. Both will be discussed synthetically, to allow comprehending how such processes work. Moreover, examples of issues and criticalities caused by the conventional design process will be shown, in order to demonstrate the need of a change in the conventional processes, being it no longer able to address modern AESs IPSs design issues.

It has to be remarked that ship design is a complex process, involving different branches of engineering, teams of several designers, and relevant time and financial resources. Due to that, it is impossible to give a complete discussion of it in this thesis work. However, if more information about ship-design are sought, a good source is the book "Ship Design and Construction" [29].

2.2 Conventional design process

2.2.1 Relevant definitions in ship design process

To comprehend the complex process needed to design a ship, some definitions have to be given. In particular, in such an activity are involved several entities with well-defined tasks and related liabilities, which are peculiar of the marine sector. Moreover, the design activities could greatly vary depending on the extent of the design and the related building activity.

In the following, definitions and concepts about ship design are given.

Ship Design: The process by which, from a sea or inland waterways transportation problem, characterized by transporting a given flow of a given cargo type from point A to point B in a given time period, it is sized a vessel, specifying all of its systems, and it is developed the information necessary to build and assemble it.

The ship-design process can greatly vary, depending on the type of the project to be developed. The design process depicted in the following sections has been tailored on a completely new design, thus addressing the most complete process structure. However, other type of shipbuilding projects are possible depending on the peculiar application, with a reduction in design and building activities involved. Four types of projects can be identified, as follows:

Routine projects: projects that are not substantially different from the previous ones in the same class. The design process is limited to addressing possible differences in requirements/equipment desired by the owner (when their impact is limited). Building process is complete, due to the construction of an entire ship.

Creative projects: projects with substantial differences in the solutions applied in respect to previous designs, mostly caused by the introduction of new impacting requirements or equipment. The design process is extended to relevant ship systems, up to complete redesign of the ship, but indications on the feasible solution can be inferred from common designs. Building process is complete, due to the construction of an entire ship.

Innovative projects: projects with substantial differences in the solutions taken, due to the introduction of new technologies or challenging requirements. The design process is extended to the complete ship, requiring a complex activity to identify the feasible design. Building process is complete, due to the construction of an entire ship.

Refitting projects: projects dedicated to the modification of an existing ship, due to change in requirements from regulatory bodies, different application area from the owner (e.g. conversion of a dry cargo ship in an offshore supply vessel), or improvements in subsystems. The design process can greatly vary, depending on the extension of the refitting (it can span from simple subsystem's substitution, up to the cut of the ship in two sections to add a newly built section in between). The building activity is done accordingly to the extension of the refitting process. An example of the impact such projects can have on vessel's IPS can be found in [30] [31].

Several entities are involved in the process of building a ship, each with defined tasks and liabilities, as described hereinafter.

Ship Owner: It is the entity that starts and finishes the process. It may develop the concept design of the ship. It contracts the basic design whit the shipbuilder. It detains the property of the ship after it is built, although it is not necessarily the entity that operates it.

Designer: It is the entity which is responsible of the development of the basic design of the ship, and which prepares the related technical documents. It can be either an independent design office or a department of a shipyard. It can sub-contract the development of some parts of the design to other designers.

Ship builder: It is the yard building the ship. It is responsible towards the Owner for the compliancy to all the contract clauses and to the ship design given by the designer. It develops detailed design accordingly with its facilities and equipment/capacities. It can sub-contract other entities for both the development of some parts of the detailed design and building of some parts/sections of the ship.

Classification society: An organization that establishes and applies technical standards for the design, manufacture and maintenance of installations in marine field (regulatory body). Technical standards are developed by classification society, on the base of other relevant standards if applicable, and published in the form of Rules and Regulations. It has also a verification and classification function. Indeed, a ship built in compliance with the rules of a Classification Society can obtain from it a Class Certificate. The Classification Society gives such a certificate only after the approval of the design and a set of inspections during construction to check the design and building compliance. Classification Societies are important in marine industry, because their approval is related to the liabilities that arise in case of accident. Indeed, if a classified ship has an accident related with its design, the responsibility is lifted from the designer because it was compliant with rules and regulations (a similar condition happens in land power systems with IEC regulations).

National Authorities: State Authority that has the responsibility of conceding the Building License and of verifying the compliancy with international conventions (IMO, ILO, etc.) and relevant national standards, issuing the related Certificates. It can delegate such a work to other recognized institutions (the Classification Societies).

It has to be remarked that in Naval Architecture and Marine Engineering the terms *ship* and *vessel* are not equivalent. In fact, the term *vessel* is more general than *ship*, because it includes all the possible floating structures (such as ships, barges, platforms, etc.). In this thesis, such terms will be often used as equivalent, to ease the comprehension. However, this is an incorrect practice and should be discouraged.

2.2.2 The ship design process

The process of designing a new vessel generally starts from a ship-owner need. Ship-owners continuously monitor the maritime market, to identify new business opportunities. When such opportunities appear, ship-owners start the decision process that will possibly lead to the acquisition of a new vessel. An analysis of the business opportunity and available ships in the ship-owner's fleet is done, to assess the best method to take advantage of the emerged opportunity. A concept design is conceived, to define the ideal vessel that will be the best suited for the application. Such a vessel can be either present on the market or not, so a study of the possible alternatives is made, to assess which is the best course of action to take. The results of such a study can vary, depending on the current ship-owner fleet and the market. Five alternative decisions can result:

- Relocation of a ship from the existing Owner fleet;
- Freight of a ship;
- Acquisition of an existing ship (2nd hand);
- Refit of an existing ship;
- Building of a new ship.

If the ship-owner decide to build a new ship, the design process can start. A diagram of all the stages of the ship design process is shown in Figure 7, to help in comprehending the process flow [32]. For each design phase are also highlighted the results of the activities done into it, to explicit the flow of information developed in each phase and the consequent data transferred to the following one. The first step is the basic design phase (divided into concept, preliminary, and contract design). In the diagram of Figure 7, two different subdivisions of basic design and product engineering (detailed design) are given. This has been done because the functional stage is the bridge between system-oriented phases (thus basic design) and component-oriented phases (thus detailed design). Due to that, functional design can be either grouped in basic design or detailed design, depending on the preferences of the single analyst. However, such a distinction is not relevant to the aim of this thesis work, and no further discussion is done about it.

Similar decision process happens in Navies, where the decision to acquire a new ship is done when it is identified a gap in the overall Navy operational capability. In this case, the gap can be either due to the application of new operational roles for the Navy (such as humanitarian assistance), or due to the presence of new threats (e.g. new weapons systems developed by enemy forces), or due to fleet modernization needs. Similarly to what happens in merchant area, an analysis is done to identify the best way to fill the emerged gap. Once the concept design is defined, the following steps generally proceed almost in the same way as in merchant area [33].

Once the decision to build a new ship is taken, a designer has to be chosen. This can either be independent or a department of a shipbuilding yard. The designer develops the preliminary design, which is used to estimate the main ship data. The preliminary design is a significant design step, because it is used as a starting point for the negotiation of the new ship's construction with the shipyard. Indeed, preliminary design allows estimating ship building and exploitation costs, and can be used as a base to request quotations from different yards. Once a yard is selected, the contractual phase starts, where owner and yard negotiate the terms of the contract and the requirements of the ship to be built.

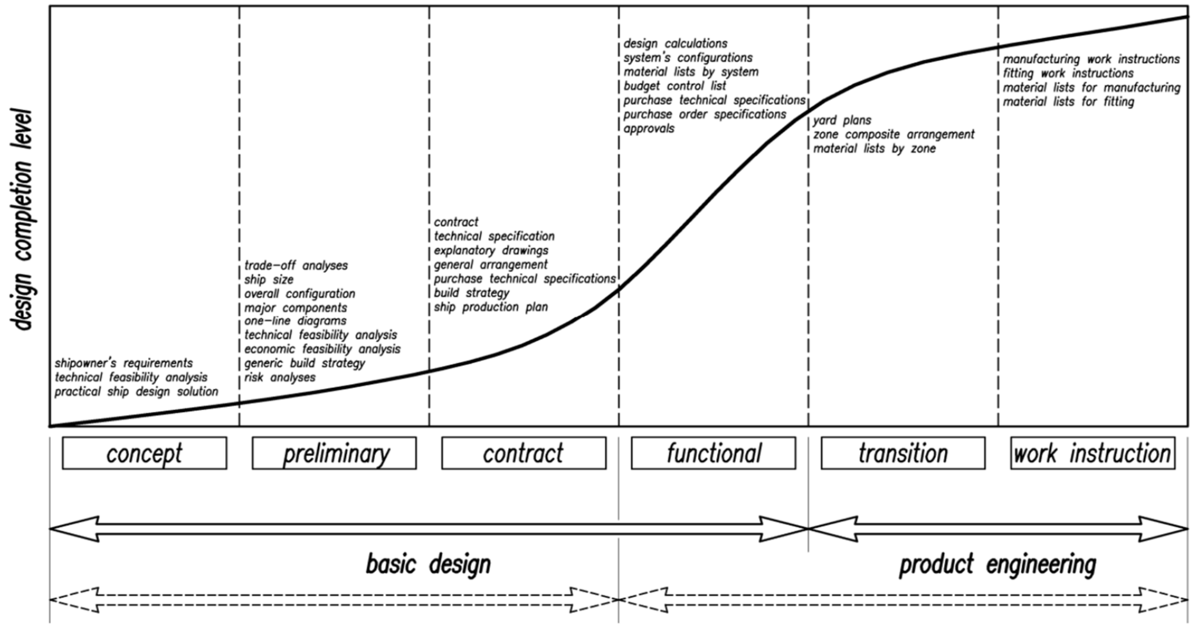


Figure 7 - Ship design process [32].

The selection of a particular yard can be made evaluating several different variables. Not only the quotation for the new ship to be built, but also other parameters affect such a decision: the reputation of the shipyard, eventual commercial agreements between yard and suppliers, presence of peculiar contingencies (e.g. US Navy ships are mandatory built in USA yards), and so on. The negotiation between owner and shipyard concerns both building and service costs (because both the shipyard and the components/subsystem's suppliers have obligations in respect to the owner also after the ship's delivery). One significant term of negotiation are the ship's requirements. In fact, the requirements deeply affect the design, with an extension that cannot be measured without knowing how a vessel is designed. As an example, a single designer, with several possible propulsion solutions, can easily address a maximum cruise speed requirement. Conversely, compliance with SRtP regulation imply the work of a dedicated designer team already from the first phases of design, because such a requirement involve the precise topological placement of several vessel's subsystems, with consequent impact on resources to be dedicated to design process. In fact, negotiation on requirements is important for the ship design process, because less requirements are imposed (or, equivalently, looser the requirements are), more freedom the designers have, making it simpler and faster the achieving of a feasible design.

During the contractual phase, the designers use preliminary design to develop the contract design. Contract design is a set of documents related to the ship to be built that define its design following the contractual requirements. Both the owner and the applicable classification society evaluate the contract design, in order to assess compliance with contractual and regulatory bodies' requirements. If the contract design is compliant with the requirements, the shipbuilding process can start, supported by dedicated design activities. After the signature of the contract, the design process prosecution is matter of the shipyard. However, ship-owner continues to interact with the yard, following the entire ship design and building processes to verify their correctness, and to assess promptly any discrepancy with the requirements.

The previous design activities have defined (and verified) the general ship arrangements, the subsystems to be integrated onboard, and the ship body. At this point, it is possible to start the detailed design phase. During this phase, all the documents and drawings needed to effectively build the ship are produced and given to the yard, in order to start the acquisition of the materials and to initiate the ship construction process. Detailed design (or product engineering) can be divided into sub-phases, which are functional design, transition design, and work instruction.

Functional design is dedicated to the definition of all the ship's subsystems. Relevant calculations are done and proper configurations are chosen. This phase is the last phase in which choices about systems to be installed onboard is made, because the following phases are dedicated only to the production of documents for the yard. In this phase, all the materials and components to be acquired are defined, and purchased accordingly.

During transition design phase the ship is divided into zones in accordance with the established building strategy. Workshop drawings, material lists and arrangements are documented for each zone, allowing the shipbuilder to start organizing the construction of the ship.

Work instruction phase is dedicated to the production of the instructions needed to correctly assembly (if purchased) and manufacture (if built "in house") all the ship's components. The result of this phase is a manual for the construction of the ship, starting from the base components acquired by the shipbuilder. Thanks to these instructions, the shipbuilder can correctly assemble the ship. Ideally, this is the last stage of ship design, but in fact it is not. Even if a detailed design is fully specified, engineering and design work may be necessary during the construction phase. Indeed, problems commonly arise during vessel's building, either caused by errors in design or by discrepancies between documental and real data. Due to that, modifications during construction are done, and as-built documents and drawings are produced. Once the vessel is built, tests are done with the aim of assessing its compliance with the requirements (the so called sea-trials). Finally, ships is delivered to the owner.

The depicted design process (Figure 7) is generally valid for most of the ships. Still, differences can be present depending on ship's complexity (e.g. a cruise ship vs an aircraft carrier) and on the design extent (e.g. new ship vs refitting of an old vessel). Moreover, also knowledge, skills, and number of the involved personnel affect design process, as well as the design tools and the priorities defined in the contract (e.g. cheap ship vs costly ship).

The most challenging aspect in the design of complex systems, such as ships are, is related to how the design process works, starting from conceptual design up to detailed. In fact, it is during conceptual design that the most impacting decisions are taken, using a limited amount of information with a high data uncertainty. Conversely, as the detail of the design increases the degrees of freedom are reduced more and more. Such an issue is driving towards new design concepts, conceived with the aim of including into the early-stage design of the ship tools able to assess the future impact of design decisions. These tools are system simulations and computer aided modeling [32] [34].

The design resulting from the above-depicted complex multi-stage process is commonly a balanced and feasible design. However, it may or may not be the optimum design for the ship. In fact, defining the optimal design for a ship is a complex matter strictly depending on the definition of "optimum" (the choice of the parameters to be maximized during ship design drives the design). The design of a ship implies designing a high number of interrelated subsystems, making the obtaining of the optimal solution more a matter of luck than of designers' competence. Due to this, current research is focused on finding design methodologies able to identify the optimal design solution for a given problem. However, each methodology requires being supported by appropriate software tools, which allow finding automatically the optimal solution for a given problem (such as internal systems' arrangements). This is leading to an evolution in ship design, from the nowadays computer aided design to a computer driven design concept. However, such an evolution has not yet reached the designers, whose diffidence towards new tools and technologies is commonly high. Similar behavior is common in industry, being the major obstacle to possible improvements. Nevertheless, some "enlightened" companies, or even other related entities, open the way to these innovations dragging the rest of the industry with them. An example of such a behavior is the US Navy, whose recent funding are focused on integrated and optimized design for its vessels. Such a behavior is causing an increase in research in the area and a subsequent modernization in related shipyards, which are obliged to adopt the innovative tools if they want to continue working with the Navy.

2.2.3 Ship design methodologies

Modern ships are complex systems, whose design cannot be done by a single person anymore. Indeed, the entire design project exceeds the capabilities of a single person, thus being necessary to split the work among several designers' teams. To do that, it is necessary to breakdown the overall design into sub-designs, each dedicated to a specific subsystem or aspect. Obviously, such sub-designs retain interrelations between them, thus being necessary to consider them during design. As a result, each sub-design process is correlated to the others and the optimal solution is not apparent. In fact, in complex systems the overall optimal design solution rarely is the composition of the optimal solutions of the sub-design processes. Due to that, the division of the design into sub-designs has to be done carefully, trying to achieve an optimal subdivision able to limit the interrelations among them and at the same time limiting the number of sub-processes to be done [35]. The most common subdivision criterion that is applied in ship design is the division by functions: hull structure, propulsion plant, electric plant, auxiliary systems, and so on.

Once the proper subdivision is achieved, a design methodology has to be applied, thus defining the process used to achieve the overall design solution through the sub-designs application. Several design methodologies can be found in literature; the most relevant three are briefly explained in the following, starting from the most conventional up to the most innovative.

The Design Spiral: The conventional representation of the ship design process is a spiral (shown in Figure 8). In such a process, the sub-design activities are accomplished in sequence, starting with a general design in the first round and detailing it more and more in each round. By doing this, the information resulting from a design round can be used to improve the following round, both developing detail and guiding the sub-processes to a common target [33]. The design spiral process begins from a rough design and develops a feasible solution through iterations, adopting a trial and error approach. Due to that, each spiral can lead either to a refinement of the chosen design, or to a redesign of some sub-systems to solve previous design errors or wrong evaluations. The design spiral allows highlighting graphically the previously described design phases, easing their comprehension (see Figure 9). Although being the design process commonly used to explain the basics of ship design, the design spiral is not perfectly representative of how real ship design works. In fact, the sub-design activities have a certain level of independency among them, leading to the common development of more than one activity at the same time. Doing that, each activity can proceed independently up to the point in which they need information from another one, yet retaining an overall spiral process. An example of modern ship design flow chart is shown in Figure 10. In such a figure are highlighted the parallel activities occurring, starting from the conceptual design (*Marketing* in figure) to the detail design [36]. Obviously, the depicted process is not sufficient to achieve the final design, but some iterations have to be done. Nevertheless, to ease the comprehension of the figure only one round of the spiral is shown.

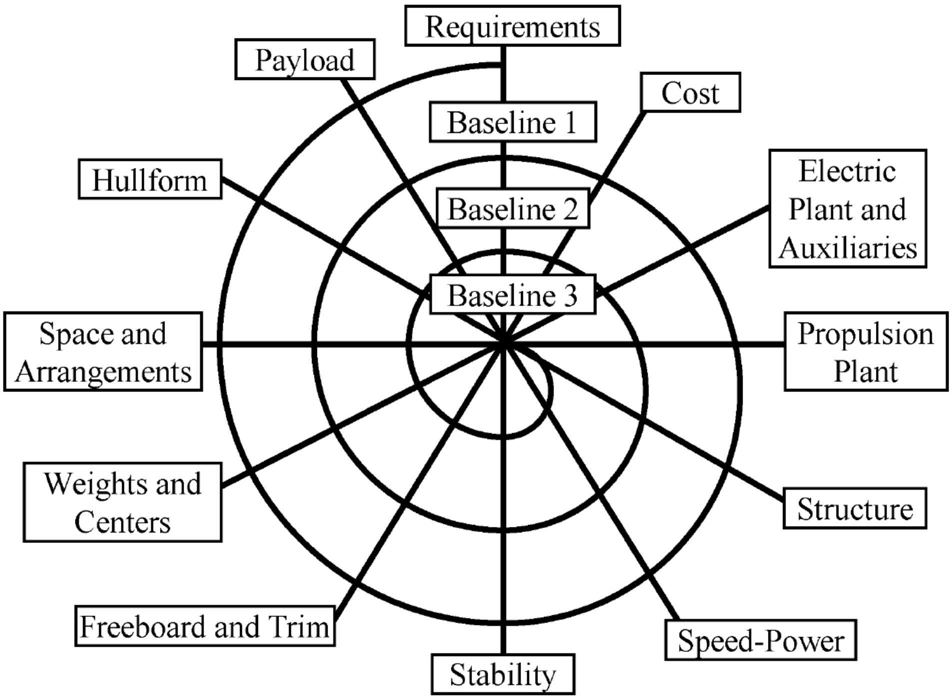


Figure 8 – Spiral vessel design process [33].

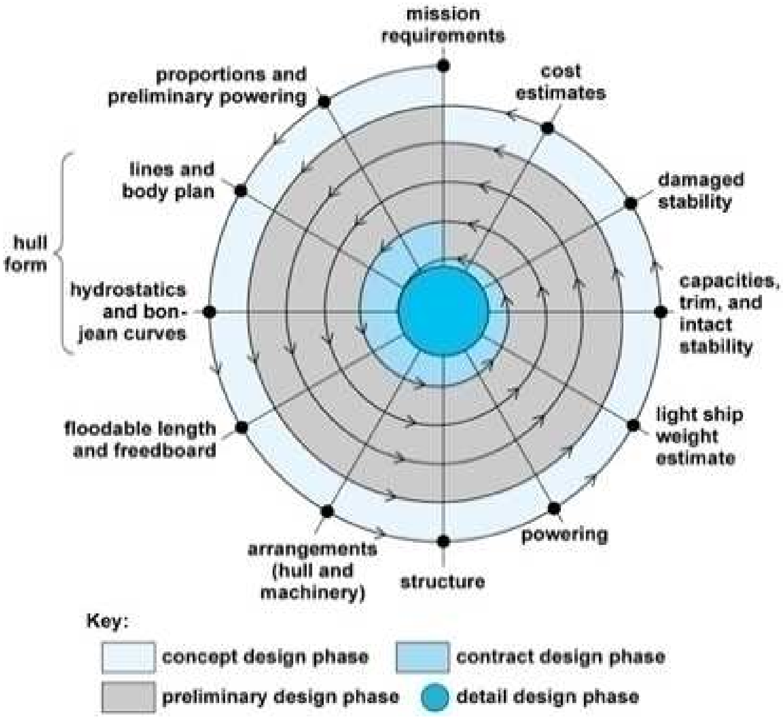

mission requirements
proportions and preliminary powering
cost estimates
lines and body plan
damaged stability
hull form
hydrostatics and bon-jean curves
capacities, trim, and intact stability
floodable length and freeboard
light ship weight estimate
arrangements (hull and machinery)
structure
powering
Key:
concept design phase
contract design phase
preliminary design phase
detail design phase

Figure 9 – Spiral vessel design process, design phases highlighted

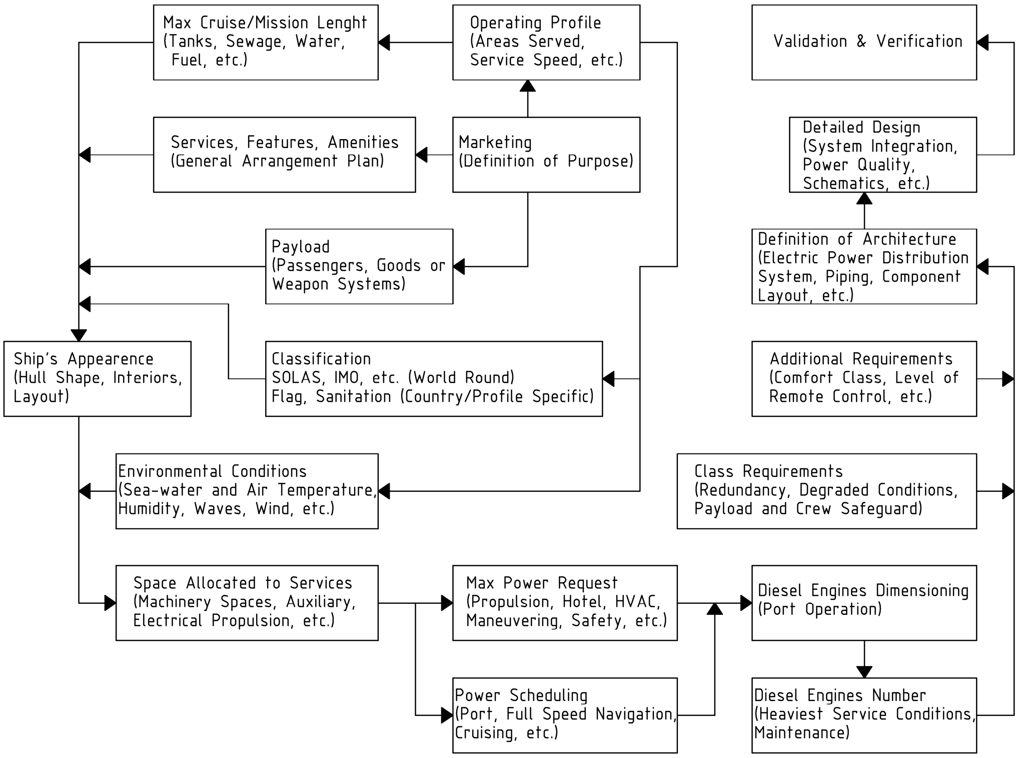

Max Cruise/Mission Lenght (Tanks, Sewage, Water, Fuel, etc.)
Operating Profile (Areas Served, Service Speed, etc.)
Validation & Verification
Services, Features, Amenities (General Arrangement Plan)
Marketing (Definition of Purpose)
Detailed Design (System Integration, Power Quality, Schematics, etc.)
Payload (Passengers, Goods or Weapon Systems)
Definition of Architecture (Electric Power Distribution System, Piping, Component Layout, etc.)
Ship's Appearence (Hull Shape, Interiors, Layout)
Classification SOLAS, IMO, etc. (World Round) Flag, Sanitation (Country/Profile Specific)
Additional Requirements (Comfort Class, Level of Remote Control, etc.)
Environmental Conditions (Sea-water and Air Temperature, Humidity, Waves, Wind, etc.)
Class Requirements (Redundancy, Degraded Conditions, Payload and Crew Safeguard)
Space Allocated to Services (Machinery Spaces, Auxiliary, Electrical Propulsion, etc.)
Max Power Request (Propulsion, Hotel, HVAC, Maneuvering, Safety, etc.)
Diesel Engines Dimensioning (Port Operation)
Power Scheduling (Port, Full Speed Navigation, Cruising, etc.)
Diesel Engines Number (Heaviest Service Conditions, Maintenance)

Figure 10 - Conventional ship design flow chart [36].

Collaborative, Concurrent Design: Modern vessels are complex systems, whose design process show some apparent paradoxes. Indeed, it has high degrees of freedom due to the possibility to achieve a single function in several different ways, but at the same time, the interrelations between each subsystem are significant, making nearly impossible to modify a subsystem without affecting the others. Due to that, the spiral process depicted above cannot address anymore the needs of a modern ship design. In fact, modern systems' design imply a movement around the design spiral in both directions in order to achieve an initial design which is well-balanced already in concept stage. Once the concept design is identified, all the sub-processes should work in parallel exchanging information through all the design, allowing them to proceed together towards the common target. Such a design process is called "collaborative, concurrent design" [33]. As it is evident, collaborative concurrent design requires proper communications between the design teams dedicated to each sub-design due to the high amount of information exchanged throughout the process. Moreover, a good leading activity has to be done not only to keep the focus of each team on the common target, but also to ensure proper decision-making procedures. Indeed, due to the presence of interrelations among sub-designs the design of one sub-system can limit the degrees of freedom of other sub-systems. In such a case, a mediation has to be done, defining what results can be kept and when a redesign activity has to be done in order to take into account the presence of new limits given by other design activities. Such a design process can be represented as a set of areas, whose limit is pushed forward and back by the sub-design activities (depicted in Figure 11). Since not all the activities proceed at the same speed, areas have an irregular profile but collapse in a common point when the design able to comply with the requirements is achieved.

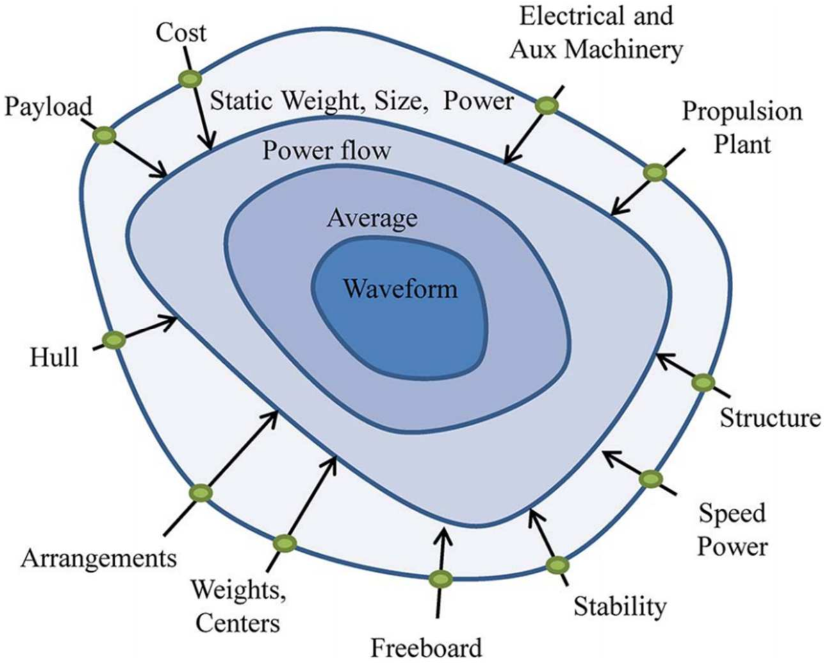


Figure 11 - Collaborative, concurrent design [33]

Design Space Exploration: Instead of selecting one possible vessel's design and then refine it through a spiral process or concurrent design, design space exploration focuses on the examination of a broad range of basic designs (defined at very low detail) to select the most promising for further exploration. The detail level of selected basic designs can be then improved and all the viable possibilities within these designs are explored, in order to select the most promising ones among them. Such a process proceeds until the best design solution is achieved [33]. Due to the extremely high number of design combinations, design space exploration can be achieved only through the aid of a computer software, which automatically synthesizes the design possibilities, calculates related attributes, and selects the ones complying with a predetermined set of requirements. As appears evident, such an approach is possible only through a complete shift towards a computer based design and implies the application of advanced optimization techniques (such as genetic algorithms, or particle swarm optimization) to achieve a feasible solution, limiting at the same time computational effort and calculation time. Due to that, design space exploration is an innovative design methodology not yet applied nowadays. Furthermore, it is unlikely to be applied in the short term with the possible exclusion of vessels with high added value (such as naval vessels).

2.2.4 Integrated Power System design process

The design processes depicted above are general, thus being valid for all kind of ships. When referring to All Electric Ships, the design of the Integrated Power System becomes a main concern. Indeed, the design of a power system able to correctly feed both propulsion and onboard loads is a complex task, especially if the goal is to obtain an optimized integrated design. Analyzing the spiral design process shown in Figure 8 it is possible to see two significant design steps: “Propulsion Plant” and “Electric Plant and Auxiliaries”. In an AES, these two sub-processes comprehend the design of the whole IPS, together with all its subsystems (such as propulsion, generation systems, power distribution, etc.). Therefore, it is important to analyze the IPS design sub-process in order to understand how a system of such an importance is designed. Moreover, such an analysis is significant because the innovative design process, topic of this thesis work, will be integrated in those sub-processes.

Similarly to what happens for the overall ship design, also IPS design can be done applying different methodologies starting from the simple spiral design to complex automated optimization processes. To allow comprehending the IPS design process and the related issues, in the following discussion it is considered the simple spiral design, shown in Figure 12 [7].

The IPS design process begins with the estimation of the so-called “electric loads balance”, which is a list of all the electric loads to be installed onboard. Such loads are weighted using appropriate load factors to account for both the ship’s operating conditions and environmental conditions. The result is a matrix depicting the expected amount of electric load to be supplied by generators for each possible ship’s operative condition and environmental condition, propulsion included.

Electric loads balance is then used, along with other impacting requirements (such as SRtP or classification societies regulations), to define rating and number of generators to be installed onboard. Commonly, those two parameters are selected trying to achieve the maximum efficiency in all the operative conditions of the ship, while maintaining the compliance with requirements from rules and regulations. Obviously, also installation costs and occupied onboard space have to be taken into account (and have to be reduced as much as possible).

The total electric power generation capability installed onboard drives the main bus voltage selection, while frequency is usually defined by the ship’s area of operation. Voltage is kept as low as possible to limit electric machines costs and volumes (which depends on electric insulation level), while keeping fault current levels within the limits of commercially available protection devices.

The selection of the plant configuration is the following step, which is in practice the design of the power system to be installed onboard. Obviously, the power system design has to take into account requirements from Rules and Regulations, applicable laws, and Owner. Due to that, IPS architecture generally is chosen between some configurations already validated in the past to decrease the design effort. Such configurations depend on the scope of the vessel to be built: some examples of IPSs have been depicted previously, both comprehending conventional and peculiar distribution systems.

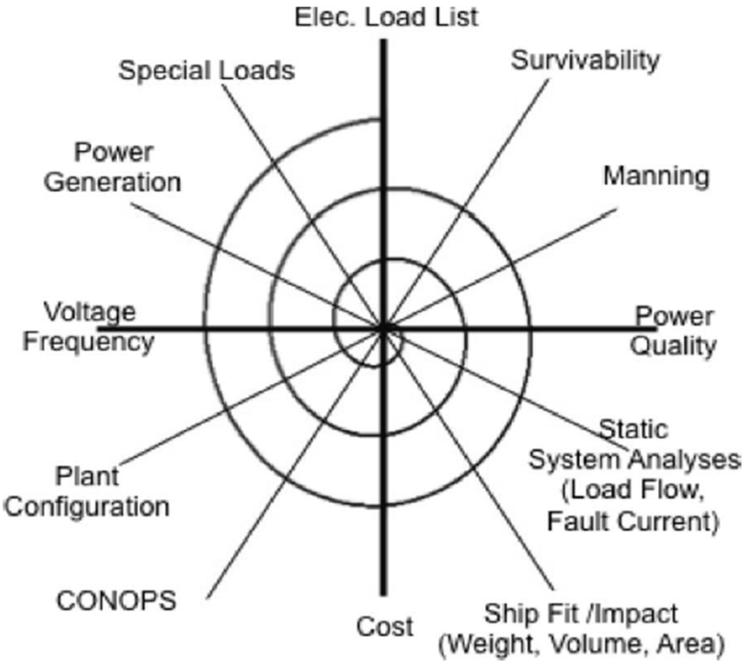


Figure 12 - IPS design spiral process [7]

In this regard, it has to be remarked that complex distribution systems are applied only when the eventuality of a black out (due to internal or external causes) is to be avoided as much as possible (such as in naval vessels or dynamic positioned ships). Otherwise, simple radial configurations are preferably used. Apart from the presence of high power propulsion converters and generators, the power system detailed design is similar to industrial power plants design, therefore little attention will be given to it in this thesis work.

After the design of the power system other activities are done, depending on the ship's scope of work. The activities dedicated to cost and ship fit impact evaluations allows assessing the impact of the designed IPS respectively on the project budget and on the rest of the ship. Results from these activities are used to adapt the ship to the designed IPS if possible, or to start an IPS redesign activity if the results are not compliant with the requirements. When an acceptable compromise is achieved the IPS design can be considered concluded.

However, other activities are done such as Static System Analyses and Power Quality assessment. In this regard, a concise but complete overview on common studies and analyses performed onto onboard electrical system can be found in [37]. Such analyses are mainly used as verification and to obtain data used to set system control systems and protections, thus being not used to achieve results able to aid in designing the IPS. This happens because IPS design is done already taking into account the expected results of these analyses, so failing in meeting the required results commonly happens only in case of a totally wrong design. Obviously, a failure in meeting one or more requirements can happen in real world, but if the design is well done the analysis results are only slightly outside the imposed limits and the issue can be solved with limited effort and impact.

2.3 Issues and Criticalities of Conventional IPS Design Process

2.3.1 Conventional design process issues and criticalities

The conventional design process is the result of an evolution in ships' design lasted centuries, started when ships became so complex to exceed a single person's design capability. Such a process demonstrated its validity until nowadays, being capable of addressing the issue of designing such a complex product with an organized and analytical approach. However, nowadays the need to integrate new systems onboard and to comply with ever more strict requirements it is bringing out its flaws. Indeed, the conventional design process is suitable to the design of well-known systems, where the interrelations between subsystems are clear and easily addressable in advance. Conversely, in the case of new subsystems and innovative power system architectures, the knowledge of how their operation impact on the other systems and on the overall ship lacks, leading sometimes to unforeseen harmful consequences.

A wide range of problems can come from flaws in design process, from design errors not found during the verification phases to unexpected harmful interactions between apparently well-designed sub-systems. These defects can be found only during the final verification of the system, which is done on the constructed ship during the so-called Sea-Trials, or even never found until they cause harmful consequences. In the former case, solutions can be applied at heavy cost due to the need to modify the already built system, while in the latter the solutions can be applied only in new ships or in case of the ship’s refitting. Obviously, this can happen only if after the harmful event it is possible to investigate its causes and highlight the root cause, process that is not simple as it may seem.

To aid in comprehending why conventional process needs to be modified, in the following some examples of issues and criticalities coming from poor design and inadequate system analysis are shown, taken from both literature and the PhD student activity performed during the three years of course.

2.3.2 Integration issues

Integration issues refers to problems arising due to the wrong integration between well-designed sub-systems. Such issues can happen because sub-systems design is done separately, without taking into account the complex interrelations that appears between them when connected together. Due to that, well-designed sub-systems can lead to unexpected behavior when connected together, or faults in a system may lead to the failure of other systems that did not seem interrelated. Integration issues can be caused by innovative sub-systems (such as high power pulsed loads) on which poor expertise and little knowledge are available to designers, but can be also caused by well-known sub-systems if it is not given proper attention to their integration into the IPS during design. Examples of such well-known systems are propulsion systems and thrusters, whose operation greatly influence the IPS, and proper management of loads and generators by the PMS and their control systems [3] [38].

An example of poor system integration could be made referring to an electric accident occurred to a cruise ship during sea trials [3]. Such an incident was caused by two faults in subsystems that in turn highlighted a series of faults in design. Indeed, some evident relations between subsystems were ignored during design or deemed non-critical by designers. The two faults triggered such interrelations causing an unexpected blackout for the ship during a maneuvering operation. Such an accident is dangerous because an AES relies on electric power to keep its maneuverability. Losing electric power during maneuvering means having an uncontrollable ship moving only by inertia, situation dangerous because maneuvering operation is used commonly near fixed structures and other ships (e.g. the maneuvering operation is used to moor the ship at the pier).

The ship subject of this incident has a common IPS architecture with six generators, such as the one shown in Figure 1. The incident occurred during ship maneuvering, with three generators running and harmonic filters connected to main switchboards. Propulsion converters were in operation. The PMS recording of the incident is shown in Figure 13, where the currents of generators and propulsion converters are depicted (two current traces are shown for each propulsion drive, due to the presence of a 24 pulse converter using two three-windings transformers for each electric motor). Before the accident, the ship was in low load condition, which consisted mainly in the propulsion at low speed (due to speed limitations in maneuvering operation), five thrusters idling (waiting for maneuvering commands), some HVAC systems, and a very low hotel load (because of the presence on board of only the necessary personnel for tests). Due to such a low load, also the resultant Power Factor was low, requiring the connection to the switchboard of the harmonic filters not due to power quality issues but due to their power factor correction function. The first fault to happen was a malfunction in a PMS sensor, which impaired the PMS capability to sense a reactive overload on one of the generators. Such a fault was hidden (no alarm to crew or alternative sensing means) probably due to missing automatic verification of coherency from sensor results by the PMS. In normal conditions, such a fault poses no harm to the IPS but the second fault triggered an unexpected reaction. The second fault was the failure of the lubrication system installed in one of the two onboard power stations. Such a system was deputed to the lubrication of the bearings of all the diesel-generators of the power station, causing the subsequent failure and disconnection of two of the three running generators. The two generators disconnection is clearly visible in Figure 13 due to the instantaneous drop to zero of their output currents. Both the generators' disconnections caused the consequent disconnections of the harmonic filters by the PMS, in order to avoid reactive power overcompensation on the remaining generator. Moreover, an automatic reduction in propulsion power were applied, to avoid active power overload. Until this moment, the system behaved as expected: the PMS reacted to the faults applying the correct countermeasures. At this point, the fault in the remaining generator's sensor became relevant, leading the system to black out. Indeed, the automatic reduction in propulsion power was perceived by the ship's pilot but the causes were not yet found (as can be seen by the time scale in the figure, the accident happens in about three minutes). Due to that, the pilot required an increase in propulsion power to recover the drop caused by the faults. The PMS was meant to limit such an increase up to the capabilities of the remaining generator, but the faulted sensor caused the PMS to allow a higher amount of power absorbed by propulsion. Moreover, being unable to sense the reactive overload on the remaining generator, no filter was reconnected to the switchboard leaving the generator alone in supporting the power grid. This in turn caused the reactive overload of the remaining generator and the consequent power system voltage drop. At this point, generator's under-voltage protection triggered causing the ship's black out.

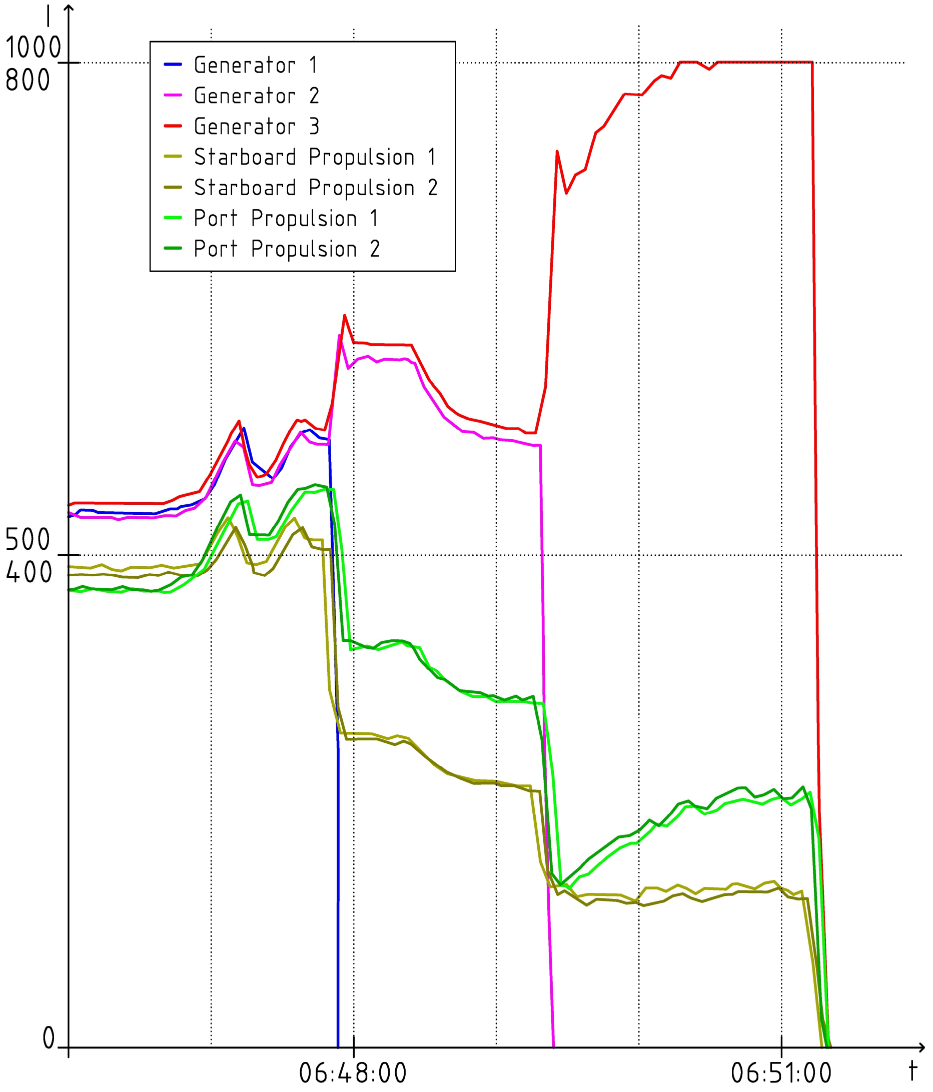


Figure 13 - Ship's PMS recording of an incident leading to blackout, generator (1000 A scale) and propulsion (800A scale) currents records [3]

Analyzing what happened, the causes of such an accident are obvious. The two faults have triggered unexpected interrelation between sub-systems that seemed well designed when analyzed alone: the generator, the PMS, and propulsion system. The most evident design flaw in this case is the common lubrication system, shared between the generators' of a single power station. If each generator had its dedicated lubrication system, the failure in one of them will have left untouched the remaining generators. Such an evident design flaw should have been easy to find during design but designers ignored it, maybe due to insufficient design verification or due to the costs of a separate lubrication system. (It is quite likely that the real cause will never be known outside the designer's office). However, also the sensor's fault is relevant and poses the attention on the so-called hidden failures: faults that are not sensed/signaled until they cause harmful consequences. In this regard, the last few years trend is to increase the PMS managing functions, sensors and actuators, acquiring more data from the system and acting more and more as an integrated platform management software. This allows lowering the possibility of such faults to go unnoticed due to the presence of coherency controls on sensors measures. Nevertheless, there is still way to go. The innovative design process proposed in this thesis work will allow finding such flaws before ship's construction, through a systematic procedure able to highlight each possible interaction between sub-systems.

2.3.3 Harmful interactions between real time control systems

During the description of the IPS design process, it was stated that the design of the ship's onboard power system is similar to land systems' design. However, some peculiar issues may arise due to both the reduced spatial extension of onboard power systems in respect to land systems and the IPS operation as an electric island. In fact, the former cause a reduced decoupling between onboard loads and sources, while the latter imply the absence of a power buffer able to stabilize the system during transients. Due to these, the IPS is not capable to remain as stiff as land systems during load variations, leading to wider voltage and frequency variations during transients. This specific character is addressed by Rules and Regulations by widening the ranges of acceptable voltages and frequencies variations both in steady state and during transient, as shown in the Table 1 depicted in the previous chapter (page 10). Nevertheless, respecting such limits is difficult despite their wide range, leading to the need of installing onboard high-performance real-time voltage and frequency controls. For what concerns voltage control systems, the performance given by standard AVRs is sufficient (equivalent time constant ≅ 0.5 s), while common SGs may result too slow (equivalent time constant ≅ 5 s) leading to excessive frequency drop when high power loads are connected to the grid. Depending on the characteristics of the ship, high bandwidth Speed Governors coupled with low inertia diesel generators may be needed to keep the IPS frequency into the limits imposed by the rules. This solution solves the issue of complying with requirements, but brings to light another issue related to the control systems' regulation bandwidths. Indeed, AVR and SG may interact, leading to unpredicted behavior of the generation system (mainly electromechanical instability [39]). Due to that, it is not possible to apply the common design practice used in land power systems, which implies consider the voltage and frequency control bandwidths well-separated and the consequent separate design of the two control systems. Conversely, AVRs and SGs design have to be done considering their interactions, both among themselves and with the power system, to guarantee their stable operation thus avoiding the rise of harmful situations [39].

Such an issue is peculiar of high performance AC IPSs, such as the ones installed onboard all electric naval vessels. Indeed, in such ships it is necessary the maximum propulsion performance to allow attaining the maneuverability level needed to make the difference between a successful or a failed mission. Due to that, high power load steps can be applied to the IPS due to the ship maneuvering operation leading to the need of high performance generation systems (including their controls). Instead, common ships have a less stressed power system due to the possibility to delay connection and disconnection of loads, to avoid the application of too high load steps, and to modify propulsion power more gradually due to their lower maneuverability requirements.

2.3.4 Voltage stability issues due to pervasive electronic power converters presence

The AESs were born when the electric propulsion met the electrification of the onboard loads. Nowadays, another evolution is in course: the progressive adoption of electronic power converters to supply the onboard electric loads. In fact, static power conversion has proven its usefulness, due to the possibility to achieve variable speed/torque operation for electric motors. Such a possibility allows removing mechanic and oleo-dynamic drives from the ship, both reducing maintenance costs and increasing safety. Also excluding this particular application, electronic power converters are still being adopted more and more in marine power systems, being they integrated in the UPS systems and in the new automation systems. Indeed, the use of power converters allows achieving higher performance, increasing redundancy, increasing reconfiguration options, and raising overall efficiency. Due to that, nowadays the electronic power converters are spreading more and more on ships, to the point of reaching a share of loads fed from converter higher than 80% (data taken from a modern cruise ship). However, such advantages are balanced by a significant drawback: the Constant Power Load (CPL) voltage instability. A CPL is defined as a load that tends to absorb a constant electric power from the power grid, in spite of the disturbances on the supply network, showing a nonlinear behavior. In fact, such loads increase the absorbed current when system's voltage drops, which is harmful for the voltage stability of the system. The CPL behavior is the downside of one of the main advantages of electronic power conversion: the ability to decouple the loads from the power supply, keeping constant voltages and/or currents supplied in spite of input variations. In fact, electronic power converters are able to achieve such a decoupling through a high control bandwidth, obtained setting accordingly their control law. However, if the control bandwidth is set too high the converter can behave like a CPL, applying a destabilizing action on the power system. Such a destabilizing action depends not only on the converter's bandwidth, but also on system parameters and working point. Indeed, the same converter can hinder the stability of a particular system (behaving like a CPL) while in another one can have no impact. CPL instability has been extensively analyzed in DC [40] [41] [42] [43] [44] and AC distribution systems [45] [46] [47] [48] [49] [50]. In the paper [50], two models to assess stability in AC power systems in presence of CPL loads are presented, and a simplified approach dedicated to early design stage assessment is given. In addition, case studies are shown, together with a discussion on system parameters influence and possible solutions to avoid instability. The results given and discussed in the paper clearly demonstrate the possibility of CPL voltage instability in AESs IPSs. Moreover, analyzing the references it is possible to infer that such an issue depends not only on the load supplied by the electronic power converter, but also on the supply system's parameters. This demonstrate the need of an IPS design process that is able to consider the system as a whole, and not as a bunch of separately designed sub-systems as conventional design does.

2.3.5 Insufficient analysis and verification during design phase

As can be easily seen at this point, the design of a ship is complex and flaws may happen regardless the attention given to them during design. For this reason, system analysis and verification have to be done particularly well, as to reduce as much as possible the possibility that some flaw goes unnoticed. Obviously, such need is in contrast with the available design times and resources (both human and financial). Due to that, the depth of the analyses has to be reduced to an affordable level, thus leaving possible flaws in the design. Some examples of critical flaws that could have been found and solved through a well-done system analysis are depicted in [51] and [18].

Regarding verification, the tests are commonly executed in two steps: the vendors test single subsystems during the Factory Acceptance Tests (FAT), while the correct operation of the ship is tested during Sea Trials by a team involving shipyard, classification society, and owner. In both these verification activities, the choice of the tests to do is left to regulatory bodies' requirements and verification staff's competence and knowledge. Owner may also specify in the contract some peculiar tests that are to be done on the ship's systems. Nowadays, both FATs and Sea-Trials are fairly standardized, thus implying the use of fixed routines and sets of tests chosen depending on the ship's scope of work. However, standardized test address common issues, leaving unverified a high number of possible harmful situations. Similarly to what happens with system analyses during design stage, such limitation in testing activities is to be done due to the understandable limits in the resources to be dedicated to verification. In fact, due to the complexity of a ship, testing all the possible harmful situations that may arise on it may require a time exceeding its life expectancy.

Although system analysis is not able to highlight all the possible flaws in the system, most of them can be found. Due to that, the innovative design process, goal of this thesis work, will integrate a detailed system analysis using the dependability theory, which is able to assess the interrelations between sub-systems (and between components) and to assess the effect of components faults on the overall system.

Conversely, the verification phase is not considered into the innovative design process because it is done after that the design is completed. However, dependability theory tools are capable to guide in the choice of the tests to be done on the system, focusing on the conditions that most probably will happen onboard.

3 Innovative distribution systems and new requirements

3.1 Introduction

Goal of this chapter is to present some innovative distribution systems and new requirements. Indeed, onboard systems are evolving from conventional radial AC distributions to new ones, on which no previous design experience is available. Moreover, new requirements from owners are creating new issues in ship design never faced before. The design of an IPS endowed with these new characteristics is difficult to face with common design process, pushing towards the need of a new methodology able to address the design of such an innovative systems.

In the following, these innovative distribution systems and possible new impacting requirements will be described, to allow comprehending the problems the designers are facing nowadays.

3.2 Innovative distribution systems

3.2.1 MVDC distribution

In recent times, the most advanced navies in the world are adopting the AES concept for their new vessels through the installation of Medium Voltage Alternate Current (MVAC) IPSs. To successfully design such ships navy designers have drawn largely from the knowledge gained in the merchant field. Due to that, in such ships the design effort has been put mainly on achieving high levels of reliability and to improve mission capabilities, starting from a well-known design base. Examples of the most recent naval vessels built using AES concept are UK Navy Type 45 and the abovementioned aircraft carrier HMS Queen Elizabeth, and the French/Italian FREMM frigates. Moreover, the use of hybrid-propelled ships (which have installed onboard both mechanical and electrical propulsion systems) is foreseen for all the new ships planned for acquisition by the IT Navy, exploiting the interest of Navies in AES concept. However, the nowadays adoption of MVAC systems is only a starting point for navies, because the struggle in achieving ever higher performance is pushing the research (on ship's power systems) towards new concepts, such as the Medium Voltage Direct Current (MVDC) distribution system. [44] [52] [53] [54]. In recent years, the research has been focused onto this topic mainly because of the financing of US Navy, whose interest in such a technology is major. Such a high interest is due to the advantages that can be given by DC distribution to naval applications. Still, some relevant issues are present, whose solving require both academic and industrial research effort.

A review of the pros of DC power distribution over AC one is given in the following:

a. Simplifying connection and disconnection of different types and sizes of power generation and storage devices;
b. Reducing the size and ratings of switchgear;
c. Eliminating large low-frequency (50 Hz or 60 Hz) transformers;
d. Limiting and managing fault currents and enabling fast system reconfigurations;
e. Eliminating reactive voltage drop;
f. Reducing power system weight by using high speed generators;
g. Enabling higher power ratings for a given cable size;
h. Enabling active power flow management, especially during transients and in emergency conditions;
i. Reducing fuel consumption by allowing variable speed prime mover operation;
j. Improving efficiency when energy storage is used;
k. Rationalizing power conversion stages;
l. Eliminating the need for phase angle synchronization of multiple sources and loads.

Most of these advantages are related to the high amount of electronic power conversion systems present in an MVDC system. In fact, conversion systems are needed in DC power system to allow their proper operation (as an example, in DC no simple static machines to change the voltage level are available). However, such a pervasive electronic power conversion presence leads to the main technical issue of MVDC power systems: the Constant Power Loads voltage instability issue. Such an issue has been already discussed in case of AC systems, in chapter 2.3.4 (page 45 ff.). In DC systems such issues is also present and depends on similar causes. Several research activities are aimed at solving such issues, applying different approaches. A good reference to such an issue, and methods to solve it, can be found in [55], together with relevant bibliography. In addition to that, MVDC systems present other relevant issues, which need to be solved prior their common adoption as onboard systems:

a. Difficulty in extinguishing DC arcs in the absence of a voltage or current zero crossing (issues in building appropriate breakers).
b. Definition of an effective grounding strategy to provide crew electric safety.
c. Lack of an established industrial base, being MVDC systems an insignificant commercial market nowadays.

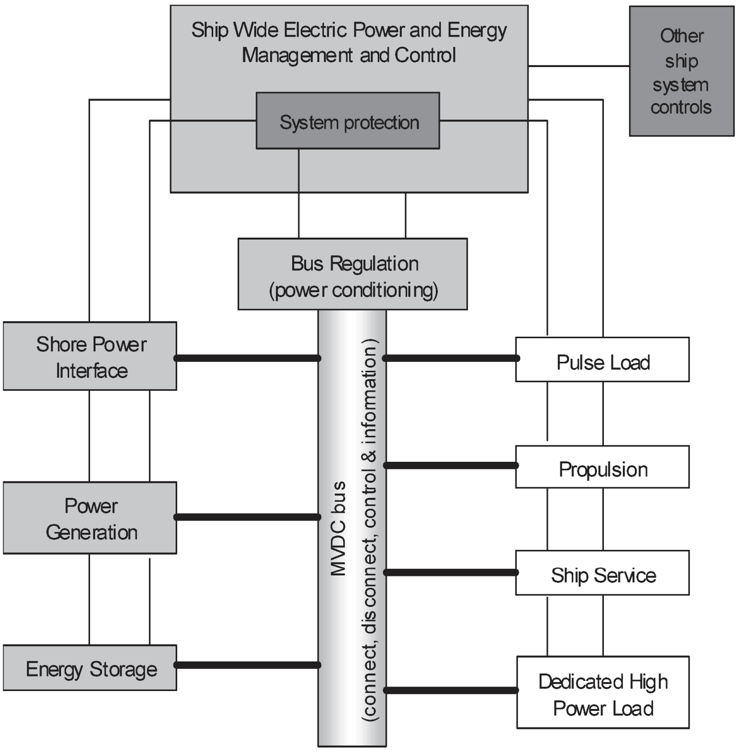
In particular, the last point is one of the most significant obstacles to the adoption of MVDC power systems. In fact, the absence of industrial partners able to supply the components needed to install an MVDC system leads designer to generally ignore such a solution for onboard distribution, which in turn discourages suppliers' investments in the MVDC sector.

Luckily, in order to exit from this impasse situation some major power components suppliers are starting investing in industrial research to put on the market products for the MVDC systems, because they see in such distribution systems a business opportunity.

To allow comprehending what might be an MVDC power system, a possible functional block diagram is depicted in Figure 14 [44]. The functional blocks can be defined as follows:

- Shore power interface: a power source that adapts electric energy from the utility system on shore to MVDC power system (e.g. transformer + AC/DC interface converter).
- Power generation: a power source that converts prime energy from fuel into electric energy, hereinafter adapted to MVDC (e.g. prime mover + generator + AC/DC interface converter). It may also be a fuel cell system.
- Energy storage: a system capable to store energy, taken from the system, in order to supply it back when needed (e.g. super-capacitor, battery, flywheel), used to face transient power unbalances and as an active filtering unit to improve Power Quality.
- Pulsed load: a load center that draws intermittent pulses of power from the power system, (e.g. electromagnetic aircraft launch system, rail gun, and free electron laser), generally a load specific to military area.
- Propulsion: a load center constitute by electric motors, supplied from the DC distribution bus through variable speed drive inverters, used to achieve the ship movement and maneuverability.
- Ship service: a load center that primarily draws power from the system to ship services (e.g. hotel load).
- Dedicated High Power Load: a load center that draws high amount of power from the power system (1 MW or more of power in steady-state operation) (e.g. military radar, large thruster, compressor).
- Ship-wide power and energy management control: PMS conceived to maximize the continuity-of-service of vital loads during reconfiguration operations, optimizing the power flows throughout the ship.
- System Protection: DC system protection is achieved through a combination of converter control and other DC circuit breaking devices (e.g. solid-state DC breakers).
- MVDC bus: the ensemble of busbars and breakers of the MVDC system, allowing its division in sub-sections.

As aforementioned, the MVDC power system foresees the extensive use of power converters [56]. Indeed, each electrical power source and each load must be interfaced to the MVDC bus via converters, as clearly shown in the hypothetical notional MVDC power system with radial architecture shown in Figure 15. This enables innovative functionalities to be integrated in the converters, such as short circuit protection integrated directly into the converter, or fast reconfiguration, now never used in industrial applications.



Ship Wide Electric Power and Energy Management and Control
System protection
Other ship system controls
Bus Regulation (power conditioning)
Shore Power Interface
Power Generation
Energy Storage
MVDC bus
(connect, disconnect, control & information)
Pulse Load
Propulsion
Ship Service
Dedicated High Power Load

Figure 14 - Functional block diagram of MVDC power system [44].

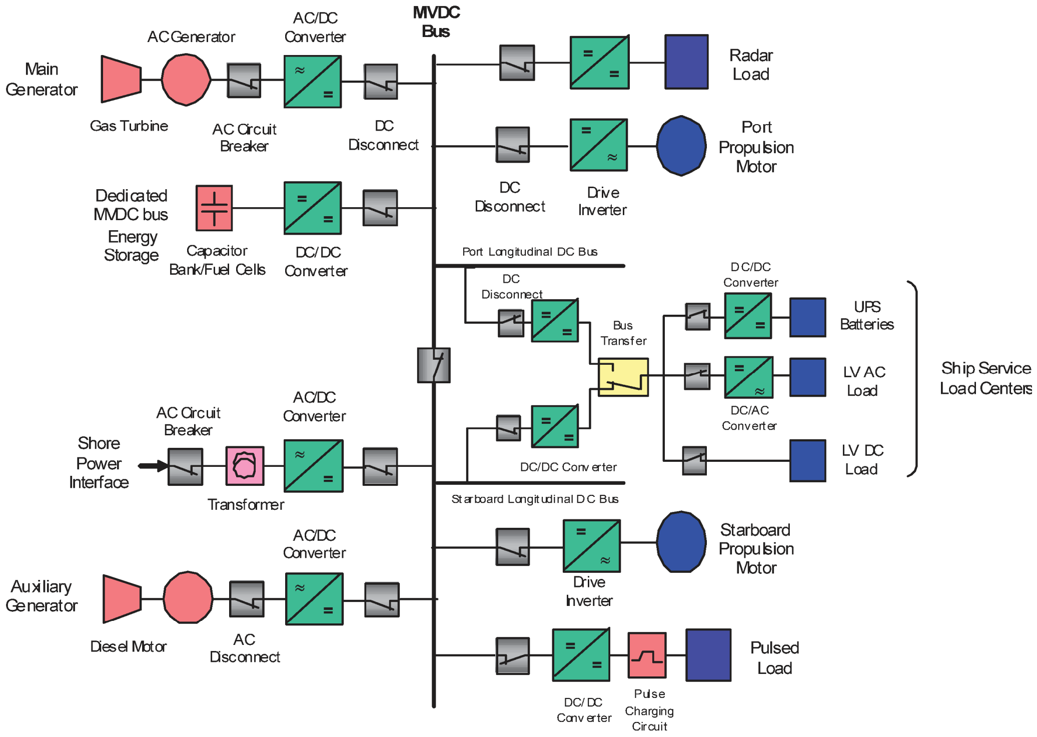


Figure 15 - MVDC radial distribution [44].

Such an innovative power system requires new tools to be designed due to the absence of prior knowledge. Moreover, components never used before are foreseen to be installed in MVDC systems. This leads to the need of a design process that is able to infer the impact of all these new components on the overall system and which can help designers in comprehending how such systems are supposed to behave. In this regard, the innovative design process proposed in this thesis work can help designers in building a ship endowed with an MVDC power system.

3.2.2 Zonal distribution

Besides conventional radial distribution, which is the standard in shipboard applications, and ring distribution, which is scarcely used onboard ships, another distribution topology emerged recently: the zonal distribution. Zonal Electrical Distribution Systems (ZEDS) mimic in small scale the meshed distribution used in land power systems, with some modifications due to the different scopes of the two. In fact, shipboard zonal distribution is conceived to maximize the continuity of service ensuring at least two different and independent power supply inputs for loads. A notional diagram of a zonal power system is shown in Figure 16, while Figure 17 depicts the single zone electrical block diagram [57]. IEEE Std. 1826 collects the standard practice for power electronics open system interfaces in zonal electrical distribution systems rated above 100 kW and it is the baseline on which such systems may be designed [57]. The blocks included in the block diagram, taken from such a standard, can be described as follows:

- External-to-bus conversion:

  The external-to-bus conversion element has the functions of
  a) Preventing fault propagation to the external power system or other zone(s) due to faults within the zone;
  b) Preventing faults observed on the external interface from propagating to the in-zone distribution bus;
  c) Converting power received through the external interface from the external power system or other zone(s) to the power type needed for the in-zone distribution bus;
  d) Converting power from the in-zone distribution bus originating from in-zone energy storage or in-zone generation to the power type needed by the external power system or other zone(s) via the external interface (optional).
  ZEDS may have multiple external-to-bus conversion elements to interface with one or more external power systems or other zone(s).

- In-zone distribution bus:

The in-zone distribution bus provides a means for the exchange of power among external-to-bus conversion, in-zone energy storage, in-zone generation, and bus-to-internal conversion. The in-zone distribution bus may be totally enclosed within the boundaries of a single equipment cabinet or distributed throughout the zone. The in-zone distribution bus may be segmented into multiple buses.

- In-zone energy storage:

  An in-zone energy storage element stores electrical energy received from the in-zone distribution bus that later may be used to provide power back to the in-zone distribution bus. An in-zone energy storage element is an optional element of the ZEDS. In-zone energy storage is typically employed to achieve QoS (Quality of Service) requirements but may also fulfill power quality and other system requirements. An in-zone energy storage element shall protect the in-zone distribution bus from faults internal to the in-zone energy storage element.

- In-zone generation:

  An in-zone generation element converts fuel into electrical energy to provide power to the in-zone distribution bus. An in-zone generation element is an optional element of the ZEDS. An in-zone generation element shall protect the in-zone distribution bus from faults internal to the in-zone generation element.

- Bus-to-internal conversion:

  A bus-to-internal conversion element converts electrical power from the type and quality of the in-zone distribution bus to the type, power quality, and QoS required by end-use devices or distribution panel elements. A bus-to-internal conversion element shall protect the distribution panel from faults internal to end-use devices, connected power cables, and distribution panel elements. A power system designer may optionally design the bus-to-internal conversion element to provide regenerative power produced by end-use devices to the in-zone distribution bus.

- Distribution panel:

  A distribution panel element accepts power from the bus-to-internal conversion element and distributes the required type, power quality, and QoS to multiple end-use devices. The distribution panel element shall protect the bus-to-internal conversion element from faults internal to end-use devices and power cables. The distribution panel may include power conditioning.

- End-use device:

  An end-use device is typically an electrical load. It does not connect directly to the in-zone distribution bus. It also may be a source. It is provided power from or may provide power to one or more distribution panel elements or bus-to-internal conversion elements. To prevent catastrophic failure due to the end-use device fault, a back-up disconnect system may be necessary.

As can be easily seen from the above list, ZEDS imply an extended use of power conversion in order to achieve its expected advantages. Due to that, issues like the CPL voltage instability discussed in Sections 2.3.4 (page 45 ff.) and 3.2.1 (page 49 ff.) may happen. Moreover, the major advantage of a zonal architecture (which is the possibility to have several different power sources, energy storage systems, and external power supply paths) is also its main disadvantage. Indeed, such a degree of freedom implies an inherent difficulty in defining the optimal configuration of the system. To allow achieving the most from ZEDS a complex automation system is required, able to continuously monitor the system and perform optimization algorithms to dynamically set the system near its optimal point of work (the definition of "optimal" obviously depends on the requirements of the system: the goal may be the efficiency, or the resiliency to faults, or both).

ZEDS are a promising solution for shipboard power systems when Power Quality or Continuity of Service requirements became stringent (IEEE Std. 1709 depicts also a zonal version of its notional MVDC power system, shown in Figure 18). However, their use is also foreseen for land Micro-Grids, where the ZEDS concept allows the integration of active users and renewable power sources in a systematic way. The design of such systems lacks a standardization due to its novelty, and the presence of a high number of active components opens the path to unforeseen issues caused by hidden interrelations among them. Due to that, the proposed design process could be used also in this case, to help in designing both shipboard and land based ZEDS.

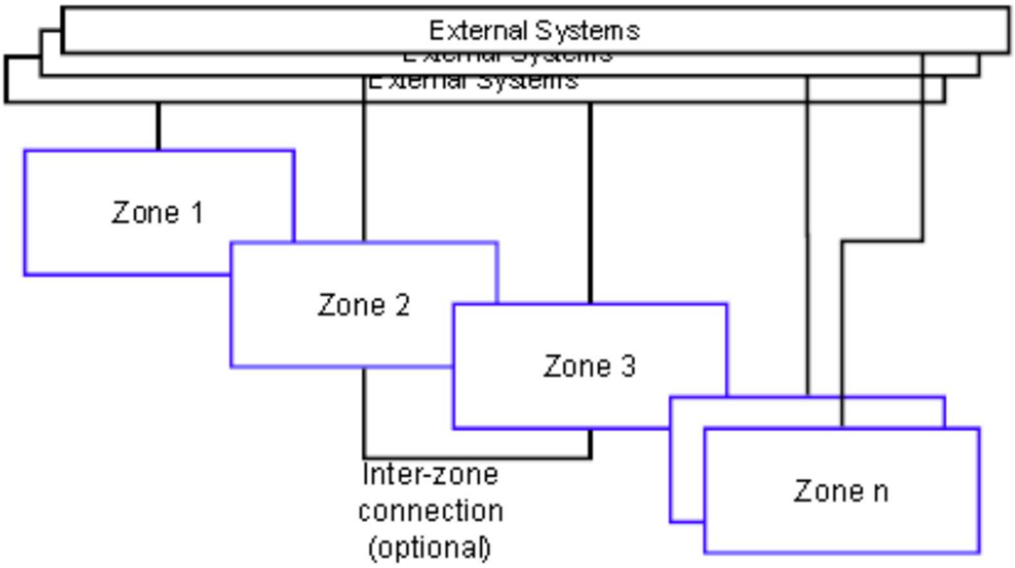


Figure 16 - Notional diagram of a zonal power system [57].

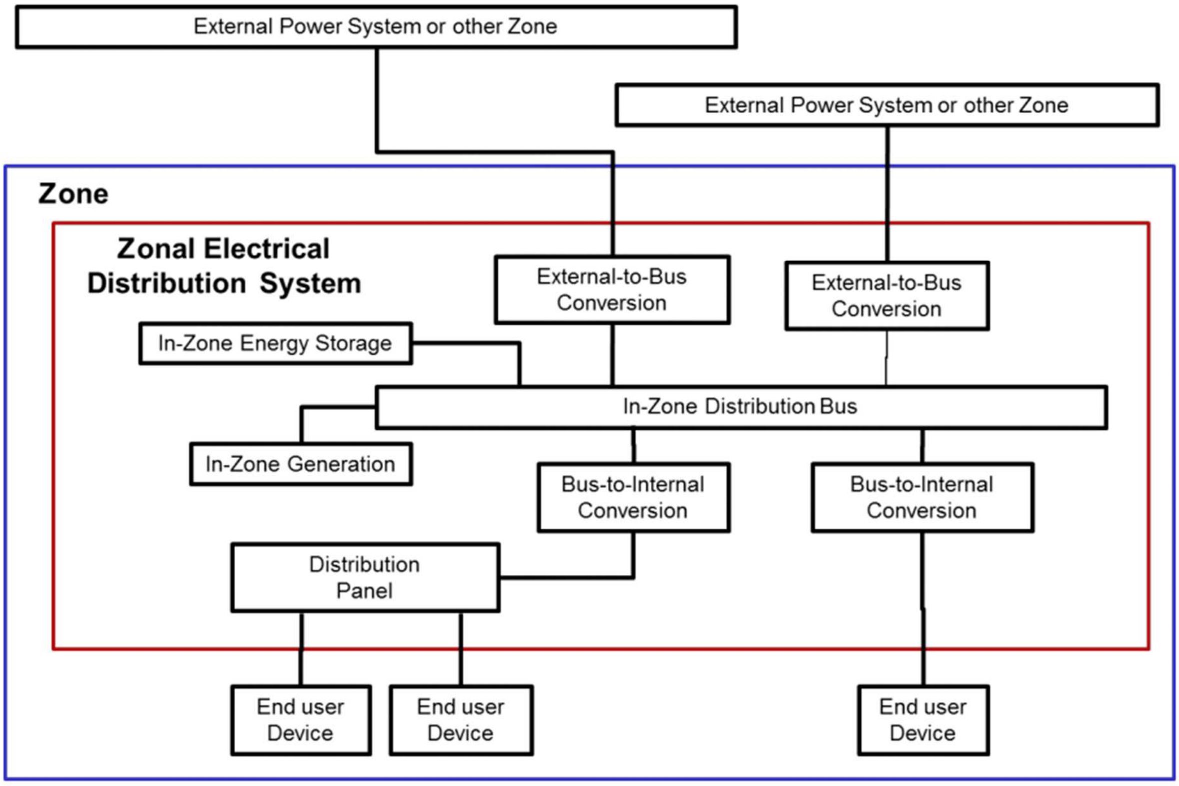

External Power System or other Zone
External Power System or other Zone
Zone
Zonal Electrical Distribution System
External-to-Bus Conversion
External-to-Bus Conversion
In-Zone Energy Storage
In-Zone Distribution Bus
In-Zone Generation
Bus-to-Internal Conversion
Bus-to-Internal Conversion
Distribution Panel
End user Device
End user Device
End user Device

Figure 17 - ZEDS, single zone electrical block diagram [57].

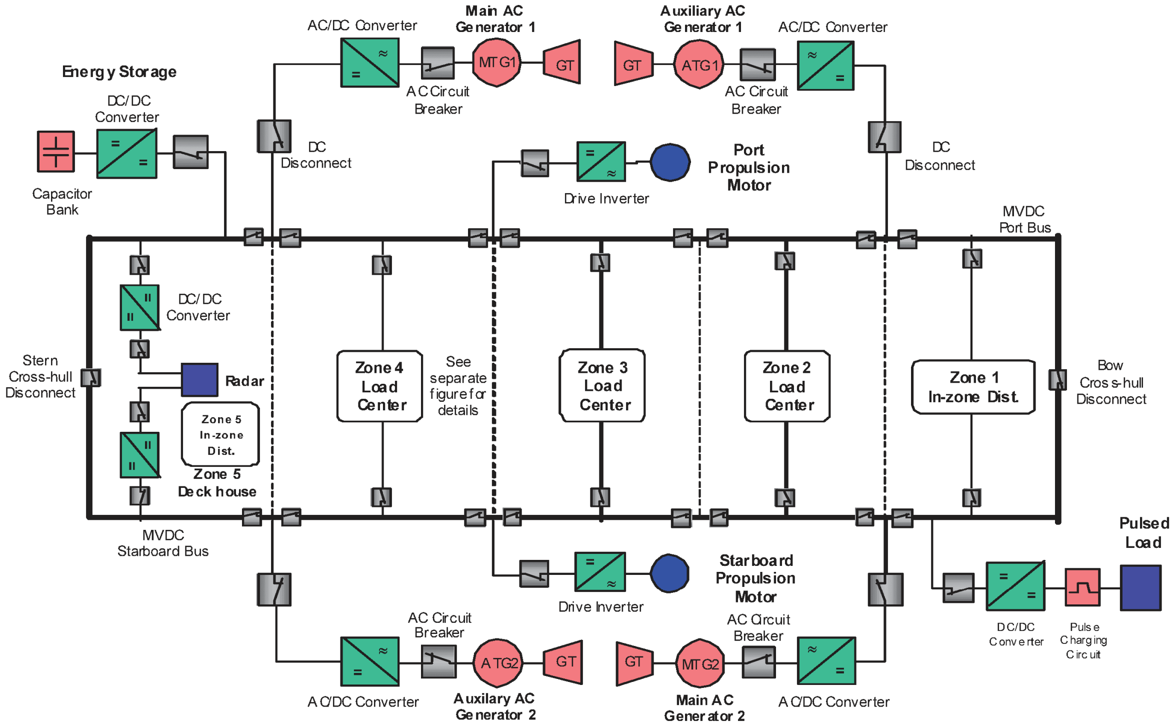


Figure 18 - MVDC zonal distribution [44].

3.2.3 Mixed AC/DC distribution

Section 3.2.1 described concisely the shipboard MVDC distribution system. Such an innovative system is yet to be installed onboard a ship, tough several land based demonstrators have been built worldwide and are currently used for the de-risking of such a technology. A less complex but still innovative technology is the use of the LVDC (Low Voltage Direct Current) for the secondary power distribution, coupled with a conventional MVAC main distribution system. Such a solution allows achieving some of the advantages of the MVDC distribution, making it possible both the integration of a zonal distribution for the essential loads and attaining a high Power Quality for sensible loads. A notional scheme of a mixed MVAC/LVDC power system is shown in Figure 19 [58]. As can be seen, the main distribution is a conventional MVAC system, while DC is applied for the low voltage zonal distribution thus enabling fast reconfiguration actions, high power quality, active control of power flow, and easy integration of energy storage systems. This allows achieving most of the advantages of both the DC systems and the zonal distribution architecture, mainly for the loads that mostly will benefit from them: the essential loads (e.g. navigation and communication subsystems for merchant ships, radars and electronic warfare systems for naval vessels). At the same time, mixed MVAC/LVDC distribution system lowers the requirements for the DC section, making it possible to build a fully operational system already with nowadays technology. In fact, a ship endowed with such a distribution system has been built and its sea trials are in course now: the US Navy guided missile destroyer USS Zumwalt (DDG-1000) (Figure 20) [19]. The design and construction of such a ship has required many years, and issues arisen during the construction led to several in course modifications causing a dramatic increase in the cost of the ship. Due to that, the US Navy limited the number of ships that will be built to three, from an initial number of thirty-two. Even IT Navy is financing research on such a topic as demonstrated by the Naval Smart Grid research project [59]. The aim of such a research project is to obtain results that can be used to define guidelines for the new design of IT Navy AESs. In particular, the possible use of mixed AC/DC distributions is foreseen, as a way to achieve both improved mission capabilities and innovative weapon systems supply. The results are presented in form of guidelines, to be used as an aid to define operative requirements. Such guidelines are aimed at the integration of the best actual technologies with the future ones. In particular, the goal of the project is to obtain research results useful to:

- emit new operative requirements;
- design electric propelled vessels endowed with an IPS;
- identify the most effective actual technologies which can be used for the definition and the engineering of the new requirements;
- integrate the best actual technologies with the technologies research activities future results.

Mixed AC/DC power systems can be a solution to achieve some of the DC advantages, at the same time avoiding the lack of MVDC components on the market. However, as US designers learnt with the DDG-1000, also an architecture with lower design impact than full MVDC distribution can present unforeseen issues, leading to the need of a new design process able to assess such issues as soon as possible.

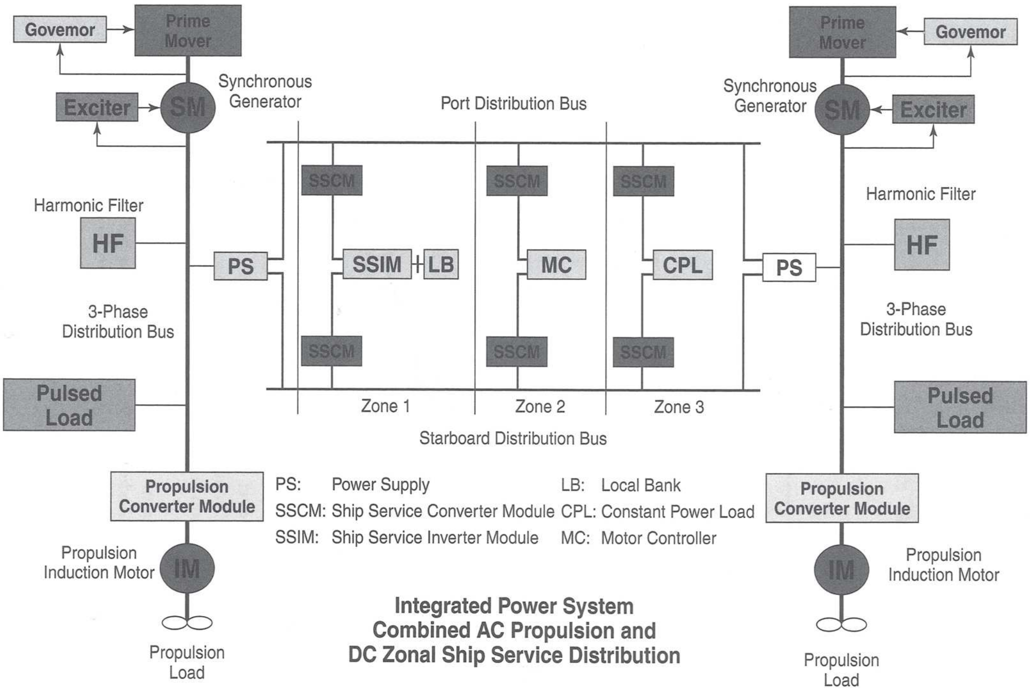
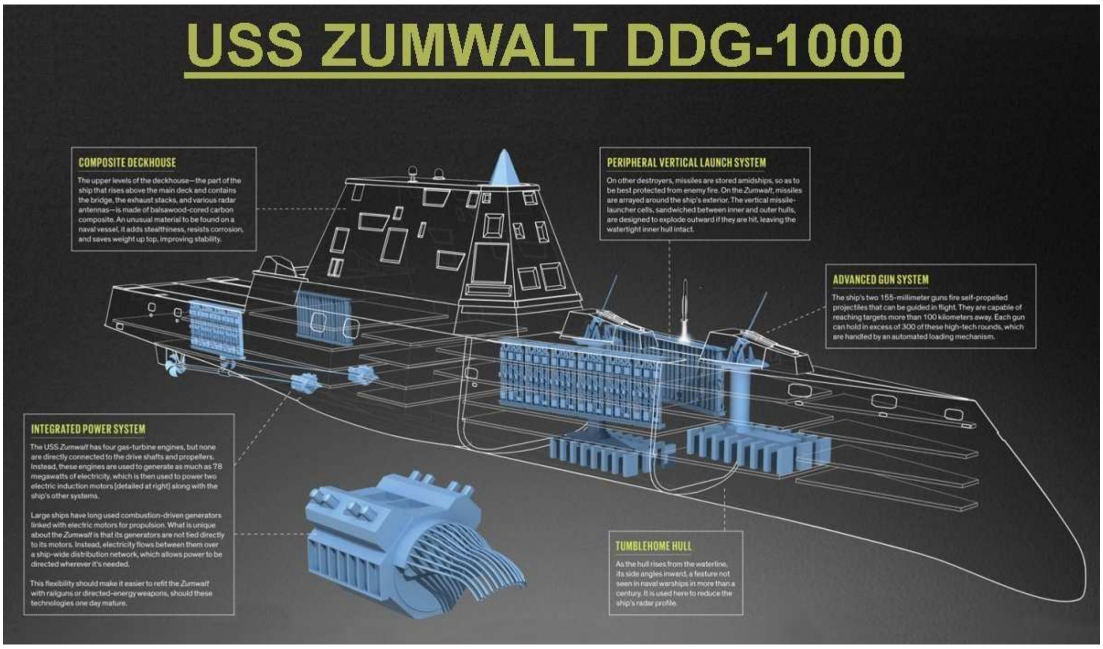


Figure 19 - Notional mixed MVAC/LVDC integrated power system [58].



COMPOSITE DECKHOUSE

The upper levels of the deckhouse—the part of the ship that rises above the main deck and contains the bridge, the exhaust stacks, and various radar antennas—is made of balsawood-cored carbon composite. An unusual material to be found on a naval vessel, it adds stealthiness, resists corrosion, and saves weight up top, improving stability.

PERIPHERAL VERTICAL LAUNCH SYSTEM

On other destroyers, missiles are stored amidships, so as to be best protected from enemy fire. On the *Zumwalt*, missiles are arrayed around the ship's exterior. The vertical missile-launcher cells, sandwiched between inner and outer hulls, are designed to explode outward if they are hit, leaving the watertight inner hull intact.

ADVANCED GUN SYSTEM

The ship's two 155-millimeter guns fire self-propelled projectiles that can be guided in flight. They are capable of reaching targets more than 100 kilometers away. Each gun can hold in excess of 300 of these high-tech rounds, which are handled by an automated loading mechanism.

INTEGRATED POWER SYSTEM

The USS *Zumwalt* has four gas-turbine engines, but none are directly connected to the drive shafts and propellers. Instead, these engines are used to generate as much as 78 megawatts of electricity, which is then used to power two electric induction motors [detailed at right] along with the ship's other systems.

Large ships have long used combustion-driven generators linked with electric motors for propulsion. What is unique about the *Zumwalt* is that its generators are not tied directly to its motors. Instead, electricity flows between them over a ship-wide distribution network, which allows power to be directed wherever it's needed.

This flexibility should make it easier to refit the *Zumwalt* with railguns or directed-energy weapons, should these technologies one day mature.

TUMBLEHOME HULL

As the hull rises from the waterline, its side angles inward, a feature not seen in naval warships in more than a century. It is used here to reduce the ship's radar profile.

Figure 20 - USS Zumwalt (DDG-1000) most innovative characteristics [60].

3.3 New requirements

3.3.1 Navies innovative applications

In Chapter 1.4 (see page 12 ff.), the most demanding application of AESs was deemed to be DP vessels in merchant area and naval vessels in military area. While DP vessels have been addressed extensively due to their use as a case study during this thesis work, very poor information has been given about naval vessels. In fact, military area is financing innovation in AESs IPSs sector, mostly because navies need IPSs to supply some of the most advanced weapon systems in course of development, or either as a technology able enabling new functionalities that will have a significant impact on ships' mission capabilities. Such an interest has been already discussed during the previous sections, when MVDC and mixed AC/DC distribution systems have been described. In this section other significant motivations that are leading Navies in financing research in this field are given, focusing on peculiar requirements of new naval IPSs and innovative sub-systems to be installed onboard.

Pulsed loads

In their vision of next future, the most advanced navies include new weapon systems and advanced sensors. In fact, research on these innovative systems is in course, with a secrecy level related to their strategic importance, but sufficient information are known among researchers to make it possible to state that such systems are coming. Indeed, there are already working prototypes of such weapons, some of which are being installed experimentally on some ships of the US Navy. These new systems not only comprehend several types of electric powered weapons (for example railgun, laser, etc.), but also high power radars and new sensor systems. Despite the great differences in both the scope and operation of these new proposals, all of them are electric powered. To give an idea of the magnitudes involved with such systems, a list of the main innovative systems being developed, with their estimated characteristics is shown in Table 4 [61].

These systems, in addition to the high power required have another feature that distinguishes them from common loads: they are pulsed loads. This means that the continuous power absorption of such systems is relatively reduced but at regular intervals (for sensors) or when fired (for weapons) such loads have an absorption peak (which reaches the values show in Table 4) for a very short time (from a few milliseconds up to values in the order of seconds). Due to the peculiarities of shipboard power systems, this behavior stresses the IPS in such a way to impair the Power Quality down to levels below the requirements. Such an issue can be clearly seen in Figure 21, where it is shown the effect of the operation of a pulsed load on a conventional AC power system. Therefore, although being characterized by an amount of energy manageable without problems from the IPS (high power absorption but a short time of application means low energy), these types of loads require special considerations in order to be fed without affecting the overall system operation.

Table 4 – Hypothetical specification of innovative high power weapon systems [61].

High Power System	Required Power [MW]	Weight [t]	Occupied Surface [m²]
Radar Area Surveillance	4	70	137
Radar BDM Surveillance	17	250	272
Rail Gun	60	152	110
Laser (Medium Power) Point Defense	2	21	12
Laser (High Power) Missile Defence	60	65	297

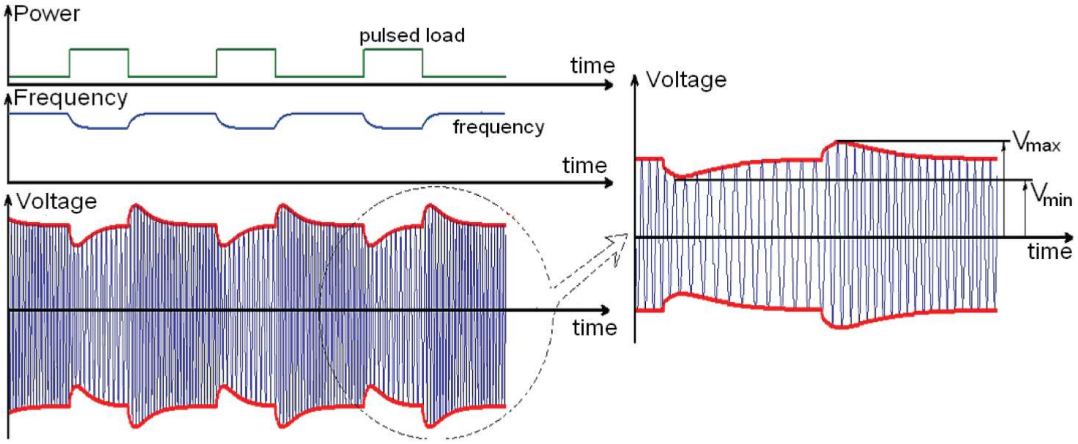


Figure 21 – Impact of a generic pulsed power load on an AC power system [38].

As stated above, it is very difficult (if not impossible) to directly connect a pulsed load to a shipboard IPS without affecting heavily the performance of the electrical system. Therefore, studies on pulsed loads in power system area are addressed to reducing their impact on the IPS to acceptable levels. (Studies are in course on technological aspects of such loads, such as materials with high mechanical resistance also at high temperatures for railguns, but are outside the scope of this thesis work.)

The most frequently applied solution is the use of a power buffer. Such systems, which may be built using several different technologies, are interposed between IPS and load. A power buffer supplies the electric power required by the pulsed load, supporting the absorption peaks using internal energy storage systems, while drawing in a constant level of power from the grid. By doing so, it is possible to decouple the pulsed load from the rest of the IPS, thus ensuring the maintenance of a proper Power Quality on the system in spite of the presence of the pulsed load. This solution seems to be the most promising one, and it is capable of providing adequate performance. Therefore, most of the researchers are focused on this topic.

However, in case of installation of such systems on an already existing vessel, an analysis has to be done to ensure the ability of integrating them into the IPS and to determine the possible refitting to be done. To correctly integrate them, not only designs and schematics have to be examined, but also the real IPS of the vessel. In fact, modifications on the IPS done a posteriori, possible discrepancies between design data and real data for single components, and components variations due to aging leads to the need of assessing IPS state before designing a possible refitting. This can be done through a dedicate measurement campaign, such as the one presented in [10]. With the measurement campaign data it is possible to tailor the interventions to be done on the vessel's IPS, ensuring the best integration of the innovative weapon system, thus allowing increased mission capabilities for naval vessels.

Ship-to-shore connection

In the last years, the onboard installed generators' power have increased, mainly due to the increase in electric loads and the adoption of hybrid (or even full electric) propulsion. This has been caused by the necessary modernization of naval platforms, whose requirements nowadays include both the increase in efficiency and some activities less related with defense, such as humanitarian mission support. Due to this, the most recent naval vessels present not only a relevant amount of electric power generation capability, but also extensively use the High Voltage Shore Connection (HVSC) to avoid keep running onboard generators during port operations [62], [63], [64]. The combination of high installed power capabilities with a shore connection opens the way for a new highly innovative concept: the supply of land loads by the ship power system through the HVSC (Figure 22). Indeed, a reversible shore connection enables new applications tactically relevant for the navies. As an example, the ship power could be used to supply a field hospital in a seashore area during humanitarian missions, or also to supply a military mobile base. A ship-to-shore connection can be easily implemented when an HVSC is already foreseen, allowing achieving new functionalities with a reduced effort. The conventional use of shore-connection is already covered by the existing IEEE-IEC-ISO joint standard on HVSC [65], whilst the case in which power is delivered from the ship to the land is not. The use of high voltage (in reference to shipboard power systems, high voltage is nominal, phase-to-phase voltage above 1 kV) for the connection point out electrical safety issues for both the ship-to-shore system and the distribution system supplied. Therefore, proper evaluations about grounding for both high and low voltage sections have to be done to ensure the safety of all the users involved, considering also that the IPS must ensure correct operation for onboard loads regardless what happens on land side. Despite being conceptually simple, the possible adoption of a ship-to-shore connection imposes to assess design and safety items, requiring case study analysis. Ship and land power systems grounding, selectivity, and equipment design must be properly assessed. Moreover, the different situations that can be found in land power systems (to be supplied by the ship-to-shore connection) require a certain degree of flexibility to adapt connection equipment, while keeping an inherent high safety level for both shipboard and land users. These issues need a detailed analysis and a careful evaluation, to assure the applicability and the successful utilization of the ship-to-shore connection concept. Such an analysis has been done in [66], resulting in a possible feasible solution. In fact, the ship-to-shore connection is a requirement for all the new classes of ships whose acquisition has just been planned by IT Navy: 1) a new Landing Helicopter Dock (LHD), which will be able to deliver up to 5 MVA; 2) a new Logistic Support Ship (LSS), to deliver up to 2,5 MVA; 3) a new class of Multi-Purpose Offshore Patrol (PPA), to deliver up to 2,5 MVA. Due to that, ship-to-shore connection system is in course of design, and the solution depicted in [66] will be the most probable to be used. However, the installation of such a system onboard a ship requires a careful evaluation of both the IPS design (to correctly integrate the shore-supply function) and the internal ship arrangements (to find the space where the new components have to be installed). IT Navy solved the second issue with a movable container based solution, while other installations can need the most extended onboard integration possible. However, the integration of such a functionality into the IPS needs rethinking its design, to ensure correct operation of the IPS, crew electric safety, and supplied land system safety.

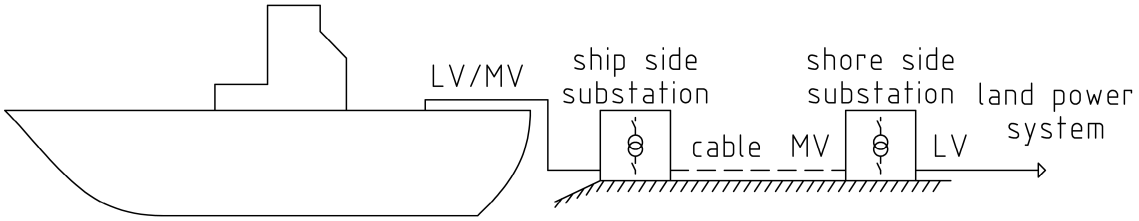


Figure 22 - Ship-to-shore connection [66].

3.3.2 Standardization of innovative power systems

A significant issue related to innovative systems is the lack of standardization. Indeed, regulatory bodies commonly emit requirements based on standards and regulations widely accepted but innovative systems may have components/parts not covered by any (or only partially covered). Due to that, not only designers, but also the others entities involved in vessels' design and construction lack a standard practice to follow. This is an issue because it implies not having a legal definition of which are the requirements needed to define the correctness of the design. Moreover, it limits the application of such technologies because there is no indication on how correctly integrate them into a product. This leads to the need of a standardization work, which is actually in course in parallel with the research (and which may require more work than the one needed to develop the innovative system).

Commonly, standards are written by technical experts in the related field, and can be based on industrial practice (if the system is well proven), or industrial research results (if an innovative system is addressed). Proper research activity, when coupled with wide experimental validation, can origin new standards or contribute to the modification of already present ones. In this thesis work some of the applicable standards are given, when relevant. However, for some of the innovative systems and requirements discussed in the present chapter standards are lacking, thus a work of standardization has to be done in parallel with the dedicated research activity.

An example of such a practice is the IEEE Std. 1709 [44], concerning recommended practice for MVDC shipboard power systems. Such a standard address most of the issues of designing MVDC power systems, but also highlights some points that needs to be studied further. One of these is the standardization of short circuit current calculation in MVDC systems. Indeed, until nowadays only short circuits on LVDC power systems have been addressed, due to the presence of DC sections in land based power stations (to supply battery banks used to black start the system in case of emergency). The related standard is the IEC 61660-1, which addresses "Short-circuit currents in DC auxiliary installations in power plants and substations" [67]. Nevertheless, such a standard move from the hypothesis of constant-voltage and infinite-power supply, being it a battery or a grid connected rectifier. Conversely, the increasing application of DC distribution systems to electrical vehicles is leading to the supply of DC system through rectifiers fed by synchronous generators. The small extension of these systems, coupled with the islanded operation (and frequently even the presence of loads whose power is comparable with the power of the generator), invalidates the hypothesis of constant voltage supply. This makes it necessary to consider the impact of generators internal impedance variation during the short-circuit transient, exactly as in AC distribution systems. Research activity in such an area is in progress, as can be seen in [68] and [69], but many more innovative systems need to be standardized yet.

4 Innovative design tools

4.1 Introduction

In this chapter, some innovative theories and techniques will be presented: dependability theory, software simulators, and Hardware-In-the-Loop testing. Although being created for rather different applications, each of them can be applied as an innovative tool for helping in system's design. In particular, the ones here presented will be relevant for the definition of the new design process goal of this PhD work.

In the following, these tools will be described focusing on how they can be used as a design aid.

4.2 Dependability Theory

4.2.1 Dependability: a universally recognized need

Marine systems design was usually done considering drivers such as performance, cost, rules and regulations compliance. Moreover, commonly the designers tend to rely on solutions and design procedures well proven, since it is common belief that what works should not be changed. However, the recent happening of significant marine accidents (such as Costa Concordia and Deep Water Horizon, to name two of the most famous in the past years) highlighted the substantial lack of attention to system's resilience to failures in system's design process. Besides their bad consequences, these accidents had a positive effect: they brought attention to the consequences for people, properties, and environment. This mostly due to the fact that the final damage cost has proven to be orders of magnitude greater than the cost of the single marine systems involved (as an example, for Deepwater Horizon see reference [70]). Those occurrences substantially changed the point of view of the parties involved in marine sector, whose interest in the consequences of faults was rather low before. Safe Return to Port regulation [8] is one example of such an increased interest in safety, defining guidelines to design marine systems and expected fault scenarios the system has to tolerate without impairing system's safety.

However, the increased interest in system's safety and resilience to failures generates in turn an increase in design burden, being necessary to analyze faults consequences and demonstrate system's compliancy with relevant regulations. This highlights the need of a different "design tool" able to integrate in the design process a more comprehensive, systematic, efficient, and widely supported approach to the analysis of system fault's consequences.

In this context, the innovative approach given by the dependability theory can be the tool capable of providing this step-ahead, as amply demonstrated in other areas where it is used (e.g. computer science [71]). Indeed, the approach given by the dependability theory has a long story, starting from nuclear plants and military telecommunication systems, and has widely proven its usefulness becoming crucial in all the safety-critical applications (like aerospace and nuclear energy) [72].

Various approaches to dependability have been developed separately in each technological sector, leading to a lack in both definitions and concepts standardization. In fact, the interest in system's response to faults, and related people/equipment/environmental safety, aroused in many different industrial applications, so a common approach could be implemented sharing the conceptual/implementation effort. Nevertheless, all these sectors addressed the problem in a separate way, leading to several different theories/definitions to analyze and solve the same issues.

In the following, a systematic formulation of dependability theory will be given, based on some recent papers [73] [74] [36] [75]. It is relevant to notice that some dependability concepts have recently grown interest in terrestrial power systems, in particular *reliability*. Indeed, in such large systems (such as electric power distribution networks) the number of subsystems is so high to require a systematic approach to maintenance and management, approach given by the reliability analysis branch of the dependability theory. In this regard, IEEE published the Standard 493 to state the "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems" [76].

The first goal of this Section is to illustrate dependability theory dedicated lexicon, concepts, and techniques. Second goal is to present some different applications of dependability theory to system design and maintenance, some of which already in use in industrial applications, to highlight the advantages such an approach could have. The last goal is to clearly demonstrate the different results given by the two main approaches of dependability techniques application to system design and verification: qualitative and quantitative.

4.2.2 Dependability theory: definitions and concepts

This section is dedicated to the basic definitions and concepts of the dependability theory, as largely accepted.

System: set of components grouped together into a single entity with the purpose of delivering a service.

Service: the set of operations performed by a system in favor of its user(s). To achieve this, the system executes a number of operations. If system's activity meets the user expectations/requirements, the service is correct. Otherwise, the service is not correct and this is due to a fail in executing one (or more) operations.

Dependability: the capability of a system to deliver the correct service with an acceptable trust.

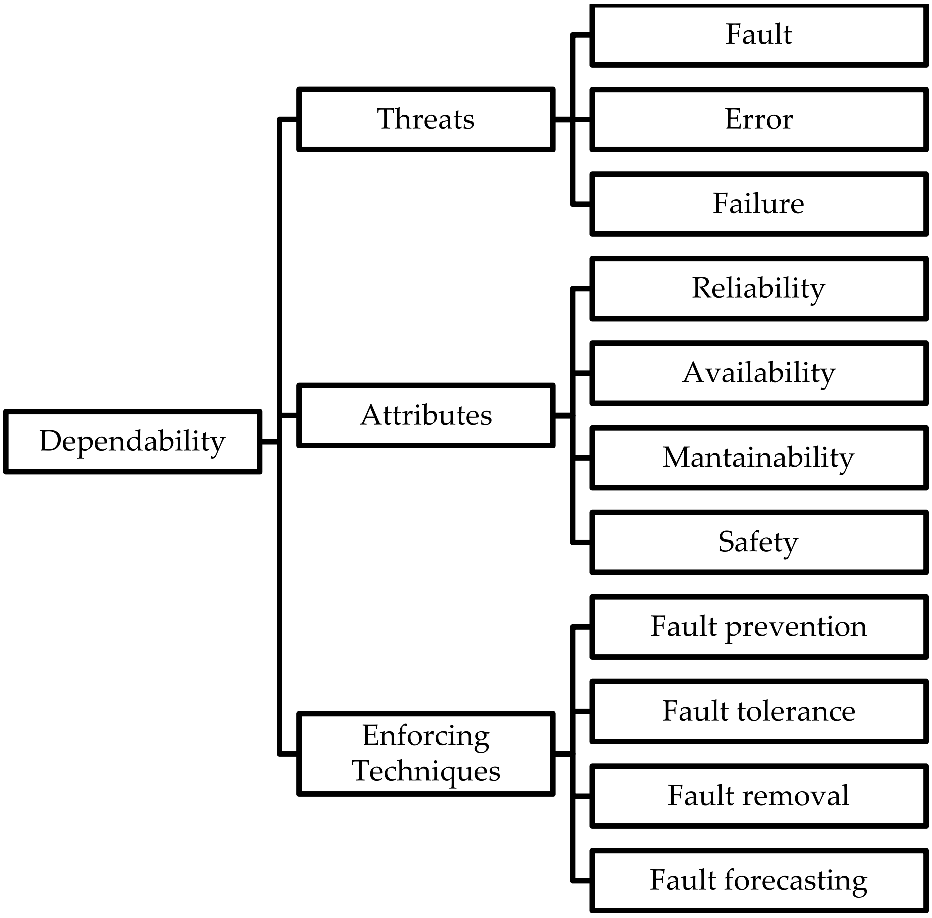


Figure 23 - Dependability key concepts, conceptual map

Table 5 - Dependability system representation with layers, and related threats

Layer	Threat
Operational	Failure
Processing	Error
Physical	Fault

Dependability theory key concepts are *threats*, *attributes* and *enforcing techniques*. In Figure 23, a conceptual map of these key concepts is shown, highlighting their interconnections and their further decomposition.

From the dependability theory perspective, three layers, each identified by the activities done, can represent a system: *operational*, *processing*, and *physical* layer.

Operational layer: the layer of service delivering.

Processing layer: the layer in which is done all the information processing, if any.

Physical layer: the layer containing the physical components operation.

System's dependability is menaced by the *threats*, classified by the layer in which they occur (as shown in Table 5), and termed *faults*, *errors*, and *failures*.

Fault: a deviation of a component operation from the expected one. It can be caused by internal events (physical phenomena such as mechanical and/or electrical stresses, wear, ageing or heating), external events (faults/errors/failures in an external system/component interacting with the considered one, or human mistake), or by flaws in system development.

Error: deviation of an internal state of a system from its true value. Errors may occur only in systems processing information (data or signals).

Failure: deviation of the service delivered by a system from the correct one. It produces a system outage.

A more detailed analysis and classification of threats can be found in [73].

Two different mechanism could lead to a system failure: *generation* and *propagation*.

Generation: the mechanism inherent in the passage of harmful events from one layer to the other. Failure is generated by errors, and errors are generated by faults.

Propagation: the mechanism inherent in the passage of harmful events in the same layer. Faults, errors, and failures can be caused by other faults, errors, and failures respectively (propagation within the same layer).

The relations between threats and failure mechanisms are depicted in Figure 24.

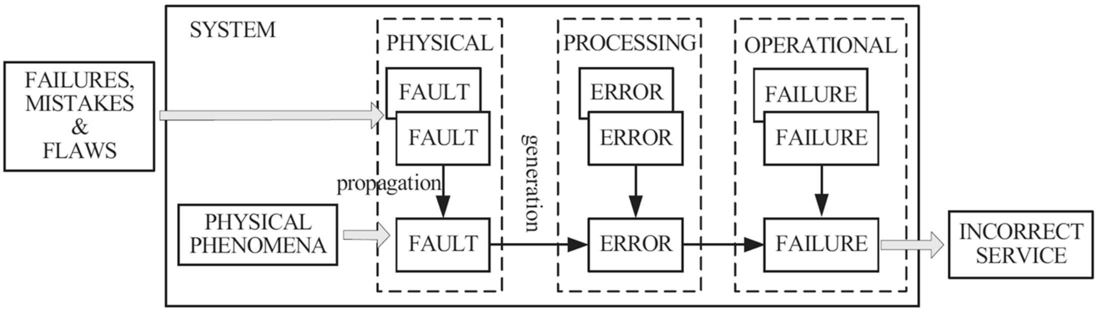


Figure 24 - Failure mechanisms [36].

System's dependability can be measured using *attributes*, which are qualities or quantities used as objective indices. As shown in Figure 23, four different attributes can be defined. The first three are probabilistic figures, thus being defined by pure numbers ranging from 0 to 1. Conversely, the last is a quality evaluated mainly relying on expertise.

Reliability: the probability that a system carries out the correct service at the time t>0, provided that at the time t_0=0 the service was correct. The expected time for a system to fail is expressed statistically as the Mean Time To Fail (MTTF).

Maintainability: the probability that a system delivers the correct service at the time t>0, provided that at the time t_0=0 the service was not correct and a repair process is in progress. The expected time for the system to be repaired is expressed statistically as the Mean Time To Repair (MTTR).

Availability: the probability that a system delivers the correct service at the time t>0, without specifying whether the service was correct or not at the time t_0=0. As a function of both reliability and maintainability, it can be calculated as:

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (4.2\text{-}1)$$

where the meaning of the parameters is given afterwards in this chapter.

Unavailability: the probability that a systems fails at the time t>0, without specifying whether the service was correct or not. It is sometimes used in place of availability to simplify dependability calculation. It can be defined as:

$$Q = 1 - A \qquad (4.2\text{-}2)$$

Safety: the ability of a system to show a safe behavior (a behavior that not cause damages) in the presence of faults generating non-acceptable failures.

Dependability attributes can be measured using several different mathematical indices, such as MTTF and MTTR seen in (4.2-1). These are related to the mathematical models used to represent the dependability behavior of system's components. Luckily, despite having a quite wide number of indices mathematical relations between them can commonly be attained, thus allowing to choose the most suited one for the application depending on analyst's preference or available data. In the following, a short list of most used dependability indices and data is given, referring to [76] in order to keep consistency in definitions.

Failure rate (λ): the mean (arithmetic average) number of failures of a component and/or system per unit exposure time. The most common unit is hours (h) or years (y). Therefore, failure rate is expressed in failures per hour (f/h) or failures per year (f/y). A synonym is *forced outage rate*.

Mean Time Between Failures (MTBF): the mean exposure time between consecutive failures of a component.

Mean Time To Failure (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 non-repairable items such as fuses or bulbs.

Mean Time To Repair (MTTR or simply r): the mean time to replace or repair a failed component. Logistic time associated with the repair, such as parts acquisition, crew mobilization, are not included. It can be estimated dividing the summation of repair times by the number of the repairs and, therefore, is practically the average repair time. The most common unit is hours (h/f).

Repair downtime (Rdt): the total downtime for unscheduled maintenance (excluding logistics time) for a given *Tp* (hours).

Total failures (Tf): the total number of failures during the *Tp*.

Total period (Tp): the calendar time over which data for the item was collected (hours).

Year (y): the unit of time measurement approximately equal to 8765.81277 hours (h). Any rounding of this value will have adverse effects on analyses depending on the magnitude of that rounding; 8766 is used commonly as it is the result of rounding to 365.25*24 /which accounts for a leap year every 4th year); 8760, which is 365*24 is the most commonly used value in power field. By convention, 8760 will be used throughout this thesis work (as it is used in the IEEE Standards).

A summary of the mathematical relations between these indices is given in Table 6.

In order to evaluate and improve system's dependability, *enforcing techniques* are given. These techniques have different approaches and objectives and can be classified in four different families, as shown in Table 7.

Fault-prevention techniques: techniques aimed at avoiding the occurrence of a fault by adopting accurate design procedures and rigorous quality controls for both components and system. These techniques affect the procedures for creating and using the product and on the technologies used for manufacturing the product. They may be applied:

- during specification phase, aimed at avoiding incomplete or ambiguous specifications;
- during design, assuring coherency in design process and tools, and controlling the correct adoption of the procedures;
- during manufacturing, adopting suitable standard of quality and verifying quality levels achievement;
- during operation, adopting both well-defined procedures (to reduce human errors) and performing diagnostics/monitoring.

Fault-tolerance techniques: techniques aimed at making the system tolerant to faults and errors. These are the most popular among all the techniques, since they act while the system is operating. Fault-tolerance requirements are divided into three different classes:

- fail-operational, when a system continue to deliver the correct service in spite of fault and errors;
- fail-safe, when a system responds to a fault or error reaching a safe state (harmless failure);
- fail-silent, when a system securely shut down after a fault.

These three classes are applied to different sub-systems depending on its importance to system operation. Fail-operational requirements are typical of uninterruptible services, where keeping the system in operation is of primary importance.

Table 6 - Mathematical relations between dependability indices

Calculated data	Formula for calculation
A, availability	A=MTBF/(MTBF+MTTR) as in (4.2-1)
Q, unavailability	Q=1-A=MTTR/(MTTR+MTTF)
λ, failure rate (f/h)	λ=Tf/Tp
λ, failure rate (f/y)	λ=Tf/(Tp/8760)
MTBF, mean time between failures (h)	MTBF=Tp/Tf
MTTR, mean time to repair (h)	MTTR=r=Rdt/Tf
R(t), reliability at time t	R(t)=$e^{-\lambda t}$

Table 7 - Dependability Enforcing Techniques

Enforcing Technique	Action
Fault-prevention	Aimed at avoiding the occurrence of a fault. Applied during system design, development and test stages.
Fault-tolerance	Aimed at coping with a fault. Applied during system operation (common implementation: redundancy).
Fault-removal	Aimed at finding and eradicating a fault, at verifying system's compliance with requirements. Applied during both system design and operation.
Fault-forecasting	Aimed at evaluating dependability attributes. Applied during both system design and operation.

A peculiar case of fail-operational level is the fail-degraded operation, which implies the delivery of a degraded, but still acceptable, service. Fail-safe requirements are commonly applied to subsystems whose incorrect service is acceptable, provided that it is safe. Fail-silent requirements is needed when the delivered service is not critical, so the user prefers to have any service instead of having an incorrect one. Fault-tolerance techniques exploits the concept of *redundancy*, which is the installation in a system of one or more extra subsystems to cope with the fault in one, or more, of them. Some examples of different possible implementations of the redundancy concept on the same system are offered in [75].

Fault-tolerance may be applied through two different strategies:

- *system reconfiguration*, implying detection of the fault presence, location of the fault, and recovery of the correct service through system reconfiguration (thus removing the fault element from the system operations);
- *fault masking*, implying riding through the fault using redundant systems, thus avoiding modifications at operational level.

Fault-removal techniques: techniques aimed at assessing system compliance with requirements (namely *verification*), including those related to dependability. These techniques apply both during system design development and system use, becoming part of the design procedure in the former, and belonging to the evaluation (tests and trials) in the latter. Verification during system design development does not require a running system, and it is performed through inspections, reviews, walk-throughs and model checking. Verification during system use is carried out by means of tests (on the real system or a prototype) and simulations (on a virtual replica). If verification process highlights differences between expected and actual performance, corrective procedures have to be adopted.

Fault-forecasting techniques: techniques aimed at assessing system *failure modes* and dependability attributes for a system. The techniques lying in this category can be separated in *qualitative* and *quantitative*, depending on the results given. Qualitative techniques are aimed at identifying, locating, and classifying the faults, and the interactions between components that may fail, that can cause a failure (failure modes). Quantitative techniques are aimed at assessing, in terms of probabilistic indices, the dependability attributes for the system.

One significant concept has to be remarked: all the defined indices are probabilistic figures, related to fault probability in a stated time. Moreover, the indices are mean values, because each component, while being apparently identical, will perform differently in reality. Due to that, dependability attributes have to be evaluated using appropriate considerations and correct mathematical/probabilistic approach.

To make an example of the misconceptions such indices can lead if not properly handled, a consideration on MTTF can be done. When using an exponential probability function, e.g. as commonly done when assessing reliability attribute, the unavailability at time t=MTTF (which is the probability of a failure from time t=0 to MTTF) can be calculated as:

$$Q(MTTF) = 1 - e^{-\lambda/\lambda} = 1 - e^{-1} = 0.632 \qquad (4.2\text{-}3)$$

As can be seen from (4.2-3), although MTTF is defined as the average time for a failure to occur, the probability to have a failure between time t=0 and MTTF is not 50%, as a mean value commonly leads to expect. This happens because the MTTF is not calculated as the time value a set of component takes to fail on average, as can be wrongly inferred by its definition, but in fact is the average time for the probability density function modeling component's reliability:

$$MTTF = \int_0^\infty t\lambda e^{-\lambda t} dt = \frac{1}{\lambda} \qquad (4.2\text{-}4)$$

This remarks the need of a coherent and systematic approach to dependability, to avoid making mistakes that will lead to wrong evaluation of data and results [77].

To conclude this section, a final remark on the dependability data has to be made: all the defined indices are time dependent. In fact, the failure rate of a component remains constant only in useful life period, as shown by the well-known bathtub curve (shown in Figure 25). During the first period, the production flaws cause a high failure rate (infant mortality). Same behavior is shown when the component approaches its end of life, where the failure rate rises due to wear out. However, the hypothesis of constant failure rate, valid only in the useful life period of a component, allows simplifying significantly the dependability data calculation. Indeed, this allows to model the component behavior using simple probability distributions (such as the exponential one), thus avoiding adopting complex models which take into account the variation of failure rate in time (such as normal distribution or Weibull distribution) [77].

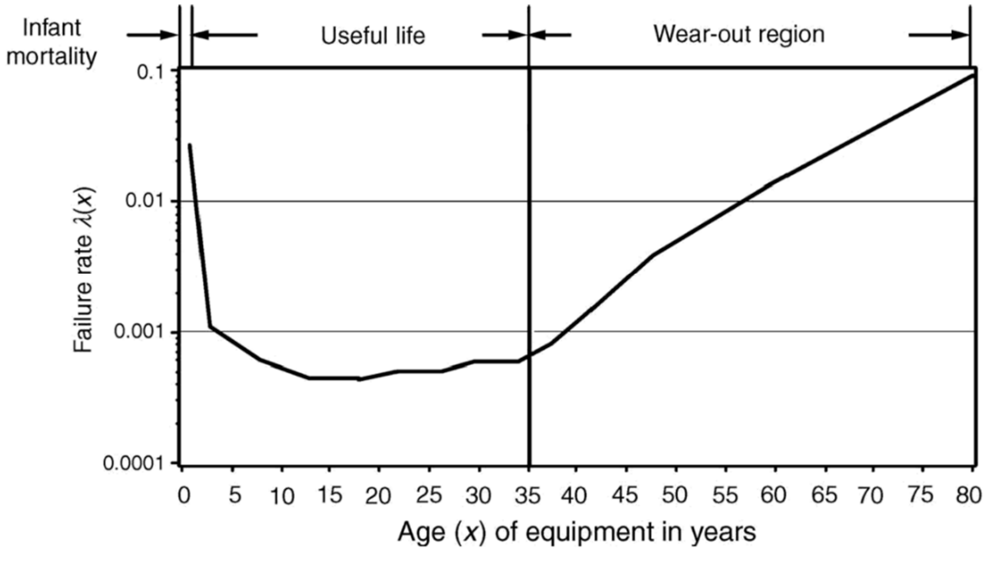


Figure 25 - Bathtub curve, failure rate versus time [77].

4.2.3 Dependability techniques currently used in system design and verification

Despite being lacking a unifying theory, dependability techniques have been used so long in system design and verification. In fact, it can be said that some of these techniques were born even before some of the stated concepts and definitions. This happened because in some demanding applications, such as aerospace and nuclear power plants, the issue of system's behavior to fault events was of primary importance. Why this happened in these two applications is evident: in both aerospace and nuclear power plants a shutdown (or even critical system behavior) due to a fault is unacceptable, being impossible to stop the system during its operation without causing harmful consequences. Another application in which system's behavior following fault events was deemed relevant was computer science, where the birth of integrated circuits led to the presence of hundreds (nowadays tens of thousands) components on a single miniaturized chip. Due to the production flaws, in such a high component number some faulty component was (and in present integrated circuits is) always present, so it was necessary to design the system in such a way to minimize the consequences of faults on system operation. In all these application areas, techniques to address these issues have born, each tailored on the system's specific needs. Each technique reflects in its structure and approach the main needs of the application in which are born, leading to a wide set of dependability techniques each able to address a specific aspect of the system response to fault events. As will be evident in the following, some techniques focuses on safety aspects, other on system's reliability, yet others on components characterization (and many more).

In the following, some of the techniques most used nowadays in dependability context are presented. A particular attention is given here to the FTA technique, due to its relevancy in the developed innovative design methodology object of this thesis work.

Premise on system decomposition

Whichever will be the analysis technique adopted, a detail level has to be defined to limit the execution effort. In fact, each technique implies the analysis of elementary components to assess the effects of their faults, and therefore determine system's dependability. Such elementary components can span from a single power electronic components to entire subsystems, depending on the needs of the analysis to be done. For this reason, a previously defined detail level is needed, and has to be chosen in an appropriate way depending on the expected results of the analysis.

As an example, when analyzing a city distribution power system it is not possible to address the analysis taking into account even the faults in the bolts keeping a single switch on the panel. This because such a high level of detail will imply a huge analysis effort, reflecting both in times (high number of elements to analyze) and accuracy (the dependability relations between elements may became less evident if too much detail is adopted).

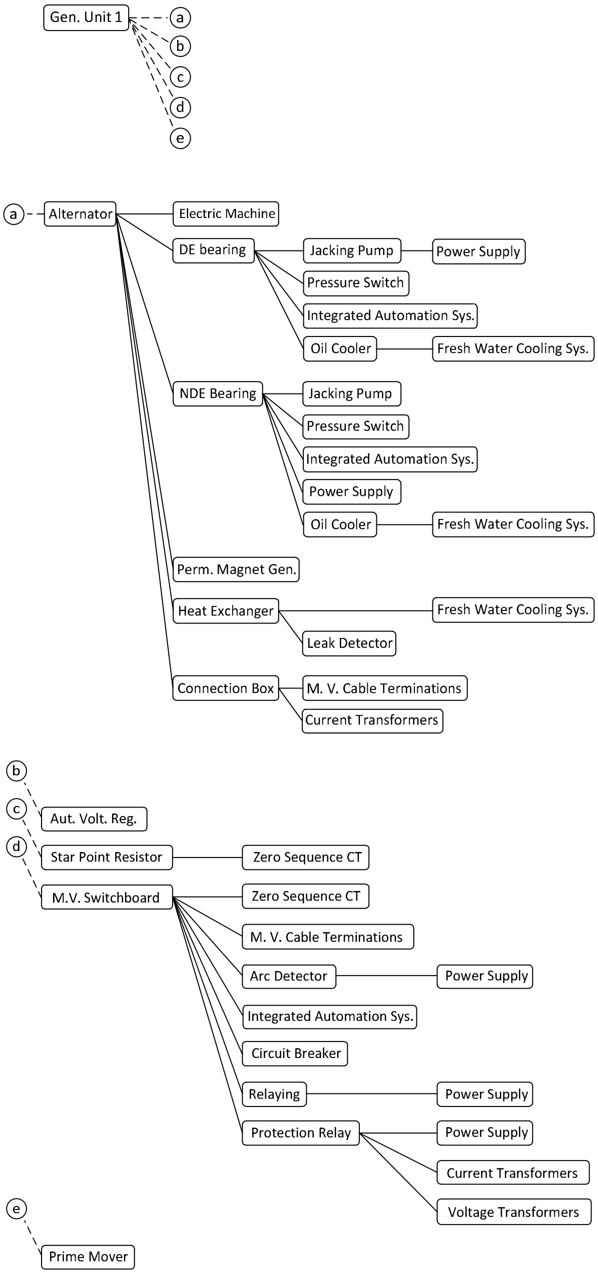


Figure 26 - Decomposition example: shipboard generator [78].

Conversely, if the switch is modeled as a single element, with its aggregate dependability attributes, the analysis of the entire power system will become viable. Obviously, the opposite situation may arise: if a too low detail level is chosen before analyzing a system, significant relations between fault events may go unnoticed. This because these happens between sub-elements being part of systems taken as a whole, whose behavior has not been analyzed.

From these considerations is evident that the definition of an appropriate detail level is relevant for the analysis and has to be carefully done in order to balance analysis effort and effectiveness of the study. To effectively address this issue, some indications can be given:

- The maximum detail level to be used is at externally procured components level. This because such elements will be always considered as a whole, and never break apart to mess with their internal components (or at least this should be the correct practice to adopt with such elements). Faults and errors internal to such components are matter of interest for their supplier/manufacturer, and their dependability behavior must be assessed as complete indivisible units from the analyst point of view. Indeed, possible harmful events generated internally to these components has to be addressed by the producer, being their way of integration in the system the only thing the designer of the system can modify. This will imply requiring some sort of data from the producer, able to represent the dependability behavior of its supplied component, which unfortunately is not often possible. As an example, in shipyard applications the highest detail level to be used in dependability techniques application is the "piece number" level, i.e. numbers identifying objects acquired externally and installed onboard by the shipyard [78].
- Once defined, the detail level has not to be considered as fixed. Indeed, it is possible to either increase or decrease it depending on the needs. During the application of dependability techniques, some systems may need further investigation, pushing toward a deeper decomposition, while others may exhibit a lack in interaction with other components, leading to neglect their further decomposition.

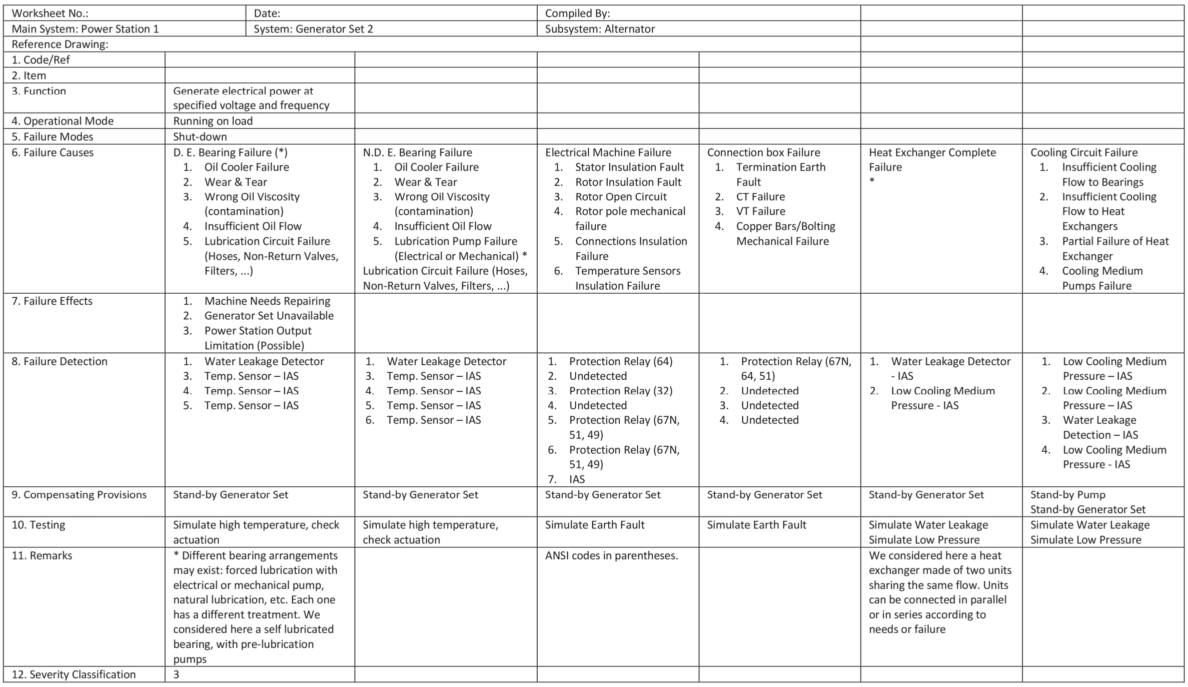
An example of a shipboard generator decomposition is shown in Figure 26 (page 75), taken from [78]. In the shown decomposition, the "piece number" detail level has been applied, and only components relevant to the electrical machine have been broken down (prime mover is omitted).

Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) was one of the first systematic analysis techniques for failure analysis. It was developed in military sector in late 1950s to study problems that may cause malfunctions in essential military systems [79].

The objective of an FMEA is to provide a systematic, comprehensive, and documented analysis to determine the relevant failures modes for the system [80] [20]. The FMEA analysts proceed to review as many components, assemblies, and subsystems as possible to identify failure modes, causes, and effects of such failures on the whole system. The analysis proceeds bottom-up, examining single components to assess whole system behavior. For each component, the relevant data (failure modes, causes, effect on system, possible solutions, etc.) is then collected in dedicated worksheets (called FMEA worksheets). An example of a rather detailed FMEA worksheet is shown in Figure 27 [78]. Through this technique, the analysis tries to find the so called "single point failure", which are the single component's faults that cause a system failure. The base hypothesis applied in such an analysis is that only a single fault at a time can happen (or a single bad human act). This simplification is necessary, because the FMEA analysis strongly rely on analysts' competences, system knowledge, and reasoning skills. Indeed, the analysts have to deduct the effect overall system of a fault in the examined component with the only aid of system schematics, components data, and other equivalent information. Due to that, the depth of an FMEA has to be a tradeoff between analysis accuracy and the ability of the analyst to deduce all the interconnections (physical, causal, etc.) of all the components at the desired detail level.

The FMEA is a qualitative technique, since it can only highlight the dependability interactions between examined elements, but cannot produce any result in terms of numerical indices for the attributes. However, its usefulness is undoubted, and it is demonstrated by its wide diffusion. Indeed, this is the most applied technique, being it commonly required by the regulations in the case of critical systems design (but also other stakeholders could be interested in it) [81].



Worksheet No.:	Date:		Compiled By:			
Main System: Power Station 1	System: Generator Set 2		Subsystem: Alternator			
Reference Drawing:						
1. Code/Ref						
2. Item						
3. Function	Generate electrical power at specified voltage and frequency					
4. Operational Mode	Running on load					
5. Failure Modes	Shut-down					
6. Failure Causes	D. E. Bearing Failure (*) 1. Oil Cooler Failure 2. Wear & Tear 3. Wrong Oil Viscosity (contamination) 4. Insufficient Oil Flow 5. Lubrication Circuit Failure (Hoses, Non-Return Valves, Filters, ...)	N.D. E. Bearing Failure 1. Oil Cooler Failure 2. Wear & Tear 3. Wrong Oil Viscosity (contamination) 4. Insufficient Oil Flow 5. Lubrication Pump Failure (Electrical or Mechanical) * Lubrication Circuit Failure (Hoses, Non-Return Valves, Filters, ...)	Electrical Machine Failure 1. Stator Insulation Fault 2. Rotor Insulation Fault 3. Rotor Open Circuit 4. Rotor pole mechanical failure 5. Connections Insulation Failure 6. Temperature Sensors Insulation Failure	Connection box Failure 1. Termination Earth Fault 2. CT Failure 3. VT Failure 4. Copper Bars/Bolting Mechanical Failure	Heat Exchanger Complete Failure *	Cooling Circuit Failure 1. Insufficient Cooling Flow to Bearings 2. Insufficient Cooling Flow to Heat Exchangers 3. Partial Failure of Heat Exchanger 4. Cooling Medium Pumps Failure
7. Failure Effects	1. Machine Needs Repairing 2. Generator Set Unavailable 3. Power Station Output Limitation (Possible)					
8. Failure Detection	1. Water Leakage Detector 3. Temp. Sensor – IAS 4. Temp. Sensor – IAS 5. Temp. Sensor – IAS	1. Water Leakage Detector 3. Temp. Sensor – IAS 4. Temp. Sensor – IAS 5. Temp. Sensor – IAS 6. Temp. Sensor – IAS	1. Protection Relay (64) 2. Undetected 3. Protection Relay (32) 4. Undetected 5. Protection Relay (67N, 51, 49) 6. Protection Relay (67N, 51, 49) 7. IAS	1. Protection Relay (67N, 64, 51) 2. Undetected 3. Undetected 4. Undetected	1. Water Leakage Detector - IAS 2. Low Cooling Medium Pressure - IAS	1. Low Cooling Medium Pressure – IAS 2. Low Cooling Medium Pressure – IAS 3. Water Leakage Detection – IAS 4. Low Cooling Medium Pressure - IAS
9. Compensating Provisions	Stand-by Generator Set	Stand-by Generator Set	Stand-by Generator Set	Stand-by Generator Set	Stand-by Generator Set	Stand-by Pump Stand-by Generator Set
10. Testing	Simulate high temperature, check actuation	Simulate high temperature, check actuation	Simulate Earth Fault	Simulate Earth Fault	Simulate Water Leakage Simulate Low Pressure	Simulate Water Leakage Simulate Low Pressure
11. Remarks	* Different bearing arrangements may exist: forced lubrication with electrical or mechanical pump, natural lubrication, etc. Each one has a different treatment. We considered here a self lubricated bearing, with pre-lubrication pumps		ANSI codes in parentheses.		We considered here a heat exchanger made of two units sharing the same flow. Units can be connected in parallel or in series according to needs or failure	
12. Severity Classification	3					

Figure 27 - FMEA worksheet example [78]

Fault Tree Analysis

The Fault Tree Analysis (FTA) technique was conceived in 1961 in the Bell Telephone Laboratories, to study the Minuteman Missile launch control system for the US Air Force [82] [83]. In the following years, its use has spread abroad, and nowadays it is commonly applied to assess reliability of complex systems in nuclear plants, chemical plants, pipelines, control systems and power systems. In the context of power systems, its use has been dedicated mostly to reliability assessment of electric and electronic components, transmission systems, supervisory control and data acquisition (SCADA) [83]. The FTA methodology is described in several industry and government standards, including nuclear power industry [84], aerospace (NASA adopt a dedicated revision of [84], while civil aerospace industry apply [85]), military systems [86], and general industrial applications [87].

A FTA is a top-down deductive failure analysis, used to understand how a system can fail, which are the sub-system and/or components implied in system failure, and what the dependability relations between them are. Starting from an undesired state for the system (namely *top-event*), which is typically a system's failure event (but can be whichever condition may result relevant to analyze), the analyst applies logic to deduce its causes, deepening the analysis up to the identification of the base causes (which are components' faults). During the investigation, the analyst build a diagram, the *Fault-Tree*, mapping the relationships between faults, subsystems, and design elements by Boolean logic. The most common approach to perform a FTA can be summarized in few steps, presented hereinafter.

1) Definition of the top-event:

   This step is relevant, because each single fault tree can be used to analyze only one top event (which may be fed into another fault tree as a basic event). Though the nature of the undesired event may vary dramatically, a FTA follows the same procedure for any undesired event; be it a voltage sag on a power grid, an undetected fire onboard a ship, or even the random, unintended launch of a ICBM. Due to labor cost, FTA is not performed for all possible failures, but only for most dangerous ones (which depend on application). The definition of the top-event is relevant, because FTA is a static technique, unable to address dynamic operations on the system (such as protection intervention, system reconfigurations, etc.). In fact, it is necessary to clearly state both the top-event and the system condition/configuration used during the analysis, to allow performing a correct FTA. Eventual dynamic actions relevant for the chosen top-event (such as load shedding when the considered top-event is a black out due to overload) have to be hypothesized as "already applied" during the analysis, but have also to be considered as possibly faulted. This doubles the FTA complexity, due to the need of considering two different possibilities: action correctly performed or action faulted. The choice between building a single fault tree including both the possible conditions for the action and building two separated ones is up to the analyst.

2) Obtain an understanding of the system:

   All causes of the defined top-event having more than null probability to happen must be sought. To achieve that, each subsystem/component fault causes have to be identified and clearly determined. To this aim, the best starting point to perform an FTA may be a previously done FMEA analysis. Indeed, firstly, the data collected in

FMEA greatly simplify this analysis thanks to the determination of fault causes and effects for each subsystem/component; secondly, the system understanding achieved during the FMEA will be useful also for this technique application.

3) Construction of the fault tree:

   After having identified all the possible fault causes for the system, it is possible to build the fault tree. This diagram visually represents the relations between each cause of fault and the system's top-event, using Boolean logic to state the cumulative effect of the fault events. The result is a tree diagram in which the single component's faults combine each other through AND, OR, and other logical gates (list in Table 8) to lead to the undesired top-event happening (an example is shown in Figure 28 build for the decomposed system of Figure 26 [78]). To build such a diagram, in addition to system's data and detailed information the analyst must have a deep understanding of the system to be analyzed and significant knowledge. The diagram construction itself is a strong tool to understand system's critical points, because the relations between events became evident during this step, possibly highlighting harmful interconnections not apparent before.

4) Evaluation of the fault-tree:

   Thanks to the fault tree(s), built for the specific undesired event(s), it is possible to evaluate system's critical aspects from the dependability point of view. The visual representations ease the identification of the so-called bottlenecks, and excessive redundancies can be pointed out. In this step, all the possible hazards affecting both directly and indirectly the system can be assessed.

5) Application of corrective procedures:

   This step depends on the system in study and on the identified hazards. Indeed, having found critical points it is necessary to solve them, applying corrective procedures. These procedures can either act on single components (changing component's attributes) or system architecture (changing relations between components), depending on analyst and system's designer evaluations (including feasibility, cost, and time constraints).

The FTA is a technique that can be classified as both qualitative and quantitative, depending on the needs and available data. In fact, the approach aforementioned permits to construct the fault tree and identify critical points, without necessarily knowing any attribute for the elementary components. In this perspective, the FTA allows to achieve similar results as FMEA, adopting an approach oriented to the system rather than to the component, therefore giving up on single component's detailed analysis in favor to a wider comprehension of interrelations between components and their impact on the system. On the contrary, if detailed dependability indices are available for each element, thus characterizing effectively all the system's possible fault events, the fault tree diagram can be easily translated into a mathematical representation. Thanks to this, accurate evaluation of entire system's dependability attributes can be obtained starting from components data, also including some significant mathematical indices useful to identify the most critical components in the system. Indeed, an FTA permits to assess not only the dependability of systems and subsystems, but also to measure the importance of faults events in regards to the entire system service. Due to that, the FTA can be also classified as a quantitative technique. This duality makes the FTA technique the most suited for the application in regards to the innovative design methodology developed in this thesis work. [81]

Despite being a versatile and seemingly complete tool, FTA have disadvantages. The most significant one is the effort needed to develop the fault tree in the first time application on a system. Other techniques, such as FMEA, have a higher performance/cost index when analyzing small systems to determine a single point of failure. Anyhow, when complex system have to be analyzed, FTA became the most suited technique. This due to the possibility to direct the analysis on the sole basic events contributing to system failure [82]. Finally, an FTA is capable to solely model static events, neglecting all system's dynamic actions such as reconfiguration and protection intervention.

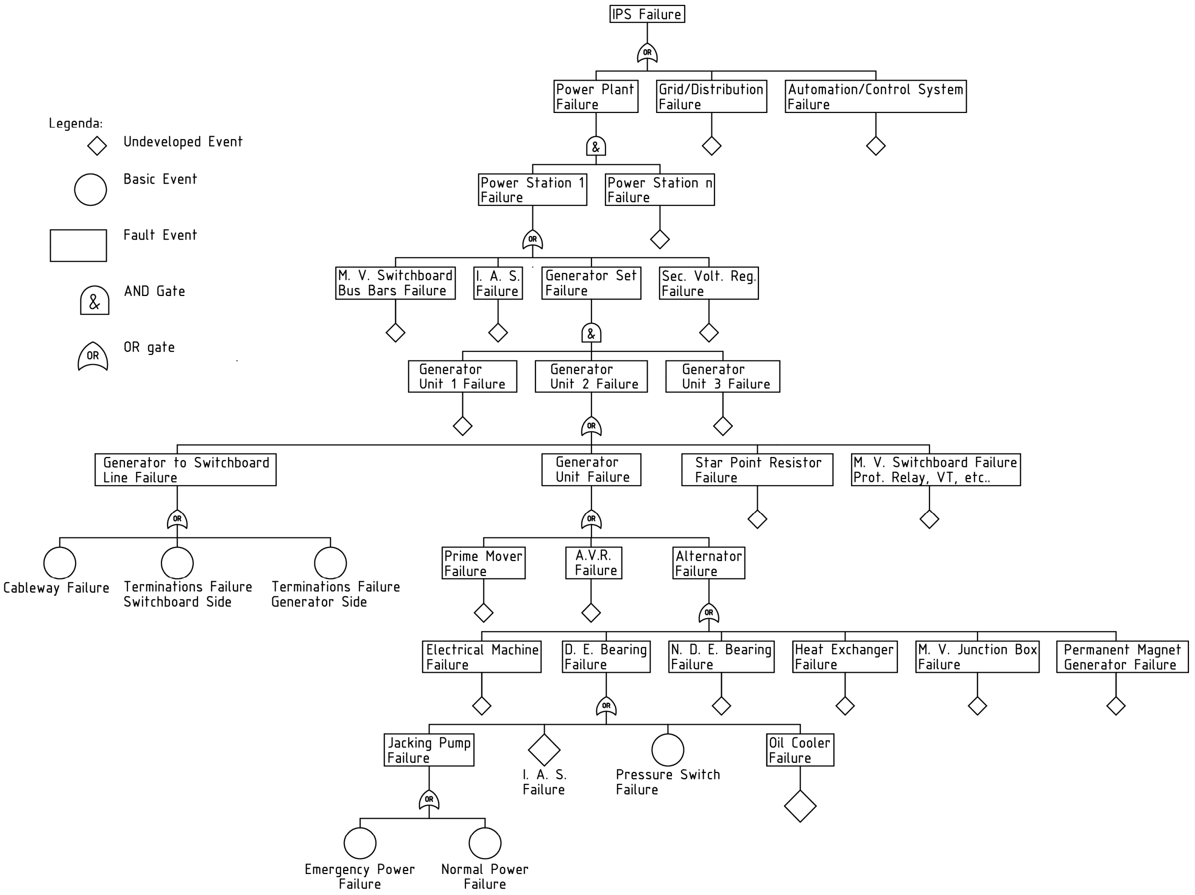
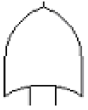
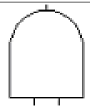
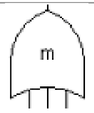
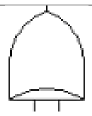
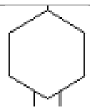
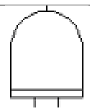
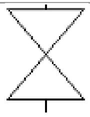


Figure 28 - Example of Fault Tree diagram [78].

Table 8 - Boolean operators used in FTA fault tree construction

Symbol	Name	Causal relation	Valid inputs n°
	OR	Output event occurs if any one of the input events occurs	≥ 2
	AND	Output event occurs if all input events occur	≥ 2
	MAJORITY VOTE	Output event occurs if m of the input events occur	≥ 3
	EXCLUSIVE OR	Output event occurs if one but not both of the input events occurs	2
	INHIBIT	Output event occurs if both input events occur. One of the inputs represents a conditional event	2
	PRIORITY AND	Output event occurs if all input events occur in sequential order from left to right	≥ 2
	NOT	Output event occurs if the input event does not occur	1

Reliability Block Diagram

The RBD (Reliability Block Diagram) is a diagrammatic system modelling technique, aimed at showing how single components reliability contributes to the success or the failure of a complex system. It implies the building of a diagram in which every components is connected (in series or parallel) with the others, following dependability relations. This leads to a diagram in which all components form a continuous path from one side to the other. Parallel-connected components imply redundancy, because all the elements in parallel configuration must fail for the paralleled section to fail. Conversely, in series-connected components the fault of one of them lead to the failure of the entire series. To ease the visual determination of the system state, failed components can be considered as "open paths". Therefore, only if there is a continuous path connecting one side of the diagram with the other the system can be considered as functioning. Otherwise, the system has to be considered as failed. An example of RBD, made for a six generator's shipboard power system, is shown in Figure 29. It represents each possible combination of generators able to achieve the necessary power supply, stated by electric load balance. In particular, in the represented condition it is necessary to have at least 5 out of 6 generators running to deliver the correct service (sufficient power generation capability).

An RBD can be easily converted in a Success Tree by replacing series paths with AND gates and parallel paths with OR gates. The Success Tree, which maps the dependability relations between components that lead to the correct service for the system, can be then converted in a Fault Tree by applying De Morgan's laws (Boolean algebra transformation rules). In this regards, RBD and FTA can be considered as equivalent techniques, one dedicated to assess each possible way to achieve system's success (RBD), the other dedicated to assess each possible way the system could fail (FTA). As well as in FTA, if a quantitative analysis is intended to be done it is possible to easily translate an RBD into a mathematical representation [88].

The RBD provides an easy to read and understand representation of the system, "mission success" oriented. This due to the fact it permits to evaluate in a simple way if the system can perform the requested service or not. However, RBD, as well as FTA, is not capable to represent the system when configuration changes (it is a static representation).

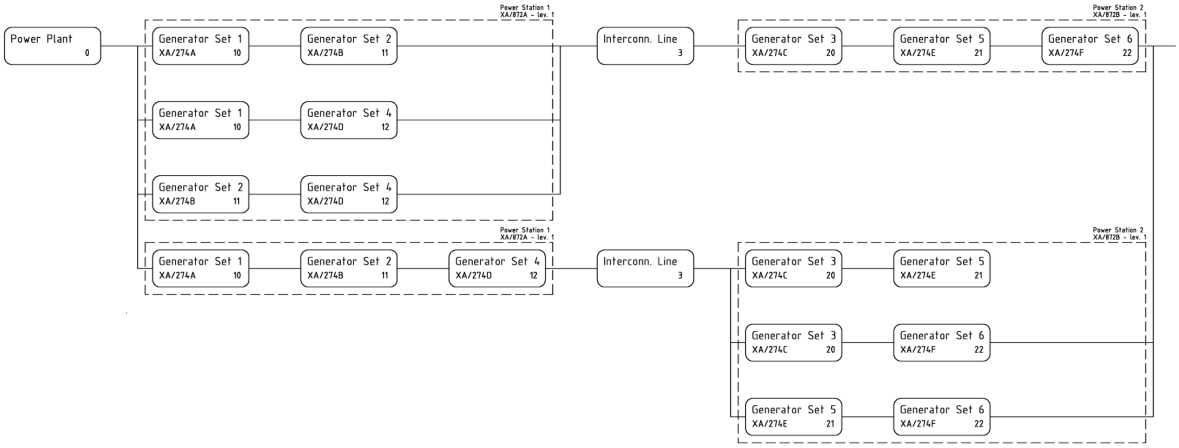


Figure 29 - Example of Reliability Block Diagram [88].

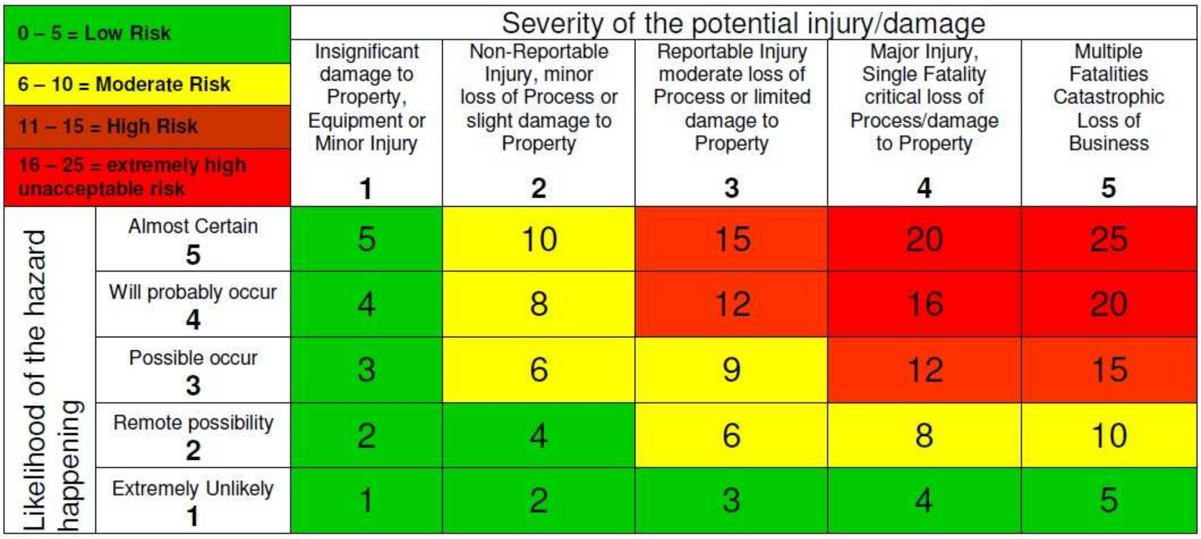
Hazard and Operability Analysis

This technique has been developed by the Imperial Chemical Industries in the 1960s, and the Chemical Industries Association has promoted its use since late 70s [89]. Nowadays, in chemical/process industry, HAZOPs are considered a safety/legal requirement and any findings become legal requirements with costly implications and on-going controls [90].

A HAZOP (HAZard and OPerability analysis) is a structured analysis of a system, process, or operation carried out by a multidisciplinary team. The team, having detailed information on the system to be studied, examine node-by-node the design of the system, to identify possible design flaws and safety, health, and environmental hazards. This is achieved using a set of guidewords (adjectives) combined with systems parameters to seek deviations from the design intent and to evaluate if such deviations are meaningful or not (meaningful deviations are the ones physically possible; things such as "no temperature" are not considered). Having identified possible deviations, the team concentrates on those that could lead to potential hazards to health, safety, or environment. For each hazard (that is a physical situation with the potential for human injury, damage to property, damage to environment, or a combination of these), the likelihood of specific undesirable event occurrence within specific period or specific circumstances is determined. The combination of severity of the hazard and its probability defines the risk related to the specified deviation, as shown in Table 9. Usually a classification of severity and probability in discrete steps is made, to ease classification. Where deviation causes are found, the team, taking into account existing safeguards and using experience and judgment, evaluates its consequences. Each identified deviation that falls in the high-risk area has to be addressed, proposing solution to lower its occurrence likelihood, its hazard, or both. In addition to hazards, team could search also for potential operating problems concerning security, human factors, quality, financial loss, etc. The entire HAZOP process can be seen in Figure 30.

Despite seeming a rather effective procedure, HAZOPs are prone to flaws, due to their approach based on expertise and judgment of human beings. A concise explanation of the issues that can arise in HAZOPs, thus impairing effectiveness, can be found in [91]. HAZOP analysis evaluates the safety dependability attribute for a system. The risk evaluation and classification depends totally on analysis' team perception of risk, thus it can be classified in the qualitative techniques branch.

Table 9 - 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				
		Insignificant damage to Property, Equipment or Minor Injury 1	Non-Reportable Injury, minor loss of Process or slight damage to Property 2	Reportable Injury moderate loss of Process or limited damage to Property 3	Major Injury, Single Fatality critical loss of Process/damage to Property 4	Multiple Fatalities Catastrophic Loss of Business 5
Likelihood of the hazard happening	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

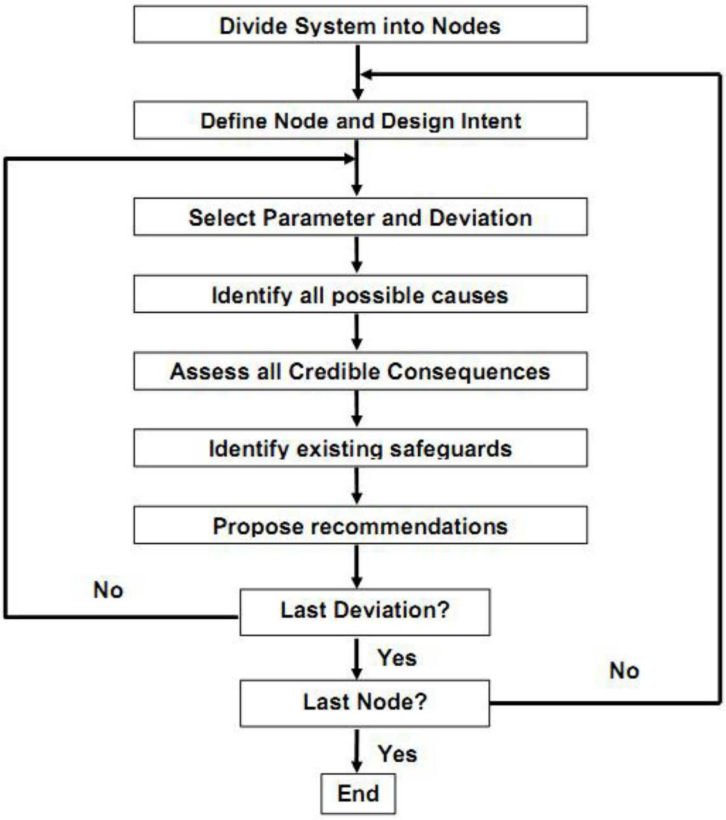

Divide System into Nodes
Define Node and Design Intent
Select Parameter and Deviation
Identify all possible causes
Assess all Credible Consequences
Identify existing safeguards
Propose recommendations
No
Last Deviation?
Yes
No
Last Node?
Yes
End

Figure 30 - HAZOP analysis process

4.2.4 Qualitative vs. quantitative techniques

As mentioned previously, fault-forecasting techniques can be divided into qualitative and quantitative techniques depending on the results the techniques are able to give. Qualitative techniques promotes an understanding of the impact of faults on the system, whilst quantitative ones permits to assess mathematical indices.

Thanks to the possibility to be applied without knowing historical/statistical data on the system, the qualitative techniques are the most used. Among them, FMEA is the most relevant. This because FMEAs have been performed for a number of years in critical industrial applications and are a generally accepted mean of demonstrating attention to dependability. Due to that, the following considerations are based on FMEAs, but are generally valid for each quantitative technique.

A benefit of qualitative techniques is that they are mainly forms-based analyses and no special software are required. Both outcomes and in-work documents may be maintained in a database, but it is not a requirement. In fact, any commercially available database software is able to handle the simple sorting and cataloguing requirements of such techniques. A qualitative analysis process is relatively straightforward and can be performed by analysts who are familiar with the system requirements and operation. The fact that these techniques are primarily used to assess the acceptability of the system design is one of their main limitations. In fact, both users and analyst perception on these techniques is that qualitative techniques must be performed to comply with a requirement, and cannot be used to guide design and system operation to obtain a more dependable system. This because their structure does not permit to easily examine design modifications, due to the wide impact such modifications can have on the system. (Often these require a new evaluation of a significant portion of the system due to the rise of new dependencies). Although qualitative techniques are virtually capable of identifying any single point failures within the system, the burden of their application has greatly increased due to the increased complexity of the systems including control functions and feedback mechanisms. Indeed, many more potential effects may results from a single fault, and the potential to oversight some of them is significantly increased in modern systems due to the complexity of equipment. Moreover, common qualitative techniques does not provide any mean to assess easily multiple failures events, which are the more likely to happen in a mature design. Besides all, it has to be remarked that qualitative techniques require that the analyst must keep the entire system in mind to be successfully applied. Possible subtle interactions, which significantly affect system dependability, may be overlooked in favor of the 'big picture' [81]. As an example of such an issue, in [18] are depicted some incidents, resulting from inadequate power system analysis in an application in which FMEA is a contractual requirement.

Conversely, quantitative techniques provide analysis methods to identify and evaluate objectively the system's interdependencies in a structured way, as a mean to assessing dependability attributes. Each quantitative technique needs the building of a system's model, capable to explain all the dependability relations among components in an easy to comprehend way. In fact, the quantitative methods' main strength lies not in the attributes' evaluation, but in the structure of the analysis procedure. The process of building the dependability model of the system (e.g. a fault tree, a reliability block diagram, etc.) allows the analyst to examine one small piece of the system at a time, assessing relations among components without the need to keep the entire system picture in mind. In this way, all the possible interdependencies can be assessed and the impacts of single or multiple failures are properly arranged throughout the system model. Indeed, all the system's failure modes can be inferred from such a model as a subset of the quantitative assessment results. Due to this capability, failures resulting from complex subsystems interdependencies can be assessed easily, as opposed to what happens with qualitative techniques. In addition to this improved failure identifications capability, these techniques are also able to provide information about system and components' dependability indices thanks to the possibility to convert system dependability model in mathematical form. Moreover, mathematical relations can be also used to rank components in terms of their importance to system's dependability, and as a tool to evaluate design modification's cost-benefit impact. Indeed, quantitative techniques allow evaluating changes in system design easily, through the modification of system's dependability model and the consequent comparison between the "before and after" system's dependability attributes. The impact of single components' dependability characteristics modification on the system can be also easily assessed, allowing to evaluate the opportunity to change their supplier to achieve a higher dependability degree. As with any analysis methodology, quantitative analysis techniques have their own drawbacks and limitations. First, the analyst must have an extended knowledge of the system, its requirements, and its operation (but this is true also for qualitative techniques). Secondly, it has to be experienced with the chosen technique to properly apply it. The complexity of the model and the wide combination of possible failures may need the use of sophisticated software tools. Luckily, modern personal computers have sufficient computational power to solve the complex models resulting from dependability analysis in a fast and easy way, at essentially no cost. [81]

The most relevant difficulty related to the application of all the quantitative techniques is the lack of pertinent failure-rate data of the single components (fault events modeling). In fact, wrong failure data impairs the calculation of dependability attributes of the whole system, leading to a wrong, maybe even harmful, evaluation of system's dependability. Failure data is difficult to retrieve and to assess, and it is prone to relevant uncertainties, being often impossible to test a high number of the same equipment in the same conditions for a significant amount of time, to assess proper dependability data. The peculiar application of quantitative techniques made in this thesis work implies knowing failure data for marine power system's components, which is difficult at the moment. Indeed, very scarce data can be found on marine applications, while land and nuclear power systems have a wide database. This is due to the difficulty of having a large base of identical installations on which made a survey. Indeed, such an issue happens both because ships power systems are commonly tailored following owner requirements and area of operation (thus being difficult to find ships with equal components used under the same external stress factors), and because ship owners are reluctant to disclose information about faults which occur on board (due to obvious marketing reasons). Some data on marine systems can be found in [20] but, in this thesis work, the reference will be made on the data given in Chapter 10.3 of IEEE Std. 493 [76]. Such data refers to extended equipment reliability surveys made between 1976 and 1989 in industrial and commercial applications. While it is not marine system's data, it has been deemed sufficient for the scope of demonstrating the possibilities given by the innovative design process, goal of this thesis work.

Though significant, the determination of simple numbers to represent overall system dependability attributes should not be considered the most significant use of dependability quantitative techniques. Indeed, the most relevant result of such analyses is the determination of the relative contribution of single/multiple faults to system dependability [79]. As a matter of fact, regardless of the failure data applied to quantify the model, all of the generated failure combinations represent valid ways for the system to fail, if the model is correct. Moreover, quantitative techniques can be useful to compare different system designs having similar components. In this case, the results will be not as sensitive to failure-rates data as in absolute determination of system's attributes (due to the uncertainty associated with the failure data, failure combinations within an order of magnitude in likelihood can be treated as having a similar likelihood of occurrence). In this regard, relative determination can be the best application of quantitative techniques, allowing to assess the best design for a system from a dependability point of view [82].

Concluding, it is evident that quantitative techniques are more powerful than qualitative ones, being able to quantify system's dependability and related mathematical figures. Nevertheless, to apply them it is necessary to have dependability data on the system components, which is not always possible. In this regard, qualitative techniques allows to assess and improve dependability of a system starting from less data than quantitative ones, even from simple ratings given from experience. Although they seem less attractive in comparison to quantitative, qualitative techniques are still a useful tool to improve the dependability of complex systems, easy to comprehend and use, and universally recognized by regulatory bodies.

4.2.5 Dependability in shipboard power systems, present situation

Nowadays, dependability concepts and techniques are used in several industrial applications, such as aerospace and nuclear power. Where its application was lacking until recent times is in marine systems. Nevertheless, its use is increasing, promoted by recent severe accidents and by stricter regulations. In this section, some examples of such a diffusion are given, mainly concerning shipboard power systems and related subsystems, but not only limited to these. An accurate analysis of the dependability theory can be found in [92], together with a study on how such concepts are already included in rules and regulations applied in cruise sector, although without a clear theoretical framework underlying.

Reliability centered maintenance

Maintenance costs are a significant part of the overall operating costs of a ship. The rigid prescriptions from regulatory bodies and the recommendations from equipment suppliers makes it appear as an obligation, rather than something positive. Nevertheless, maintenance is essential to keep the equipment in the best possible conditions, in turn affecting system's dependability and thus having both environmental and safety consequences. In this regard, an approach to maintenance focused on reliability can be applied: the Reliability Centered Maintenance (RCM). RCM focuses maintenance resources only on those items that affect the system reliability [93]. In such a way, maintenance can be applied as a cost-effective procedure, ensuring at the same time the best possible operation of equipment from the point of view of overall ship operation. Such an approach has its origin in aircraft maintenance programs (in particular from the Boeing 747 one), where a conventional maintenance approach would have led to a commercial failure due to excessive maintenance effort. RCM is formally defined as "a process used to determine what must be done to ensure that any physical asset continues to do whatever its users want it to do in its present operating context" and "RCM employs a system perspective in its analyses of system functions, failures of the functions, and prevention of these failures" [93]. Four features can describe the RCM approach:

- Preserve functions;
- Identify failure modes that can defeat the functions;
- Prioritize function need (via the failure modes);
- Select only applicable and effective tasks.

As can be easily seen, RCM roots are deeply entangled with dependability theory, using the same concepts to achieve a similar goal: keep the correct system service. An extensive description of Reliability Centered Maintenance can be found in [93], where all the issues and peculiarities of its shipboard application are analyzed. Although seeming a rather complex approach, some evidences of successful application to ships are present. As an example, United States Coast Guard recently has started investigating new maintenance strategies for its assets, in particular Diesel Engines. The most promising approach is the Reliability Centered Maintenance, and relevant results are already used to tailor maintenance schedule on the ship's needs [94].

Dependability techniques actually used in marine system verification

In marine sector, some applications have more demanding requirements than others do, in particular for what concerns system's behavior in fault conditions. Naval vessels are the most obvious ones, but also other units may have requirements as strict as they may. In particular, faults are to be taken into account in each vessel that is "mission critical", such as oceanographic vessels, pipe/cable layers, drilling vessels, and so on. In such vessels, losing the correct service means impairing the mission, or even failing it, with relevant economic impact and possible harmful consequences to human health, properties, and environment. Due to that, the issue of system's dependability emerged also in marine application, similarly to what happened in aerospace and nuclear plant systems. Luckily, solutions were already developed for these applications, so proper concepts and techniques have been brought to marine sector.

This "evolution" has been mainly driven by regulatory bodies, which have direct interest in failures consequences and related compensations. In particular, when vessels dedicated to mission critical application have to be designed and built, regulations impose requirements dedicated specifically to ensure a minimum level of system's fault resistance. This is done through the definition of rules specifying the behavior of the system following some relevant fault events, such as a generator loss (examples are the ABS Rules and Regulations [26] and [22]). As appears evident, the used approach has a major flaw: it cannot address each possible fault event and failure mode, due to the generalization applied in such rules and regulations. Indeed, it is not possible to create regulations dedicated to each particular system's design and/or specific application, so a certain amount of generalization has to be applied. In such a process, only the most relevant fault events are retained, leaving the definition of all the possible failure modes of the system to the designer. However, regulatory bodies need an assurance of the proper identification and removal of each possible point of failure. To do that, the solution used by regulations is to require a dependability analysis, commonly in the form of a FMEA (as clearly stated by rule 2/11.1 of ABS Guide on DP systems [22]).

Following regulatory bodies specifications, designers can define the preliminary design of the system, which is the one able to meet the requirements of the customer and at the same time comply with regulations requirements. Then a FMEA can be done, at first on preliminary design, and then on detailed design, to assess each possible point of failure for the system. Proper solutions for the critical point emerged from the analysis has to be taken, and the final system FMEA has to be submitted for approval to the regulatory body. Once approved, system can be considered well designed, and ship construction can proceed. Designers can also apply other techniques on their own, to the aim of improve the system (one of these is HAZOP technique). However, regulations require an FMEA, so it is common to rely only on it.

This approach has led to a substantial improvement in dependability of mission critical vessels. An example of such an improvement can be found in [20], where a brief review of the historical evolution that led to the application of FMEAs to Dynamic Positioned Vessels is presented. Nevertheless, the imposition of such an approach by regulatory bodies to designers has led to a relevant issue: both users and designers perception is that FMEAs must be performed to comply with a requirement. This cause a lack in interest in dependability techniques, which are considered as checks to be marked to build a ship, rather than powerful tools to be used to attain a better design. Conversely, academics and consultants tend to have an approach to dependability more open than users and designers, as demonstrated by several works in literature whose goal is to explain the benefits of dependable approach to ship's design ([95], [96], and [97] only to mention some). In this regard, this thesis work will try to demonstrate the advantages of a dependable approach, through a deep explanation of the benefits these techniques can bring to ships design, and through the proposal of an innovative design process integrating dependability techniques as its foundation.

4.2.6 Dependable oriented design

As explained in the previous sections, dependability techniques can be a relevant aid not only to assess system's behavior in case of faults, but also to verify systems compliance with particular requirements. To this extent, some applications in marine sector are already present, but a further step can be done: the application of dependability theory to system design. In particular, system design may positively improve though the integration of both qualitative and quantitative techniques. A design process integrating dependability theory approach can be defined as "dependable oriented design".

Dependable oriented design can be achieved introducing dependability dedicated activities to the common design process (as shown in Figure 31) [36] [98]. These activities interact with conventional design ones, in different stages of the process, to the aim of improving it:

- Specification step permits to assess faults that are likely to happen during ship's operation, starting from conceptual design and contractual requirements. Doing that, it is possible to use the desired system's behavior (in response to such faults) as an input for architectural design;
- Implementation step allows to pinpoint single subsystems and components menacing system's dependability, through a dependability analysis on chosen system architecture;
- Evaluation step is used to evaluate if the designed system meets the expectations concerning its behavior in response to fault events.

Issues emerging from each of these steps can be addressed through a feedback to the designers, to change the system design accordingly. The depth of these feedbacks (even up to requirement analysis) depend on the extent of the issue to be solved, and on the applicable solutions.

Such a design process allows pinpointing most of the issues that may lead to a system failure and solve them, depending on the skills of both analysts and designers. Both quantitative and qualitative techniques can be used during the dependability-oriented design, depending on the expected results. Qualitative techniques will allow to obtain relevant results with a limited effort, while quantitative will provide much more data and objective dependability evaluations, at the price of a relevant increase in resources to be allocated to the design process. In [98], an extended discussion on the advantages of dependable oriented design is made. The motivations, which may drive each subject involved in ship's design (shipyard, sub-contractors, classification societies, and owner) to its adoption, are also highlighted. Moreover, in [97] indications on how integrating dependable oriented design from a project management point of view are given, to demonstrate that most of the relevant data needed to apply it is already present in conventional design process (thus allowing its implementation in common system design with limited management effort).

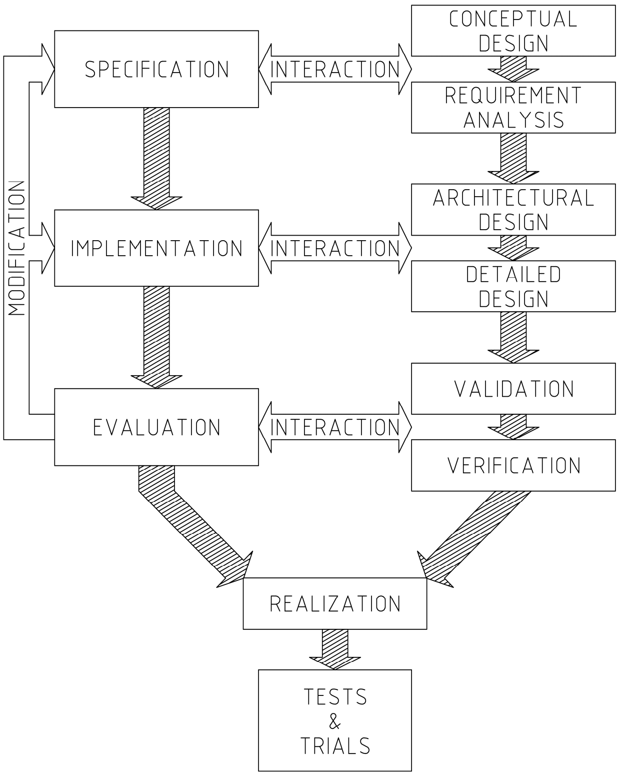


Figure 31 - Dependable oriented design [36].

Although dependable oriented design seems an innovative application, nowadays it is already applied in mission critical systems, even if not in such a systematic way. Indeed, in such applications a series of qualitative analysis (usually FMEAs or HAZOP analyses) made throughout all the system design process are used as a mean to highlight hazards and critical issues. This approach is the foundation of dependability oriented design, and demonstrated in real application to be successful, though resource consuming.

In this thesis work, this approach is limited to shipboard power system, but can be successfully applied to all shipboard systems, to improve ship's dependability.

4.3 Power system's software simulators and HIL

4.3.1 Introduction

The design of modern IPSs cannot be done without considering the widespread presence of control systems onboard a ship, whose complexity increase along with the increase in their expected performance and functionalities. The pervasive introduction of power electronic converters has led to an improvement in control above system's electrical variables, but it has also increased the number of control systems integrated in an IPS. The presence and simultaneous operation of such a high number of control systems makes it necessary to assess their correct response to perturbations and their correct functional integration (to avoid harmful interactions). Moreover, also the common system protections have a relevant impact, because their operation has to be in accordance with system's controls.

In this context, the advancements in power electronic and computer science makes it possible to implement mathematical models in an "easy to use" software environment, and to apply Hardware-In-the-Loop testing before the exploitation of a system. The former (software simulators) imply the creation of a mathematical model of the system in a computer software, in order to simulate the real system behavior in response of given conditions/disturbances. The latter (HIL testing) imply the connection of a real control system to a simulated power system, to verify its correct design and the absence of dangerous issues. In such a way it is possible to assess if the real control system will respond as designed before its installation onboard, thus allowing to solve possible issues when the cost of the needed modifications is still low. Software simulators and HIL tests are commonly used in technological research area to develop new technologies, but not applied by system designers. This is a relevant issue, because such systems allows not only to verify system design correctness and system's performance before its construction, but also to test events that normally cannot be tested due to the possibility of damaging the real system.

In this regard, it is necessary to point out that the use of software simulators and HIL tests for the key systems is imposed also by the new IEC 61892-5 [99], which is in course of approval. Studies on the subject are already underway, and some evidence of the advantages of HIL testing and simulators in shipboard power systems are already present in literature [100] [101] [102] [103] [104] [38] [105] [106] [107] [108].

Goal of this chapter is to illustrate software simulators and HIL tests capabilities, together with their most peculiar characteristics. As aforementioned, such tools are well known in academic area, so a brief explanation will be given in the following, focusing mostly on the impact they can have on system design.

4.3.2 Software simulators

Nowadays, power systems are composed by several elements connected together to supply the correct service to the users (which is, by a pure electric point of view, supplying loads with electric power and adequate power quality). For each element mathematical representations are available in literature (or can be achieved if not), dedicated to the calculation of desired output data from available input parameters. The complexity of such models depends on the output data to be calculated and on the desired approximation with real system results. The simplest ones allow calculating output variables even trough simple hand calculus (e.g. synchronous generator's Heffron-Phillips model, used to evaluate electromechanical oscillations issues, has order two [39]), while the most complex ones need a software implementation in order to calculate the desired output data (e.g. synchronous generator's complete model has order eight [109]). After having determined the mathematical models of each system's component, it is possible to merge them in order to obtain a mathematical model of the entire power system. Doing that it is possible to calculate the system's behavior in response to various events, depending on the models chosen for the elements. As an example, it is possible to model an IPS to assess its response to a disturbance, such as a high power asynchronous motor start-up transient [103]. Due to the complexity of modern power systems, the only viable option is to implement its model into a software environment, to allow doing the related calculations in a time compatible with the needs.

A system's simulator can be a great aid to design. Indeed, it allows checking the behavior of the system already during the design stages, causing no damage to the real system. Analyzing results available both in literature and developed during the PhD activity, it is evident that the use of a mathematical model that can be simulated by a software can aid in the definition of the power system components and in their verification. In a system with stringent requirements such an aid may be essential to develop a product able to achieve success on the market. In fact, thanks to a software simulator it is possible to verify the correctness of the design choices (e.g. the coordination between protections and real time voltage and frequency control systems) and it is possible to assess system dynamic response before building the real system. The capability to assess through simulations some of the relevant system's transients allows:

- a greater flexibility in design, through the study of the behavior of different system layouts;
- a simpler and immediate definition of emergency actions;
- checking correct coordination between protections and control systems;
- supporting training, allowing staff to acquire sufficient degree of confidence on system's operation;
- a simpler definition of control system's parameters.

While a software simulator seems a factotum tool, it is not. Indeed, its usefulness depends directly on its correct construction and use. The same detail level has to be chosen for each component model, and proper integration between the different models has to be made. Indeed, mixing low and high detail models it is usually more harmful than useful. This because their combination commonly causes either the calculation of output variables which not correspond to real ones (if a high detail result is expected, but a low detail model is included somewhere in the system's model), or excessive calculation time (if a high detail model is included into a model used to assess low detailed behavior). Moreover, the scope of the simulator has to be defined before its construction, to allow both the application of correct components' models and its correct use. In fact, the hypotheses applied during component's modeling (usually to simplify their mathematical modelization) affect also the complete system's model, making it incapable to evaluate variables (both input and output) which not comply with the applied simplification hypotheses. This is the biggest issue in using mathematical models, because the user tends to forgot that the mathematical models have well-defined validity areas and cannot represent correctly the system outside their validity limits. Due to that, the scope of a simulator must be well defined and must always be kept in mind to avoid misuse. As an example, a model able to simulate system's electromechanical transients can be obtained applying coherent simplification hypotheses to all components and can be used only to assess electromechanical transients. Using it to assess higher dynamic transients will result in wrong results, totally unrelated to reality, while using it to assess lower dynamic transients will lead to excessive calculation times.

Examples of what can be achieved through simulation software can be found in literature, coming from both academic and industry researches. In [103], [102], [38], and [104] simulations are used to assess the effect of relevant disturbances on an IPS, such as high power loads connection and high power motors start-up (the effect of such loads on an IPS is shown in Figure 32, taken from real ship measurements [3]). This allows verifying if the system comply with both regulatory bodies and owner requirements before having built the system, and act accordingly if not. Some examples of the results obtained are shown in Figure 33 and Figure 34, where simulated and real data from a marine application (semi-submersible drilling rig) are compared to show the accuracy level achieved in system modeling. Another example, taken from cruise ships sector, is shown in Figure 35. The figure depicts the simulated and measured switchboard voltage transients due to start-up of a thruster (high power asynchronous motor direct on line).

Conversely, in [100] a software simulator is used as a tool to define and verify a restoring operative sequence, able to avoid system blackout following a generator's sudden disconnection. Doing that it is possible to set the correct procedure in system's automation, removing the need of testing it on the real system until a correct sequence is found. This allows avoiding possible damage to system components.

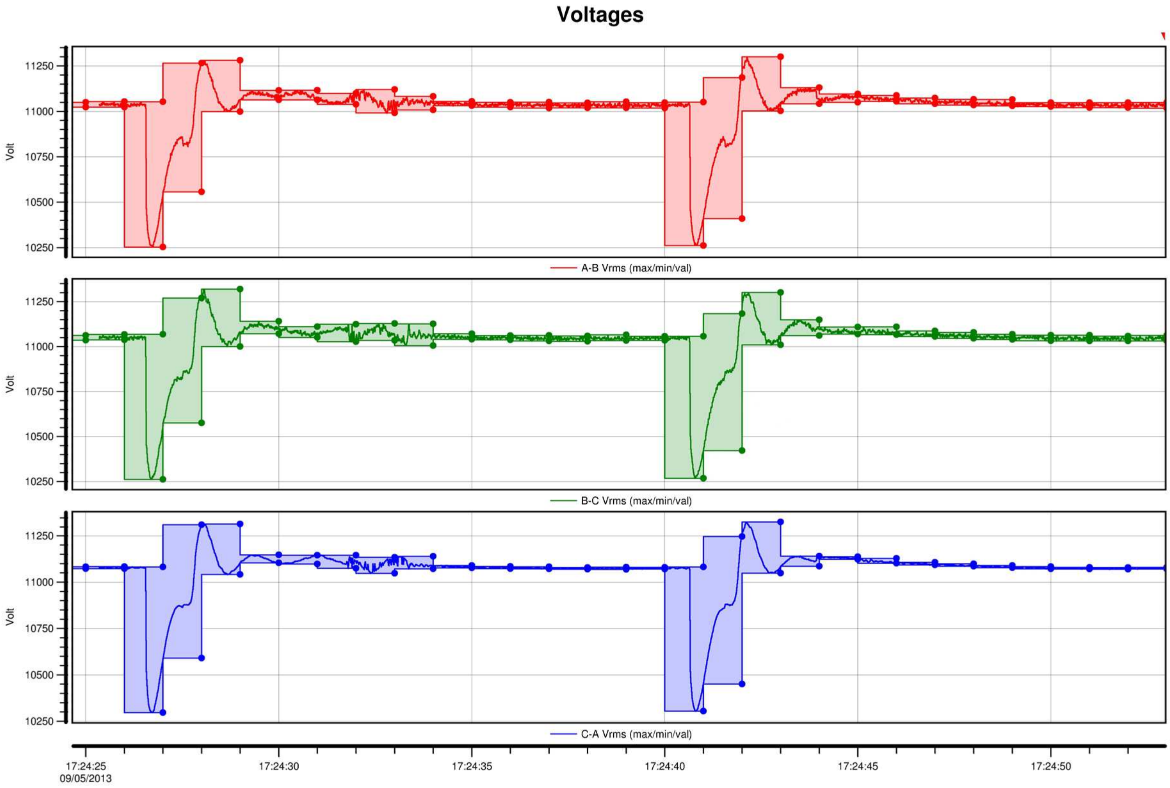


Figure 32 – Cruise liner main switchboard voltage transients due to the start-up of two 2.2-MW thrusters on an 88 MW total generator power IPS, onboard measurement [3].

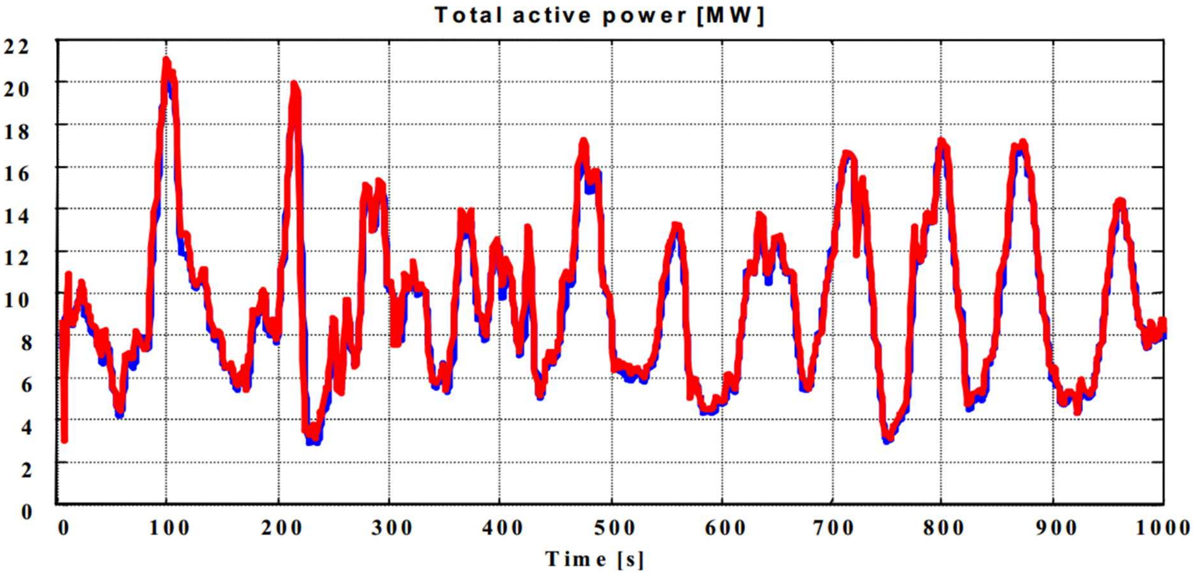


Figure 33 - Measured (blue) and simulated (red) total active power [104].

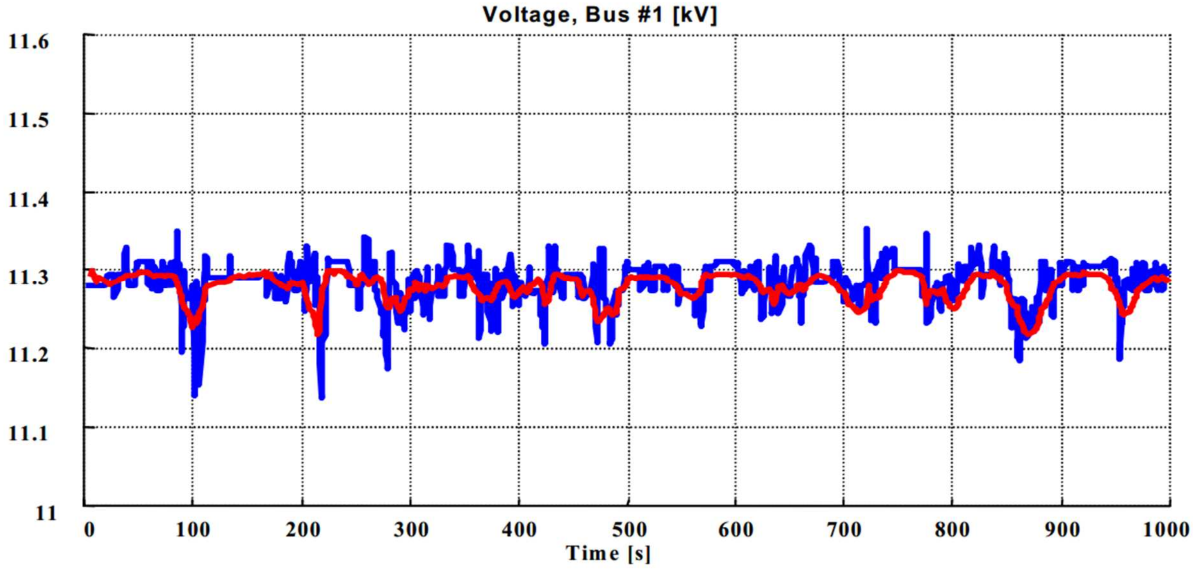


Figure 34 - Measured (blue) and simulated (red) switchboard voltage [104].

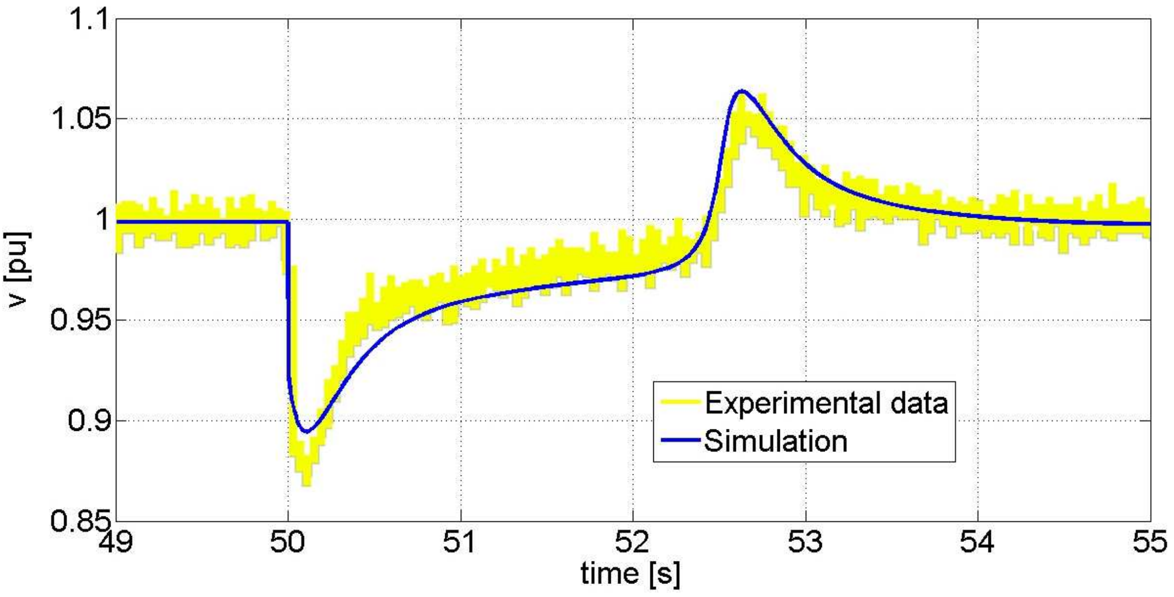


Figure 35 – Switchboard voltage transient during thruster motor direct-on-line start-up [103].

A tuning procedure has to be done, in order to achieve the minimum level of accuracy needed to successfully use a simulator. In fact, thanks to the simplifications applied in mathematical models reasonable simulation times and low computational load are achieved. However, this process also removes from the mathematical models some component's internal phenomena, leading to simulations results that does not match exactly with reality. Hence, a tuning of the simulator has to be done to reduce the differences between simulation and reality results as far as reasonably possible. This procedure can be done by means of mathematical models parameters variation, using data coming from common test performed on system's components. As an example, in shipbuilding industry is common practice performing some qualifying tests on both components to be installed onboard and on complete system, before the delivery of the ship to the customer. In particular, components producers before delivering the components to the shipyard assess their compliance with shipyard requirements through FATs (Factory Acceptance Tests). Data recorded during FATs, mainly voltage and frequency transients, allows tuning generators and motors' models. [3]

Obviously, tuning procedure can be done only if the real component has been already built, leading to believe that such a software will be of little use during design process. This is only partially true. Indeed, the tuning allows obtaining a high accuracy in simulation results. However, during system design such an accuracy may be excessive. In fact, being able to infer the possible behavior of the system in advance can be a great aid for design, even though the results are approximated. Furthermore, in design phase system components are usually not clearly defined, because their parameters can be fixed only in a later design stage. Indeed, during system design the supplier has not been chosen yet. Even if it were, precise component parameters can be assessed only after component building, through the aforementioned FATs. Nevertheless, an estimation of such parameters can be done in advance, sufficiently accurate for the design needs, based on experience and common component data. Although simulations during design stage give different results from the real system, trends and critical issues can be highlighted easily, helping in defining main system layout and controls. Once the system is in construction phase, the simulator can be tuned, thanks to the data coming gradually from the components tests. This allows using the simulator to finely tune control systems and define emergency procedures, without the risk of damage the real system.

4.3.3 HIL testing

As repeatedly remarked in this thesis, nowadays power systems have reached a rather high level of complexity, due to the presence of several control systems and fast actuators. Power electronics led to an increase in performance, together with an increase in system integration. Indeed, having a controllable fast actuator in the system, as power converters are, it is common to demand more and more functions to it. The pros of such a practice are: reduction of the number of separate components to install, thus reducing technical spaces; improved performance, thanks to the use of a single component in spite of several coordinated ones; possibility to add functions in a later moment, by reprogramming converter's control system. These advantages, however, are offset by a significant drawback: the integration of several functions in a single system led to the issue of guaranteeing its correct operation. Ensure correct operation is a primary need for such systems, because no fallback devices are present, and because the integration of many functions in the same system requires that each of them is able to operate without impairing the operation of the other functions.

In this regard, the modern Hardware-In-the-Loop (HIL) test benches allow testing control systems, demonstrating their correct operation before their installation on the field. In fact, HIL tests imply modeling on a suitable hardware and software system the system of interest, up to the desired detail level, with all input/output interfaces necessary to interact with the real world. The system to be tested is connected to these interfaces and act reading measures provided by the HIL simulator and sending to it the appropriate control signals. This allows testing the component as if it is connected to the real system, with the advantage of not risking damaging anything if the control system being tested does not behave as desired [101]. The HIL testing may be carried out at two different power levels, depending on the possibilities given by the hardware/software simulating system and the component being tested. When the test system and the simulator exchange data only at the signal level it is called HIL testing (or CHIL, Control Hardware-In-the-Loop, see Figure 36). Conversely, if the simulation system is capable of working at power level (thus providing also controllable loads and power sources) and the tested component is capable of providing/absorbing power the testing is named PHIL (Power Hardware-In-the-Loop, see Figure 37) [105] [108] [110].

An additional way of applying the HIL testing can be interfacing more HIL systems together via real data buses. In this case, the only hardware part is constituted by the communication interfaces between the systems, removing the need of a real system prototype. Doing that it is possible to apply inputs with real characteristics to simulated systems, such as delays, noise, and disturbances, and assess their impact. This application can be seen as a middle ground between simulations and HIL testing, allowing improving simulation results while avoiding the production of a test prototype. Examples of such an application can be found in [106] and [107], where an HIL hardware is used to emulate the response of an entire MVDC power system while three external FPGA are used to simulate the control system of the converters supplying the main MVDC bus (see Figure 38). The communications between FPGA and HIL hardware are made through real data buses, both for measures and command signals. Analyzing the results the non-ideal behavior of the system is clearly visible, as shown in Figure 39.

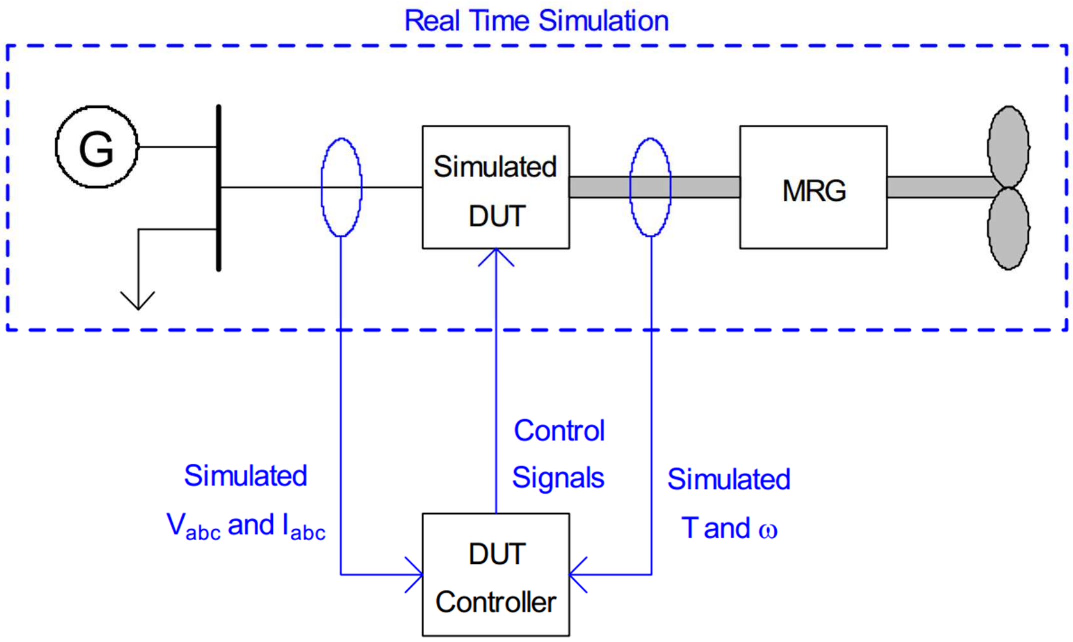


Figure 36 – Conceptual Control Hardware-In-the-Loop system scheme [105].

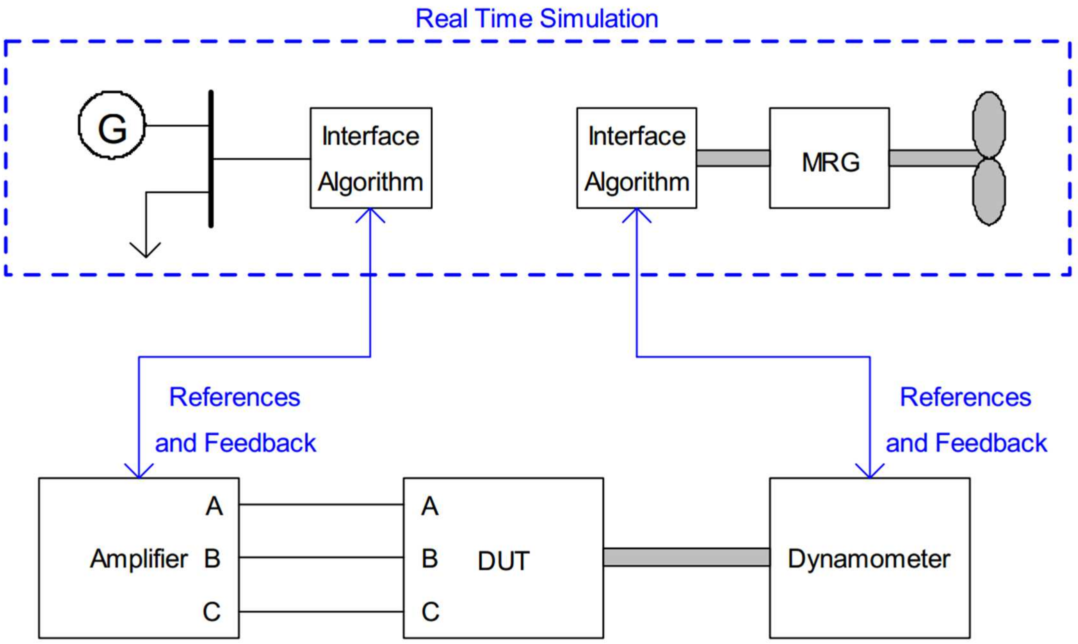


Figure 37 – Conceptual Power Hardware-In-the-Loop system scheme [105].

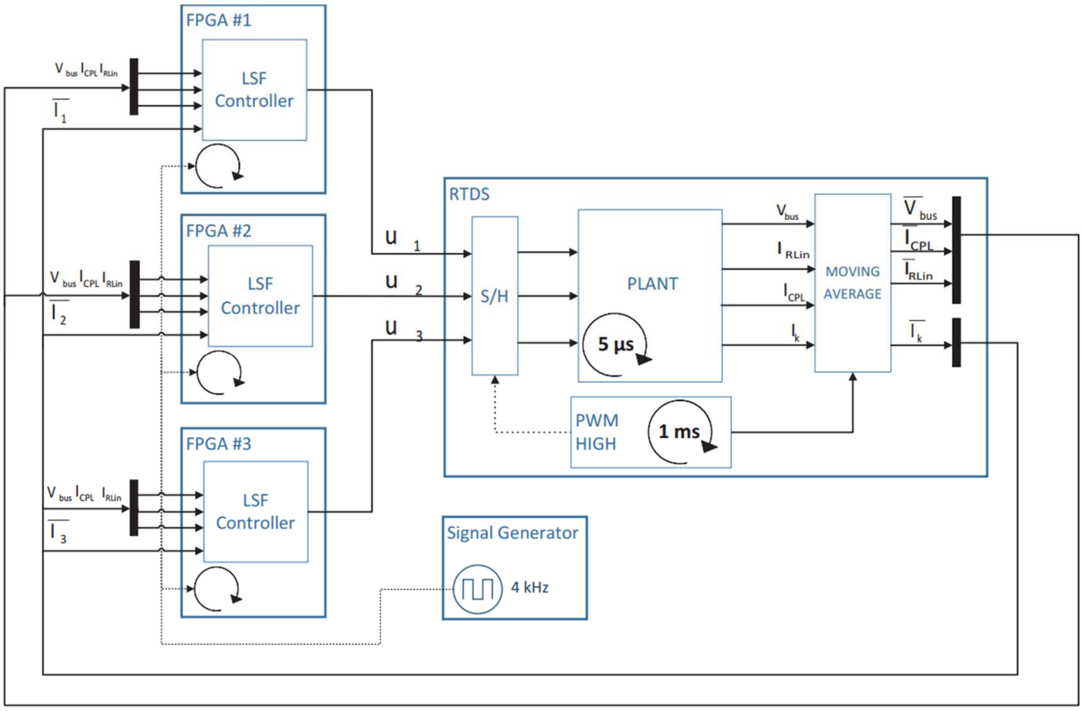


Figure 38 – HIL setup overview [107].

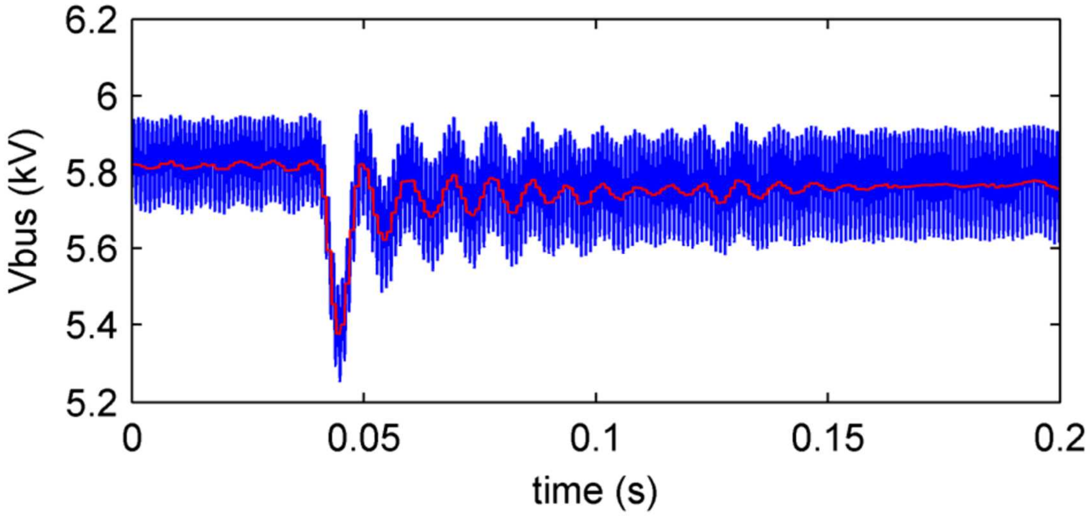


Figure 39 – HIL emulation of the response of a MVDC bus to a load increase (blue – measured voltage, red – averaged measured voltage) [107].

HIL testing commonly need a physical hardware to test, so they should not be considered part of system design. However, its aid in system design could be relevant if proper approach is applied. Indeed, HIL testing is commonly applied in prototyping new systems to demonstrate their applicability in real environment. Such a practice may take place before system design or even in the middle between design and production. In the former case, testing innovative systems will allow proving their correct operation, thus enabling the designers to include them in system design as a viable alternative to conventional components. In the latter case, innovative system design can be tested before commercialization, using HIL test as a de-risking tool (thus allowing identifying critical issues before putting system on the market). Finally, the use of HIL systems connected through real interfaces can be seen as the obvious step to be taken after software simulations, thus complementing them. Indeed, although software simulations offer the opportunity to help in the design of innovative systems, they remain approximations of the reality. Once the system has been simulated, implementing it in an HIL environment allows to get closer to reality even more, due to the possibility to consider the impact of real signals on it.

5 New design process

5.1 Introduction

The previous chapters have given all the information needed to answer to the following questions:

- what are AESs and how are designed nowadays;
- what is the IPS and why it is so significant for an AES;
- which are the issues that may arise from the conventional design process;
- what are the new trends which will increase the difficulty in designing an IPS;
- which new tools are nowadays available to help designers during design process.

In this chapter, an innovative design process will be presented, integrating the new design tools previously depicted, able to solve (or at least mitigate) the issues coming from conventional design and to aid in designing new generation integrated power systems. Such a design process, conceived during the PhD research activity, will be deiscussed focusing on the IPS's design, but it is generally applicable to each sub-system's design, also outside shipboard applications.

5.2 Proposed design process

The goal of the PhD activity was to conceive an innovative design process, easing the design of more efficient, robust, flexible, secure, and performing IPSs. At the same time, such process had to be able to limit the cost increase due to modifications a posteriori on the system, commonly caused by failures in requirements compliance found after vessels construction.

In Chapter 2.2.3 ("Ship design methodologies", at page 33), the conventional design process (spiral design) has been described, together with other innovative methodologies conceived to optimize the ship design. The advantages that such methodologies may give to ships' design are undeniable, therefore their adoption is highly recommended. Actually, the shift towards collaborative concurrent design is already in progress, while design space exploration is still far to be applied (however, some applications to define naval vessels' concept design are done, mainly by US Navy). Due to that, it was deemed pointless defining a completely new process for ship design. However, the advantages that the aforementioned new tools are able to give to the design are clear; therefore, the decision has been to develop a sub-process that integrates such tools. This decision has been taken in order to make the innovative design process as general as possible: whatever the chosen design process will be, it will be possible to integrate into it the proposed design process as a sub-process. This allows achieving the pros given by the use of both dependability theory concepts (fault events evaluation, objective comparison between designs through dependability attributes, etc.) and the possibility given by the software models for the dynamic simulation of electrical systems (evaluation of electromechanical transients after faults, reconfiguration procedures tests, etc.).

The new design process can be modeled with a circular structure (Figure 40) to be inserted within the main design process (of the IPS design, in its described embodiment). Several steps compose it, chosen in order to allow achieving significant advantages from the abovementioned new tools. The concepts on which the process is based are the following:

- Application of techniques given by dependability theory in order to assess which are the most frequent causes of a given top-event (single subsystems and elements faults) and what are the subsystems/elements that have the most impact on the given top-event occurrence (thus defining the most relevant changes in system's design and/or in components' reliability from a dependability point of view);
- Analysis of the system through time domain simulation (steady state and electromechanical transients), in order to obtain data on the dynamic evolution of the system needed to correctly define solutions to the issues highlighted through the dependability analysis, and to verify the correctness of the system design (in respect to regulations/owners requirements);
- Evaluation of the achieved improvements, using dependability theory techniques to assess if the solution is worth the adoption (or not) in terms of dependability indexes.

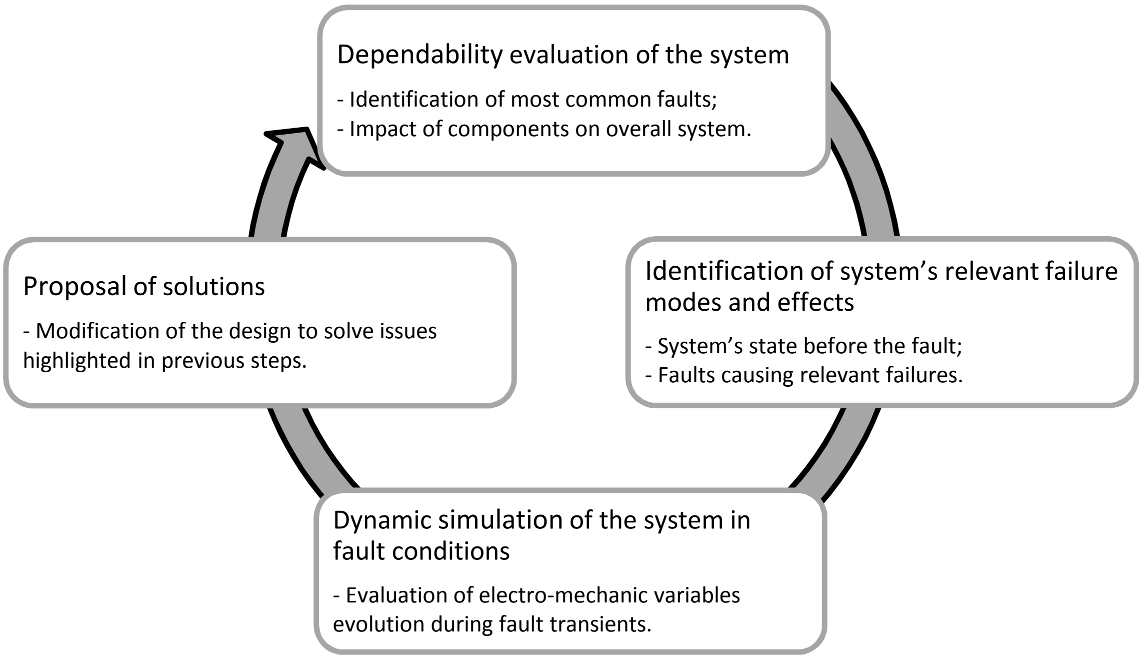

Dependability evaluation of the system
- Identification of most common faults;
- Impact of components on overall system.
Identification of system’s relevant failure modes and effects
- System’s state before the fault;
- Faults causing relevant failures.
Dynamic simulation of the system in fault conditions
- Evaluation of electro-mechanic variables evolution during fault transients.
Proposal of solutions
- Modification of the design to solve issues highlighted in previous steps.

Figure 40 - Innovative design process, subroutine to be integrated into IPS's design

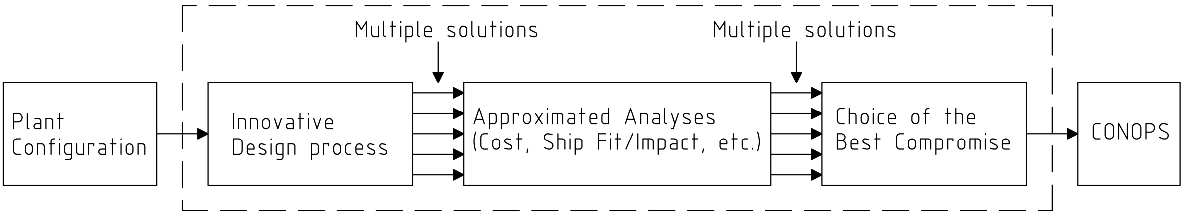

Multiple solutions
Multiple solutions
Plant Configuration
Innovative Design process
Approximated Analyses (Cost, Ship Fit/Impact, etc.)
Choice of the Best Compromise
CONOPS

Figure 41 - Integration of innovative design process in IPS design

The circular process of Figure 40 has to be inserted in a particular point of the IPS design process, due to the information needed to apply the tools. Indeed, the design of the IPS has to be defined together with its main components in order to apply both dependability techniques and software simulations. Due to that, referring to Figure 12 (see page 39), the ideal moment in which applying the new process is right after Plant Configuration step. In this way, the information needed to apply the process are available, and the process can be used to modify the design before additional time-consuming steps are made. Nevertheless, some of the steps that follows Plant Configuration in IPS design process may be relevant for the new design process (mainly Cost, Ship Fit/Impact, Static System Analysis, and Power Quality).

In fact, the new design process allows defining solutions to issues emerging from the dependability study of the system, and choosing between them following a dependability based metric. However, in ship's design also other constraints apply, such as costs and space/volumes issues. Due to that, a smart solution may be to perform Cost and Ship Fit/Impact analyses on each solution resulting from the new design process. The results of such analyses will allow selecting the most fitting solution considering all the impacting variables. The impact in terms of human and time resources of these additional analyses has to be limited, in order to avoid increasing the design effort. Due to that, a higher grade of approximation in respect to main design process can be applied to evaluate the possible solutions, and detailed analysis can be made only on the chosen design. The resulting process may be something similar to what depicted in Figure 41, where the new design process is used to find issues in the design and propose solutions. These solutions can be then evaluated, and the best compromise can be chosen to be applied in the final ship design.

The proposed design process needs detailed information on the system to be able to give all its advantages, thus being ideally applicable from functional design onwards. However, its application it is not limited to such an advanced phase of the design. Indeed, preliminary design can greatly benefit from such a process, being possible to address main system issues in a phase in which high impact solutions can be implemented without excessive modification effort. Even though the information about the system is scarce in preliminary design phase, it may be sufficient to perform an approximated dependability analysis and to perform some simulations of system's dynamic behaviour based on common components' data. Such analyses will be able to identify main design flaws, and guide the designers in the choice of the system architecture most suitable for the application.

The proposed approach seems to lead to an increase in design complexity due to both the additional design steps and techniques, but, in fact, the result is a simplification in the design. Indeed, such a process allows to design relying on methodologies useful to systematically define: critical points of the system, redundant elements to be inserted or removed, best solutions to get the required response to fault events, and also to objectively demonstrate the quality of the design to all those concerned. Doing that, it is possible to avoid the "trial and error" procedure commonly used to find solutions in case of unforeseen issues, which is the most impacting activity to do during design in term of human, time, and financial resources. Conversely, in an already well proven design devoting some effort to apply such an approach may lead to advantageous results, due to the possible design optimizations that can be deduced (thus increasing performance, decrease weights/volumes, decrease costs, and improve dependability attributes). In fact, it is demonstrable that the integration of dependable design and software simulation in such processes can be obtained with bearable effort, due to the possibility of using an already present ship design substrate. In particular, in [97] it is shown how dependability techniques can be used as a project management tool in ship design, and how these techniques can be integrated into present design tools in the least impacting way. Considering the most demanding AES application in merchant area, which are DP vessels, proposals to consider the adoption on dependability techniques during throughout all the design process are available in literature, such as in [96]. For what concerns dynamic simulations aid to system design, it has to be pointed out that such an application is already in study in most advanced IPS's components suppliers, such as ABB [104]. Moreover, as previously affirmed the new IEC 61892-5 [99] will oblige to perform HIL testing on the main shipboard control systems to ensure they are suitable for the purpose.

5.3 Analysis of the proposed design process steps

In the previous section the concept of the proposed design process has been given, together with considerations about its introduction as a sub-process in the IPS design procedure and its possible application already in early stage design. However, it is necessary to analyze each step of the innovative process to comprehend how it has to be applied and which activities have to be performed to achieve the intended results.

The first step of the process is the dependability evaluation of the system. It implies applying one of the fault-forecasting techniques described in Chapter 4.2.2 (page 66 ff.) in order to assess system failure modes and dependability attributes. In particular, among the techniques abovementioned the most suited for the application is the Fault Tree Analysis (FTA). Indeed, FTA allows not only assessing all the possible causes of a given failure (the top-event), but also allows translating the resulting fault tree into mathematical relations, thus making it possible the calculation of particular indexes relevant for the purpose of applying the proposed design process. During the failure tree construction, the interrelations among system components become evident, and can be assessed how single components' faults impact on the occurrence of the system's top-event. Through the application of component's failure data, it is possible to perform some significant calculations, with the aim of evaluating dependability indices relevant for the design process. In particular, the following mathematical figures can be deemed relevant for the application of the innovative design process: failure frequency, n° of expected failures in lifetime, total downtime, Fussell-Vesely and Birnbaum importances.

To calculate them, the first step to do is to identify the cut sets of the system, which are defined as: the unique combinations of component failures that can cause the system's top-event. If considering a single gate, the related cut sets are the ones able to cause that gate to have a TRUE output. In the following will be always made reference to gates to keep formulas as general as possible. Indeed, in FTA the top-event is also a logic gate. Due to that, the formulas depicted hereinafter allow evaluating both the indexes for normal gates and the top-event.

The failure frequency of each cut set can be determined with:

$$\omega_{cut} = \sum_{j=1}^{n} \omega_j \prod_{i=1, i\neq j}^{n} Q_i \tag{5.3-1}$$

where Q_i is the unavailability of the ith event of the cut set; n is the number of events in the cut set; ω_j is the failure frequency of the jth event in the cut set.
The unavailability of each cut set can be calculated as follows:

$$Q_{cut} = \prod_{i=1}^{n} Q_i \tag{5.3-2}$$

For what concerns gate unavailability calculation, it depends on the method applied: Rare Approximation, Cross Product, or Esary-Proschan.

The Rare Approximation method gives the following simple expression for the gate unavailability:

$$Q_{gate} = \sum_{i=1}^{n} Q_{cuti} \tag{5.3-3}$$

where Q_{cuti} is the unavailability of the ith cut set.

Conversely, the Cross Product unavailability calculation is rather complex:

$$\begin{aligned} Q_{gate}(t) = \sum_{i=1}^{n} Q_{cuti}\,(t) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} Q_{ij}(t) \\ + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} Q_{ijk}(t) + \cdots (-1)^{n+1} Q_{123\ldots n}(t) \end{aligned} \tag{5.3-4}$$

where Q_{ij} is the product of the unavailabilities of the basic events in cut sets *i* and *j*; Q_{ijk} is the product of the unavailabilities of the basic events in cut sets *i*, *j*, and *k*.

Finally, the Esary-Proschan expression for gate unavailability is:

$$Q_{gate} = \prod_{i=1}^{m} Q_i \left[1 - \prod_{j=1}^{n} \left(1 - Q_{cutj}\right) \right] \tag{5.3-5}$$

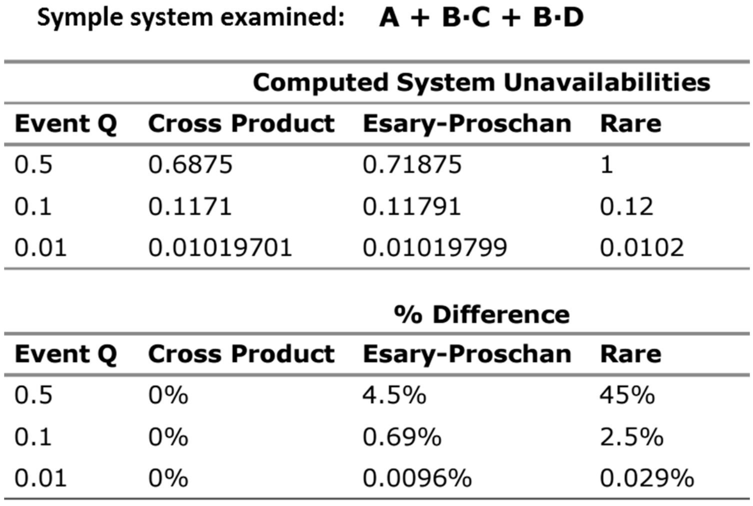
where Q_i is the unavailability of common event *i* occurring in all cut sets, *m* is number of common events occurring in all cut sets, Q_{cutj} is the unavailability of cut set *j* excluding common events; *n* is the number of cut sets.

The choice between Rare Approximation, Cross Product, and Esary-Proschan method is due to the complexity of the system:

- Rare approximation is an extremely simplified method, which takes Cross Product formula and truncates it to the first term. It is the fastest method, but leads to high errors in evaluating attributes. However, it can be used in complex systems to determine the upper bound level of the attributes (the most pessimistic level).
- Cross Product is an exact method, which implies calculation of all the interdependencies between components. However, related calculation is complex, becoming more and more difficult to perform as system's complexity rises;
- Esary-Proschan method allows approximating and bound system's unavailability through application of order reduction techniques. It allows calculating system's attributes in complex systems lowering the calculation effort in respect to Cross Product method, but remaining still fairly accurate.

To explicit how such methods approximate the real value, an example taken from the help of the software that will be used in Chapter 6 to perform dependability analysis (Isograph® Reliability Workbench®) is shown in Table 10.

Table 10 - Errors due to approximation is dependability attributes calculation



Symple system examined: **A + B·C + B·D**

	Computed System Unavailabilities		
Event Q	**Cross Product**	**Esary-Proschan**	**Rare**
0.5	0.6875	0.71875	1
0.1	0.1171	0.11791	0.12
0.01	0.01019701	0.01019799	0.0102

	% Difference		
Event Q	**Cross Product**	**Esary-Proschan**	**Rare**
0.5	0%	4.5%	45%
0.1	0%	0.69%	2.5%
0.01	0%	0.0096%	0.029%

After having defined such formulas, it is possible to calculate all the above-mentioned dependability indices:

- Failure frequency;

  It is the number of failures per unit of time measurement (here fixed as one year). In case of fault events it can be calculated knowing failure rate and MTTR. The appropriate formula to be used depends on the failure model chosen for the single component, therefore will be not shown here. Conversely, single gates failure frequency can be calculated using the formulas given in the following.

  If Rare Approximation method is applied, the failure frequency related to the gate is calculated as follows:

$$\omega_{gate} = \sum_{i=1}^{n} \omega_{cuti} \tag{5.3-6}$$

  where ω_{cuti} is the failure frequency of the i^th^ cut set.

  If Cross-Product method is applied, the failure frequency related to the gate has to be calculated by summating or subtracting the frequencies for all cut set cross-product terms. Such a formula is not shown here due to its complexity.

  If Esary-Proschan method is applied, the failure frequency related to the gate can be calculated as follows:

$$\omega_{gate} = \sum_{i=1}^{n} \omega_{cuti} \prod_{j=1, j\neq i}^{n} (1 - Q_{cutj}) \tag{5.3-7}$$

  where Q_{cuti} is the unavailability of ith cut set.

- N° of expected failures in lifetime;

  It is the number of failures that could occur in the system lifetime T (which is defined by designers). It can be calculated as:

$$W_{gate} = \int_0^T \omega_{gate}(t)\, dt \tag{5.3-8}$$

  Such an index is related to failure frequency; therefore, it can be used in place of failure frequency if preferred by the designer. However, the "expected failures in lifetime" depend also on system lifetime; due to that it can be used to compare systems with the same imposed lifetime only (while failure frequency is not "lifetime dependent").

- Total downtime;

  It is the total time a single gate will remain "failed" in lifetime T:

$$TDT_{gate} = \int_0^T Q_{gate}(t)\, dt \tag{5.3-9}$$

Such a value obviously depends on both the frequency of failures and the time it takes to repair the failed component (MTTR).

- Fussell-Vesely Importance;

  The Fussell-Vesely importance indicates the contribution of a single gate/event to the overall system's unavailability. It can be calculated for the i^{th} component as follows:

$$I_i^{FV} = \frac{Q_{sys} - Q_{sys}(q_i = 0)}{Q_{sys}} \qquad (5.3\text{-}10)$$

  where Q_{sys} is the system's unavailability, $Q_{sys}(q_i=0)$ is the system's unavailability with the unavailability of i^{th} component set to 0 (which means never faulted component).

- Birnbaum Importance.

  The Birnbaum importance measure the sensitivity of system's unavailability with respect to changes in i^{th} component's unavailability. It can be calculated through the following formula:

$$I_i^{BB} = \frac{\partial Q_{sys}}{\partial q_i} \qquad (5.3\text{-}11)$$

  where q_i is the unavailability of the component i.

The dependability indices depicted above give significant information about the power system in course of design. Failure frequency (or similarly the n° of expected failures in lifetime) allows comprehending which will be the most frequent faults on the designed power system, thus allowing concentrating design effort in lowering either their occurrence or their impact on the system. Fussell-Vesely (FV) and Birnbaum (BB) importance indexes, on the contrary, allow defining how the system can be improved, pinpointing single components or sub-systems which need to be redesigned or upgraded. Indeed, through the comparison of FV and BB it is possible to define: if a subsystem/component has to be improved in terms of its inherent dependability attributes (such as MTBF, failure rate, etc.), if the design of the system integrating such component/subsystem has to be modified, or if such component/subsystem may be left untouched. The combinations of FV and BB indices are shown in Table 11, together with the potential action to be applied to improve the system [111].

Table 11 - Possible improvements determination through FV and BB importance indices evaluation [111]

FV	BB	Possible improvements
High	High	Component/subsystem, system design
High	Low	Component/subsystem
Low	High	Avoid component/subsystem degradation
Low	Low	None (possible relaxation)

The four possible combinations lead to four possible improvements, arising from a reasoning that is rather simple to comprehend if the meaning of FV and BB is known:

- A high FV index means having a component/subsystem whose attributes have a high impact on the system's unavailability. A high BB index means having a system design that is poorly defended from the component/subsystem failure. Due to that, it is possible to act improving the component/subsystem (to lower its possibility to fail) or redesigning the system (to lower the impact the component/subsystem has on system).
- A high FV index means having a component/subsystem whose attributes have a high impact on the system's unavailability. A low BB index means having a system design that is well defended from the component/subsystem failure. Due to that, the redesign of the system is not required (because already well done), but the component/subsystem dependability attributes needs to be improved (to improve overall system's attributes).
- A low FV index means having a component/subsystem whose attributes have a low impact on the system's unavailability (commonly because their value is already good). A high BB index means having a system design that is poorly defended from the component/subsystem failure. In this case, the redesign of the system is not required, because the impact of the subsystem/component on the overall system is low, but it is necessary to avoid degradation in such a component/subsystem in order to avoid an increase in its possibility to fail (it is commonly attained through proper maintenance).
- Having both low FV and BB indices means having a component/subsystem which has a low impact on the system and whose fault is coped easily by the actual design. This case does not require improvement, but opens space for possible relaxation. Indeed, really low values for FV and BB indices means having both a component/subsystem with high availability and a system design that allows the correct operation also in presence of the component/subsystem fault. This may imply two different "incorrect" design practices:

    1. having put an excessive effort in reaching high dependability attributes for the component/subsystem (which imply a significant cost to design, to buy, and to maintain such a component/subsystem), if the design is taken as a fixed point;
    2. having conceived an excessively complex design to lower the impact of such a component/system fault on the system (which imply a significant design and installation cost), if the component/subsystem attributes are taken as given.

    Due to this, it is possible to simplify the design, obtaining as a side effect also a reduction in costs and volumes of the system. Otherwise, it is possible to use a component/subsystem with slightly worse dependability attributes, saving on its costs.

As can be seen in Table 11, the evaluation of FV and BB allows an intervention on design which is focused on the overall system improvement. This avoids off-the-cuff interventions, which commonly lead to an increase in system complexity and costs without ensuring the desired improvement.

The second step of the proposed design process is a phase of preparations for the dynamic simulations to be done in the third step. In fact, it is necessary to analyze the outcomes of the dependability analysis to define which the dynamic simulations to be done are. This imply identifying the system's failure modes and effects relevant for the design, to determine which fault scenarios have to be simulated and which is the system's condition before the fault which leads to the considered top-event.

The identification of the fault events to be simulated can be done analyzing the failure frequency of all the gates and events in the system, which are available because of the dependability analysis. Most frequent components' faults are the first to be considered. Among them, it may happen to found some faults already considered by requirements (as shown in chapter 1.4.3, at page 17). However, requirements depict clearly only main subsystems' faults (such as generators' fault or thruster faults), while dependability analysis is able to highlight also more specific faults (such as a sensor fault, or a breaker fault) depending on the detail used during the FTA. The suggestion here given is to consider both faults imposed by requirements and most frequent faults highlighted by the dependability analysis. This avoids leaving possible faults unconsidered, thus allowing to improve the system design comprehensively. Not only base fault events, but also the fault frequency data of the fault tree gates must be taken into account. This has to be done because such data is able to highlight the composition of single events that may lead to a frequent cause of failure, despite being events singularly infrequent. The simplest example of such a behavior is an OR gate with two single fault events as inputs: the OR gate failure frequency is the sum of the failure frequencies of the two input events, because the fault of one of them is sufficient to achieve the failure of the gate, thus resulting in a more frequent event.

After having identified the events that likely will happen in the system, it is necessary to define which have to be simulated. Being simulations a time consuming activity, it is necessary to make a choice between all the possible fault events. If a complete dependability analysis has been done, considering all the possible system configurations and all the possible harmful top-events, it is sufficient to extract from each case the most frequent events that leads to the top-events. The composition of all these events is the set of failure modes to be simulated, and the system state before the fault is given by the analysis of the faults leading to such events (which can be easily done through the failure tree diagram examination). Otherwise, if such a complete analysis is infeasible (due to resources constrains), it is needed a reasoning activity by the analyst to infer the possible outcomes, in terms of impact on system operation, from the list of the most frequent events. In this case, also events not leading to the top-event have to be considered because these may lead to another top-event that have not been analyzed. This process is more qualitative than quantitative, and must be done with an approach similar to an FMEA (refer to chapter 4.2.3, page 77 ff.).

Up to this point, dynamic simulations have not been done yet, but the outcomes of the dependability analysis are already sufficient to allow improving the common design procedure, focusing the designers' effort on the most relevant issues of the system.

The third step to be done is the simulation of the dynamic evolution of the system in response to the failure events identified in the previous design step. As affirmed in Chapter 4.3.2 (page 93 ff.), a complete mathematical model of the system can be achieved. However, the software implementation of such s detailed model would require a high amount of resources to run due to the complexity of IPSs. Due to that, it is necessary to limit the detail of the model focusing onto the transient most relevant for the application. In such a way, the overall system behavior can be simulated through the software in a bearable time, also on common personal computer (thus not requiring dedicated hardware). More detailed simulations can be achieved through dedicated hardware, such as in HIL testing, but requiring both higher time and knowledge resources in order to being implemented. Due to that, the suggested approach is to define a model of the system that has reduced detail (thus having a reduced calculation time impact), while retaining the capability to simulate the system's transients relevant for the design. Leaving out the fast transients given by protection operation, which depend on parameters difficult to assess during design, the most significant behavior to be assessed in an IPS is how its main electrical variables evolve following a perturbation. The variables of interest in IPS design are mainly voltage and frequency in AC and voltage in DC, while perturbations may be: reconfigurations of the system, connection/disconnection of a generator or a load, variation of a reference in real-time control systems, etc.

The most significant transients to be simulated and evaluated pertain to the electromechanical transient area, which means transients whose time constant allows modeling the system on the assumption of neglecting transformer *emfs* (fast voltage and current changes already under steady state conditions) [109]. Indeed, simulating system behavior in electromechanical transients' domain allows defining the impact of the design variables that are commonly defined during IPS design: size and number of generators, setting of voltage and frequency controls, power system architecture, and PMS response to system events (such as reconfigurations, start/stop of generators, and load shedding). In this way, it is possible to make use of the simulations in order to foresee the impact of design choices on system's behavior, thus allowing defining the most suitable design. Conversely, detailed models' use can be limited to the case of peculiar issues presence. As an example, mathematical models able to show the electrical transients on the system can be applied to assess over-voltages caused by vacuum circuit breakers operation, but only if such a behavior proves to be an issue on the real system. Indeed, the simulation of a whole ship's IPS to assess electric transients behavior needs a level of detail so high to became practically infeasible during system design. This happens mainly due to the lack of proper system data (in this case, also parasitic elements are relevant, which can be assessed properly only on the built system). Due to that, such a detailed simulation can be used only if unforeseen issues arise, both as a tool to gain knowledge on system's improper behavior and as an aid in finding solutions. Conversely, its usefulness during design is questionable.

Having defined the detail of the mathematical models to be used to build the software simulator, it is possible to implement them into the software, connecting their input/output each other in order to obtain the complete system's model. Such an operation, despite seeming easy at a first sight, it is not. Proper knowledge is required to both obtain the system's simulator and to evaluate the results of the software. In fact, the simplifying hypotheses (applied to reduce the detail of the models) lead to the presence of transients that not perfectly match real systems ones in certain situations. As an example, the electromechanical transients' hypothesis removes the derivative components from loads inductances and capacitances (because electric transients are not of interest). Due to that, when calculated through a model tailored on electromechanical transients loads insertion/disconnection are characterized by a step current rise/fall, which is obviously not what happens in real systems. However, the rest of the transient approximates well what happens in the system, thus making it possible to successfully use such a model to assess system's behavior. Once the system's model has been implemented into a software and the designers have gained the proper knowledge to interpret results, it became possible using it as an aid in design.

Another issue related to the use of software simulators is the correctness of the parameters to be set for system's components. Such parameters are the ones of the components that have to be installed in the real ship, which means knowing them exactly only at detailed design phase. Due to that, simulations done during basic design phases have to be based on the most probable parameters the components will have, thus implying a certain grade of approximation. This issue is common in ship design: as previously mentioned in Chapter 2.2, the most impacting decisions are taken when the less is known about the system. Luckily, sufficient knowledge of marine power systems allows guessing values for components' parameters that are very similar to real ones. Moreover, the design process is made in such a way to allow integrating new information at the moment they become available, so new simulations can be run to assess if the design defined previously can be kept or needs to be modified.

The proposed design process imply using the simulator to evaluate the system electric variables transients following the fault events defined in the previous steps. During the second step, such events have been clearly defined together with the system configuration in which these events lead to a failure. In this step, all these events are simulated and the results are collected. The evaluation of the electromechanical transients allows comprehending how the system dynamically moves from the correct service condition, before the event, to the faulted condition, thus highlighting possible areas of improvement. As an example, if a fault event leads to a system failure due to under-frequency protections triggering, some different areas of intervention can be identified. These can be: modification of protection trigger levels, modification of SG settings, load-shedding, modification in system configuration to ensure more generators running or to avoid the single fault effect propagating to the whole IPS, and so on.

The fourth step involves the definition of corrective solutions for the failure events simulated in step three. In the previous step some areas of intervention have been identified for each simulated fault event. Now design solutions able to intervene in the identified areas have to be found, trying to conceive them as less impacting on design as possible. Indeed, solving one issue may cause the birth of another issue, or may lead to system designs not compliant with requirements. As an example, a possible solution to the example made above (the under-frequency trip) may be the connection of two main switchboards through the tie-breakers, to ensure the presence of more running generators. However, the owner could have specified as a requirement the open-bus configuration for the system in the operational condition in which the issue arise, so this solution is not feasible due to its non-compliance with requirements. Obviously, all the feasible solutions proposed by designers have to be validated through simulations of the system behavior, to assess if these are able to solve the issue and at the same time does not cause other issues. More than one solution can result from such a process. Due to that, each of them have to be evaluated and results have to be saved for the following step. The solutions that both have proven to be able to solve the issues and are feasible can be implemented in the design. Having possibly proposed more than one solution for each problem, multiple designs origin from this step.

At this point, the process returns to the first step: the dependability analysis. The multiple designs given by the previous step need to be analyzed through dependability techniques, to assess the attributes and the failure frequencies resulting from each design. Comparing the dependability analysis results of each solution it is possible to discard the ones leading to the lesser improvement (or even leading to a deterioration). As an example, the closed-bus operation may solve the under-frequency issues depicted above, but may cause an unbearable rise in failure frequency due to the interactions between switchboards, which were not present before due to the electric separation.

It must be remarked that the dependability analysis helps in defining the most suitable design solutions between all the ones conceived, but the suggestion here given is to avoid selecting a single solution. The smartest design procedure is to select the most attractive designs (how many to choose is up to the designer) as the output of the innovative design process: each of them is a solution able to both solve the issues highlighted during the design and improve the dependability of the system. The final decision on which implement has to be made following the most significant constraints in AES IPSs, which are costs, space, and volumes. Indeed, all the attractive design solutions have to be evaluated in terms of these three parameters, as shown in Figure 41, and the one presenting the best compromise in these three terms can be finally selected as the one to be implemented.

6 Case study

6.1 Introduction

The final chapter is focused on a case study, used to demonstrate the applicability of the proposed design process. After an outline about the system to be analyzed, the chapter proceeds presenting both parameters and data about the case study. Then, the application of the innovative design process steps is made, dicussing extensively each passage in order to clarify the achievable results and the possible outcomes of the analyses done.

6.2 Oil & Gas Offshore Vessels

Oil & Gas industry is one of the most capital intensive activities in the whole world. Its importance in the world economy is undoubtable, and significant effort is given to research of new oil fields and to extraction of the related resources. Oil & Gas industry is divided into three main sectors, tied to the three main phases of the Oil & Gas resources exploitation:

- upstream:
    - exploration (search for the oil/gas fields);
    - preparation of production wells (and installation of related subsystems);
    - extraction;
- midstream:
    - transport of the resources from extraction point to refinery
    - storage;
- downstream:
    - products refinement;
    - sale of derived products.

Both offshore and onshore units are used in upstream phase, depending on the location of the oil field: offshore is related to seabed fields, while onshore is related to fields on land. In this thesis, the focus is given to vessel's design, due to that only offshore units are considered.

Exploration and extraction phases are performed by units structurally identical, differing in the onboard installed subsystems. Indeed, exploration phase require high unit mobility and versatility, due to the need of adapting to different locations and geological seabed conditions, while production phase units are mostly stationary and single-task oriented. Due to that, the exploration units are commonly used only to find the oil field, leaving the extraction work to a dedicated unit that will arrive in the production area later. This specialization lead to a wide range of offshore units, which can be divided by scope of work (exploration or production), mode of operation (floating or fixed, anchored to the seabed or dynamic positioned), and structure (platforms/barges or ships).

The main units used in exploration are: jack-up rigs (jack-ups); semi-submersible platforms (semi-subs), drilling ships (drillships). All of them are floating, but jack-ups have rigid legs fixing them to the seabed during operations, while semi-subs and drillships are dynamic positioned (Figure 42). Conversely, a wider range of units are used in production phase, such as: fixed platforms, tension-leg platforms, spar platforms, gravity platforms, Floating Production Storage and Offloading units (FPSOs). Each of them have peculiarities and different modes of operation, which will be not given in this thesis work. Among all these, floating units endowed with DP are the most significant ones to analyze with the aim of applying the innovative design process, aim of this thesis. Due to that, the discussion will focus on semi-sub and drillship units only.

The semi-submersible platforms (Figure 43) can be considered vessels, because these units are capable to float and move on their own (through the use of the DP thrusters). These platforms have a main plain section, which houses the drilling equipment, the hotel area (for the crew), and all the other subsystems needed to correctly operate the vessel (such as power stations, storage tanks, and so on). The main section is installed over columns that are connected to submersed hulls, which allows obtaining the needed buoyancy. Semi-subs can work on very deep waters (currently up to 3000 meters, but industry is pushing towards deeper waters). The semi-subs use their thruster both to achieve dynamic positioning and as main propellers for navigation, although maximum speed is reduced due to the shape of the vessel. However, if high speed is required, tugs can be used to make transfers faster. In function of the maximum depth of water in which they can operate (but also depending on the type of propulsion), the semi-subs are classified into generations. The sixth generation is currently used, that is self-propelled platforms able to work in DP at about 3000 meters (10000 feet) depth. Regarding drillships, the onboard systems are similar to semi-subs ones. The substantial differences is to be attributed to the structural form of the unit, which is ship-like for drillships (Figure 44). In fact, drillships have the hull shape of a conventional ship, but with a hole on the bottom used to make it possible the passage of the drill (called *moon pool*).

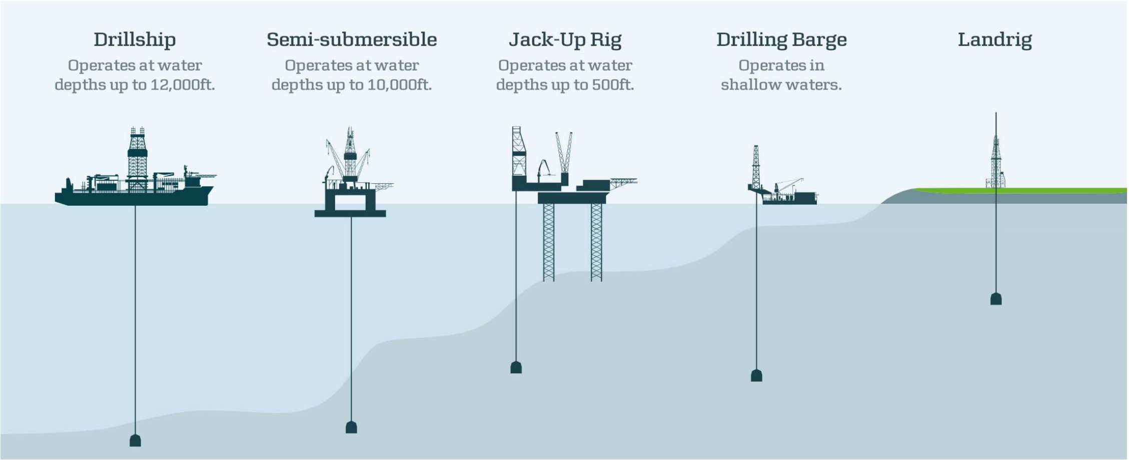

Drillship
Operates at water depths up to 12,000ft.
Semi-submersible
Operates at water depths up to 10,000ft.
Jack-Up Rig
Operates at water depths up to 500ft.
Drilling Barge
Operates in shallow waters.
Landrig

Figure 42 - Oil & Gas units used in exploration phase [112]

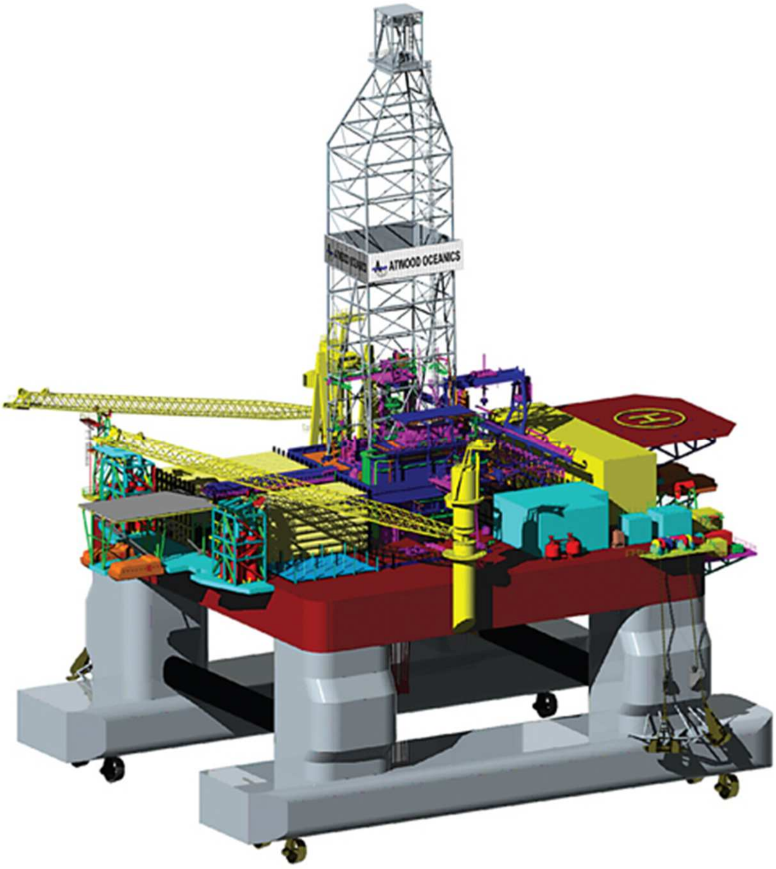


Figure 43 - 3D rendering of a semi-submersible drilling platform

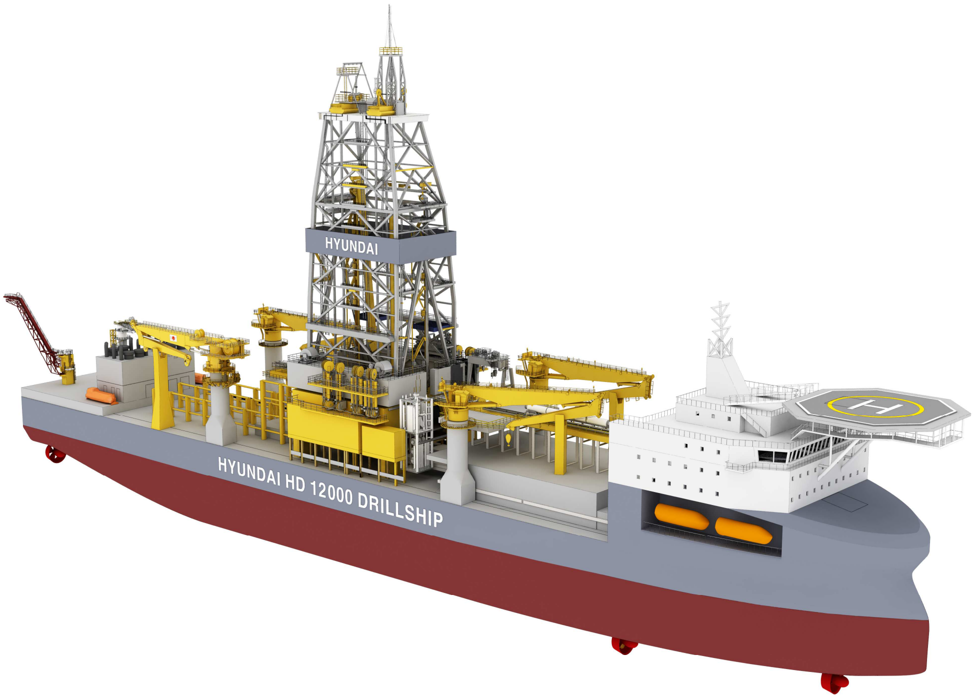


Figure 44 - 3D rendering of a drilling ship

Aside from the hull shape, the main difference between semi-subs and drillships is the so-called Variable Deck Load (VDL), which is the amount of load variation that can be managed by the unit without impairing its buoyancy and DP characteristics. In fact, semi-subs can weight much more than drillships, but the amount of VDL is lower due to the lower water displacement given by their structure in respect to drillships. This affect unit operation, because having lower VDL means the need of being supplied by land more frequently (with fuel, fresh water, and so on). This in turn means more operational costs, so drillships are commonly preferred if possible. However, VDL is not the only factor affecting the decision of the most suitable unit for a given exploration activity. In fact, other characteristics related to the unit structure are relevant, and may tip the balance in favor of either. In Table 12 are shown the main advantages of both the structures, whose comparison aids in comprehending which applications are most suited for each structure.

Table 12 - Characteristic of semi-subs and drillships

Semi-submersible platform	Drilling ship
Suitable for high waves	Not suitable for high waves
Slower cruise speed	Higher cruise speed
Small floatation area	Large floatation area
Low VDL	High VDL
Isotropic shape	Anisotropic shape (possible arousal of harmful resonances due to wind and waves)

6.3 Dynamic Positioned Drillship (class DPS-3)

6.3.1 System data

The case study selected to demonstrate the applicability of the innovative design process, described in Chapter 5 (page 103 ff.), is the IPS of a DP drillship classified in Class DPS-3 following ABS rules. Such a case has been chosen due to the strict requirements DP vessels have, whose impact on IPS design is the highest among all vessels in merchant area, as demonstrated in Section 1.4 of Chapter 1 (page 12 ff.). An example of DPS-3 vessels' IPS has been given previously, in Figure 4 at page 9, showing how complex such power systems became in order to avoid harmful consequences in case of faults [9]. Several redundant IPS sections are commonly present in DPS-3 classified vessels, to allow supplying the correct service also in case of a major failure event (the Worst Case Failure). In particular, common solution is to install three or four sections, while higher modularity can be used to lower the generator's power requirements. Such a structure comes mainly from requirements 3/1, 3/3.3, 3/5.1, and 3/5.3 of ABS Guide for Dynamic Positioning Systems [22]. (Also other requirements from the same document can be relevant. Refer to Section 1.4 of Chapter 1 for more information.) An example of a power system with a high number of equal sections is the one installed onboard of the Deepwater Horizon, shown in Figure 45 (only port side half, starboard side is similar). However, such a complex structure was not enough to prevent the environmental disaster in the specific case, due to the occurrence of an event whose impact overcame the worst case failure design intent: a well blow-out (uncontrolled rise of a mixture of gases, oil, and mud from the well) of an unforeseen magnitude. The following cascaded events have led to the outcomes known to everybody [113]. In such a case, investigation pointed out a poor decision making process as having the key role, highlighting once again the need of a coherent and systematic process to design and manage critical systems.

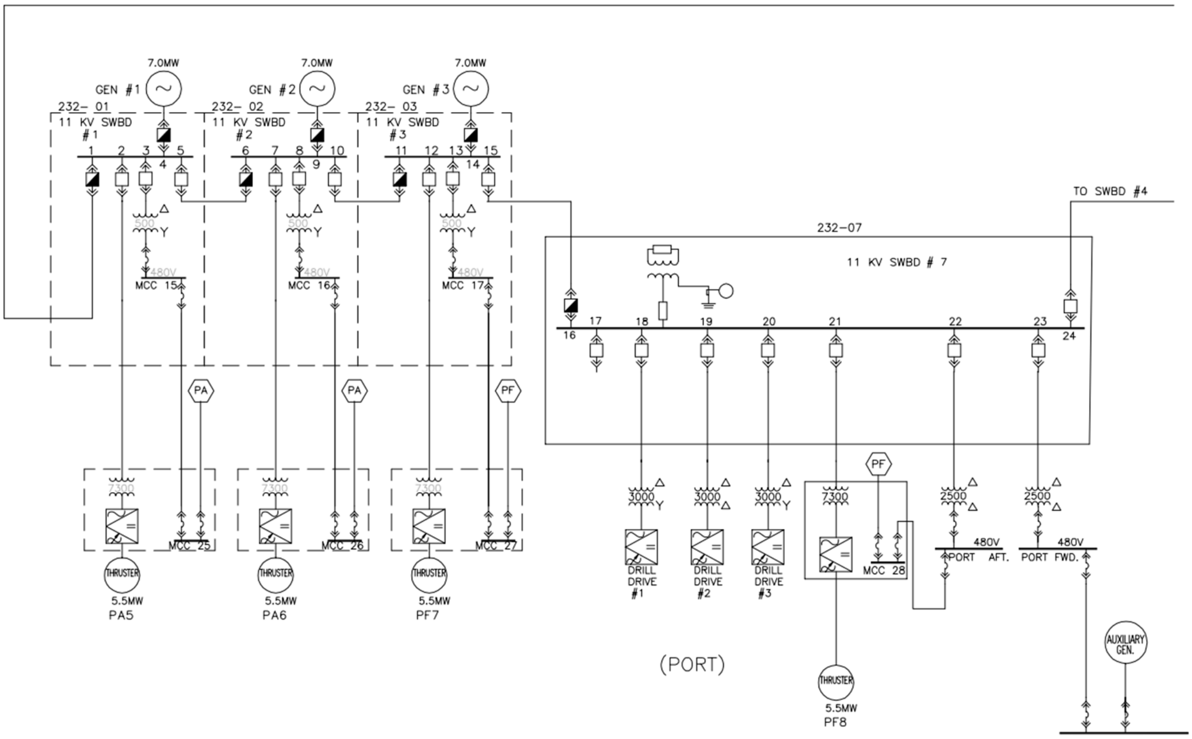


Figure 45 - Deepwater Horizon platform, port side IPS section

For what concerns the drillship used as a case of study, it has a rather common layout consisting in three fully redundant sections with cross connections between switchboards at different voltage levels. The single line diagram of one section is depicted in Figure 46, where only the MV section and the main LV switchboards are shown. The emergency switchboard has been ignored during this case study because here the focus has been given to the dependability of the IPS during the normal operation. In fact, the emergency switchboard is used only during emergencies (as its name imply), thus being the last resort for such systems. The proposed design process is aimed at aiding in system design as to achieve improved performance and fault resistance during normal operation, hence the exclusion of the emergency from the schematics.

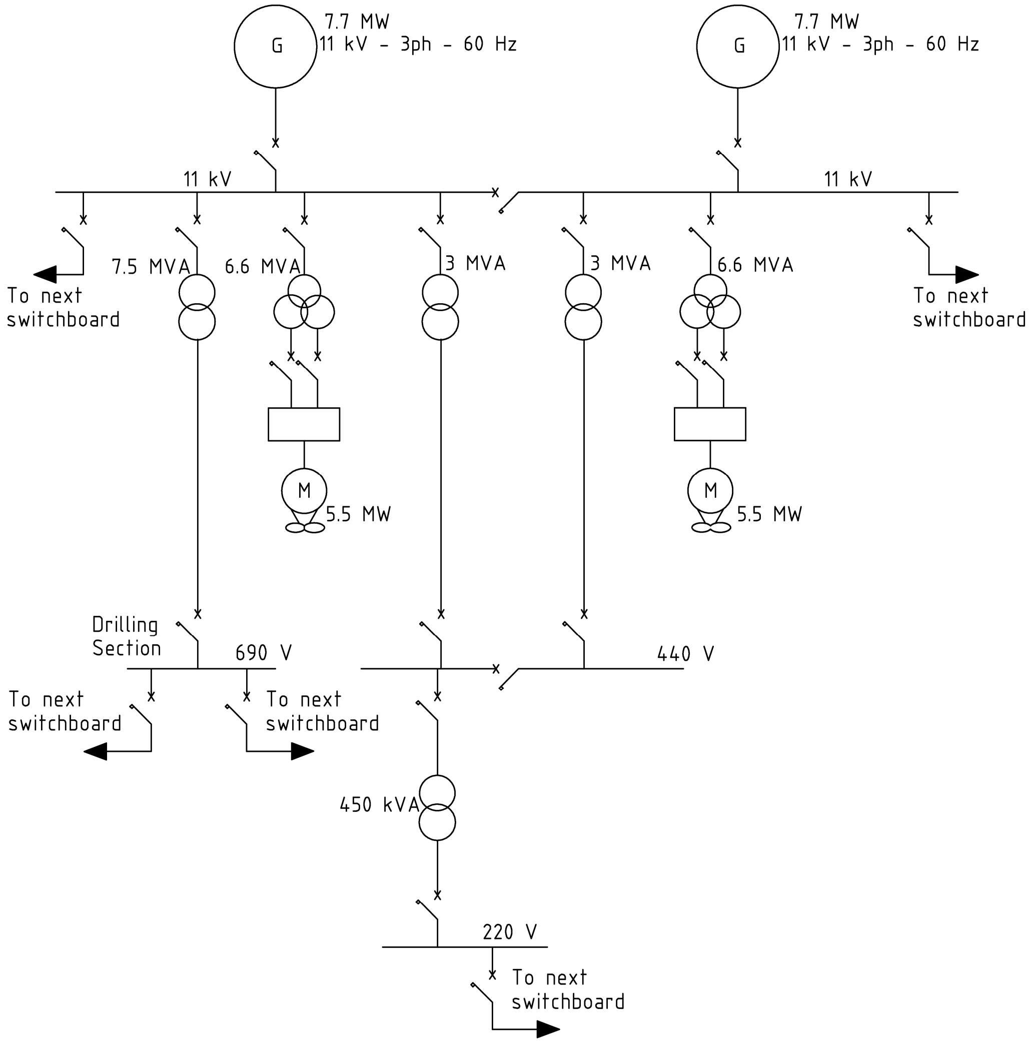


Figure 46 - Case study IPS, single line diagram of one redundant section

Table 13 - Case study IPS, electric loads balance

	Normal drilling, normal marine conditions [kW]	**Normal drilling, worst marine condition [kW]**	**Navigation [kW]**
Thrusters	9290	17710	15890
Drilling System	15400	15400	0
DG auxiliaries	450	450	410
Hull System	240	240	210
HVAC	2440	2440	2100
Accommodation	240	240	240
Total	28060	36480	18850

Main data about the system power and voltage levels can be inferred from Figure 46, while an extremely simplified electric power balance is shown in Table 13 (only a couple of the several designed operative conditions are shown here). The system has a total of six Diesel Generators (DG) and an equal number of DP thrusters (with related power electronic drive). DGs and thrusters are connected to three main MV switchboards, each divisible in two sub-sections normally tied together. The switchboard division is done with the aim of limiting the impact of a switchboard failure in a single section, thus allowing disconnecting the faulted section (and the related DG and thruster) from the healthy section. In such a way the single IPS section is able to continue half operation after such a fault. Each MV switchboard can be connected to the other two, possibly constituting a ring bus if all the tie-breaker are closed. However, the operation in ring configuration is not foreseen by design to allow installing simpler and cheaper protections on the MV sections. Due to that, it is required the presence of at least one open tie-breaker during operations. LV switchboards are divided in two sections as well as MV ones, due to the same motivations. Differently from MV, in this case the switchboards are normally separated, to avoid power recirculation through MV/LV transformers. Interconnections between LV switchboards are also present, but the normal operation configuration imply open tie-breakers. Indeed, such interconnections are to be used only for power supply in case of component's faults or maintenance. The drilling section is formed by three switchboards, each supplied by one section of the MV switchboard, whose operation is normally separated. In this case, the redundancy is achieved through both the possible connection between the drilling switchboards and the presence of redundant drilling package components, equally divided on the various sections. In addition to that, the transformers supplying drilling section are over-dimensioned, to allow the normal operation also in absence of one of the total three units (to take into account possible failures or maintenance).

6.3.2 Failure data

As mentioned in Section 4.2.4 of Chapter 4 (page 84 ff.), the application of dependability quantitative techniques needs reliable failure data about system's components. The selection of the data to be applied during the study is always a difficult task, but becomes critical in marine power systems. Indeed, data on marine components is scarce, due to both the lesser installation base of marine systems in respect to land one and the reluctance of ship owners in divulgating failure statistics about their ships (because it is perceived as "bad marketing"). Moreover, when innovative distribution systems are considered, no historical database is present, thus no failure data on the specific component can be determined. Therefore, it is difficult to find failure data with high confidence and tolerance. In fact, confidence express how near the statistical measurement of a given parameter is to the real one. Having high confidence data means obtaining results from the dependability analysis which approximates well the real system, allowing applying advanced techniques, such as RCM (see page 87).

Confidence can be increased through the increase of the sample size, which means having a high amount of failure data on the same component. Conversely, tolerance represents the capability of a given parameter to represent the component's real behavior in different conditions (physical, operating, and environmental). Having data with high tolerance allows applying the same parameter to the same component in spite of the different external conditions given by its peculiar installation. This means fixing the failure data for a component, thus simplifying the dependability analysis.

Although the peculiarities of maritime market and marine systems makes it difficult to find failure data on the components, in most cases it is possible to use data taken from other sources [79]. Indeed, land failure data use a large sample size, from different installations, with related different conditions. Thanks to the large sample size, it is possible to reduce the statistical impact of the different physical, operational, and environmental conditions on the component's failure data, highlighting the component's intrinsic failure parameters. Due to that, the use of land data on marine systems is certainly not correct, but leads to errors that may be not as high as expected. Some data on marine systems can be found in [20], but in this thesis work reference will be made on the data given in Chapter 10.3 of IEEE Std. 493 [76]. Such data refers to extended equipment reliability surveys made between 1976 and 1989 in industrial and commercial applications. While it is not marine system's data, it has been deemed sufficient for the scope of demonstrating the possibilities given by the innovative design process, goal of this thesis work. Moreover, failure parameters taken from the standard (land based) have the same order of magnitude of the ones that can be found in [20] (marine based), reinforcing the idea of a possible transfer of data from the terrestrial to the marine sector. The failure data of the components used in the case study is depicted in Table 14, as failure rate λ and MTTR. In the same table is depicted also a short description of the single fault event considered.

To simplify the dependability analysis of case study (done in Section 6.4.2), a hypothesis about components is applied: their failure model is a Steady-State model type. The steady state model assumes exponential distributions for both the failure and repair process, and constant failure and repair rates. This implies ignoring system wear, thus imposing the steady-state condition for the entire systems lifetime. The unavailability and failure frequency of a component represented by the Steady State model are given respectively by:

$$Q(t) = \frac{\lambda \cdot MTTR}{1 + \lambda \cdot MTTR} \tag{6.3-1}$$

$$\omega(t) = \lambda \cdot (1 - Q(t)) \tag{6.3-2}$$

where: *Q(t)* is component unavailability; *ω(t)* is component failure frequency; λ is component failure rate; MTTR is component repair rate.

Table 14 - Failure data of the components used in the case study [76].

ID	Description	Failure rate [failures/year]	MTTR [h]
Adjustable Speed Drive failure	Failure in Electric Motor Adjustable Speed Drive	0,02207	16,55
DG controls failure	Failure in static Automatic Voltage Regulator or Speed Governor	0,03627	74,77
Diesel Generator failure	Diesel engine generator, 750 kW to 7 MW, continuous	1,81573	25,08
DP thruster failure	Failure in azimuting fixed pitch thruster	0,9125	170
LV circuit breaker failure NC	Failure in Low Voltage circuit breaker; Drawout type, >600A, normally closed	0,00185	0,5
LV circuit breaker failure NO	Failure in Low Voltage circuit breaker; Drawout type, >600A, normally open	0,00553	2
LV Switchboard failure	LV Switchboard failure; <600V, bare bus, Circuit breakers not included	0,00949	7,29
MV circuit breaker failure low current	Vacuum circuit breaker failure <600A, normally closed	0,00281	8
MV circuit breaker failure high current	Vacuum circuit breaker failure; Draw out, >600A, normally closed	0,02352	14,8
MV Switchboard failure	MV Switchboard failure >5kV, bare bus; Circuit breakers not included	0,01794	2,27
MV/LV transformer failure	Failure in MV/LV transformer; dry type 3MVA	0,00061	4

6.4 Application of the proposed design process

6.4.1 Case analyzed

To demonstrate both the applicability of the proposed design process and the advantages it can give to design, one case study has been analyzed. The IPS shown in Section 6.3 has been considered, and the steps foreseen by the innovative process have been applied, examining only one particular operating condition due to time/space/resource constraints. In particular, the case study hypotheses are:

- Evaluation of only the MV and the main LV sections of the IPS;
- No emergency switchboard;
- No secondary LV distribution and electric panels;
- LV loads modeled as equivalent loads directly connected to the switchboards;
- Loads are equally distributed among switchboards;
- Components not present in Table 14 are ignored.

The resulting extremely simplified system has been studied in the operating condition defined by the following:

- Operation in normal drilling, normal marine conditions configuration (from Table 13, page 122);
- Open bus condition (the three MV switchboards are separated).

No hypotheses on the faults have been made: the fault condition to be simulated through the software is to be selected analyzing dependability analysis outcomes. Obviously, all the fault conditions foreseen by Rules and Regulations have to be considered in a real design process, but here only one is to be selected, in order to simplify the demonstration.

As mentioned in Section 4.2.3 of Chapter 4 (page 77 ff.), the Fault Tree Analysis moves from a precisely defined top-event to the system's components faults, assessing all the possible combinations of faults that may lead to the top-event. Due to that, the top-event has to be specified before starting the analysis. Several different top-events can be defined for a single operating condition, requiring a reasoned evaluation on which ones, and how many, needs to be considered for the system design in order to not overburden the analyst. In this case study only one top-event has been evaluated among the most relevant ones for the IPS of a DP vessel. In particular, the top-event used in the case study is:

- *DP failure*, intended as a failure in keeping vessel's position due to a failure in supplying the loads needed by the DP system to correctly operate.

Taking into account the particular top-event selected, some additional hypotheses have been applied in the dependability analysis to lower its burden:

- The drilling section, the HVAC loads, and the accommodation loads have not been considered into the FTA, because they do not affect the DP systems failure. However, their power consumption has been considered for what concerns power generation capabilities;
- The auxiliaries of the DGs have been included into the LV loads;
- No UPS has been considered in constructing the Failure Tree.

6.4.2 Fault Tree Analysis

The first tool to be used in the innovative design process is the dependability theory, along with its techniques. Dependability analysis is used to perform the first two steps of the proposed design process. In particular the technique best suited for this application is the FTA because of the possibility to achieve quantitative analysis through it, as previously mentioned. The case study defined in the previous section has been analyzed using such a technique, and considering the abovementioned top-event, with the aim of assessing all its dependability-related characteristics. To ease both the diagram construction and the following quantitative calculations, a dedicated software has been used: Isograph® Reliability Workbench®. Not only the software allows to build the diagram with an easy to use graphical interface, but also is able to do the quantitative calculations automatically if the necessary parameters are set for each fault event. The resulting Failure Tree is depicted completely in Figure 47. As can be seen, the extension of the built graph is significant, making it difficult to be represented entirely in one page in spite of the great simplification level achieved through the abovementioned hypotheses. Due to that, the Failure Tree has been separated into sections, each interconnected to the others. Such sections are depicted in the figures whose range spans from Figure 48 to Figure 62. The interconnections between them are pinpointed by page numbers, each referring to the page of the Failure Tree diagram addressed by the specific interconnection. (Such page numbers can be found both in the single diagram figures and in each figure caption.)

The Failure Tree shows all the possible combinations of components' faults leading to the top-event. Analyzing the figures, it is easy to assess that no single fault event leads directly to the top-event, demonstrating the compliance with requirement 2/3.1 of ABS Guide for DP systems [22] (refer to Section 1.4.3 of Chapter 1, page 17 ff.). Obviously, such a compliance has been verified here for an extremely simplified case, therefore this particular study has no claim of being able to assess ship's requirements compliance. If a more in depth analysis it is made, applying a higher detail in defining base events, it may be possible to find single fault events whose impact on the overall system is high in terms of effects. As an example, the black-out event depicted in Section 2.3.2 of Chapter 2 (page 41) may have been avoided if the ship design had been followed by an FTA to verify it. In fact, the common lubrication circuit would have appeared clearly into the Failure Tree as a highly impacting event, thus leading designers to solve such an issue before the ship construction.

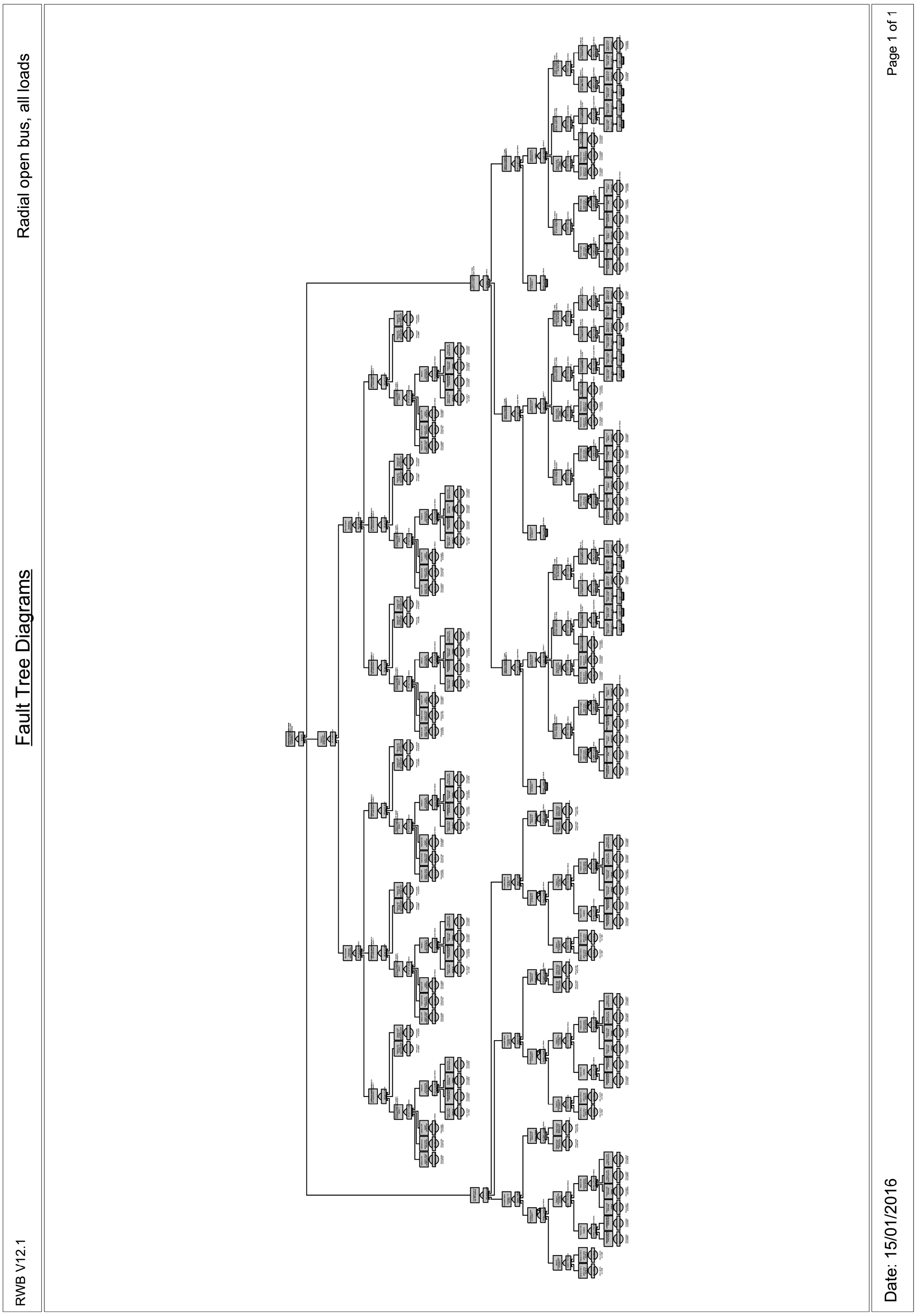


Figure 47 - Complete Failure Tree diagram of the case study system

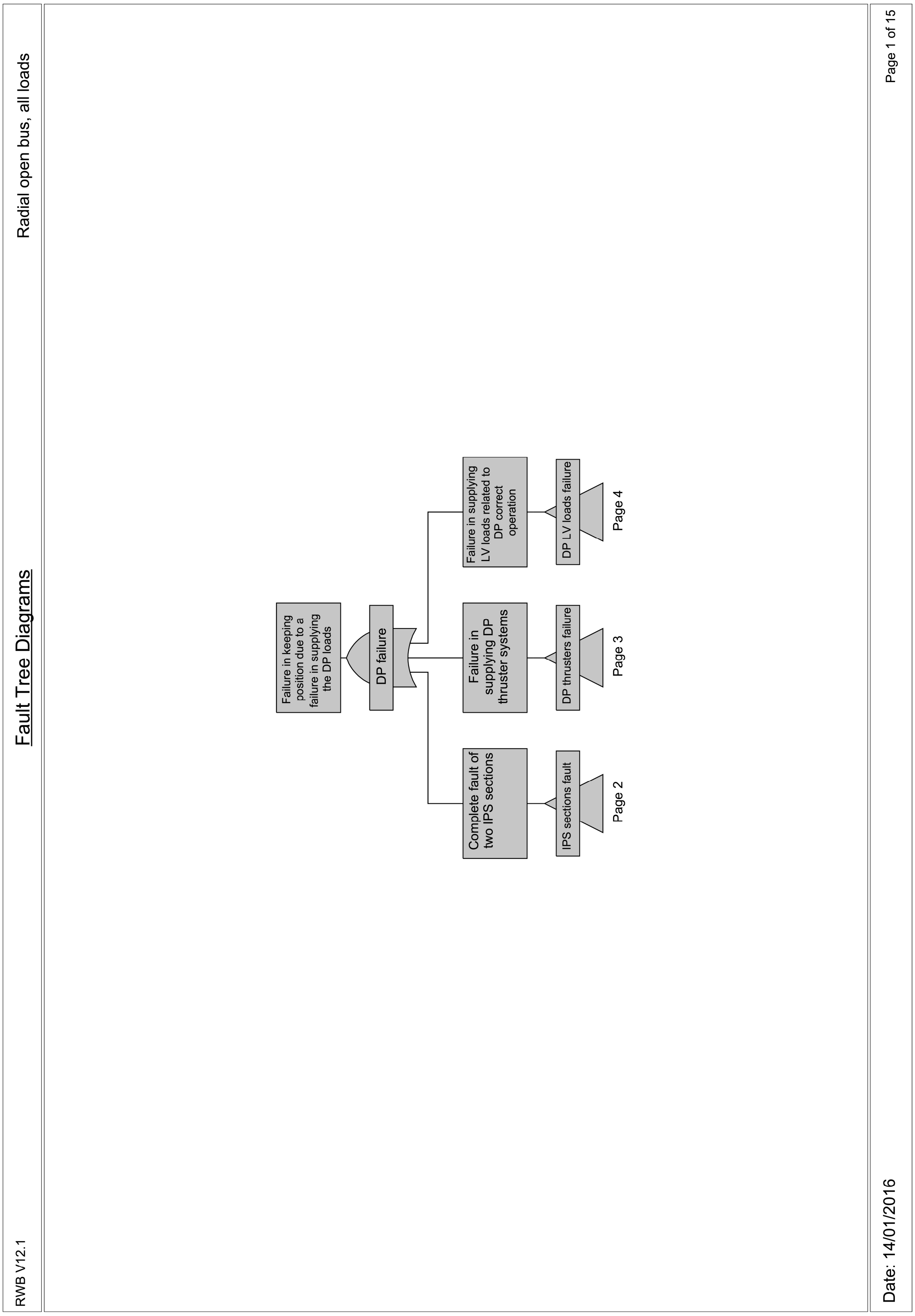

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Failure in keeping position due to a failure in supplying the DP loads
DP failure
Complete fault of two IPS sections
IPS sections fault
Page 2
Failure in supplying DP thruster systems
DP thrusters failure
Page 3
Failure in supplying LV loads related to DP correct operation
DP LV loads failure
Page 4
Date: 14/01/2016
Page 1 of 15

Figure 48 - Failure Tree, page 1/15

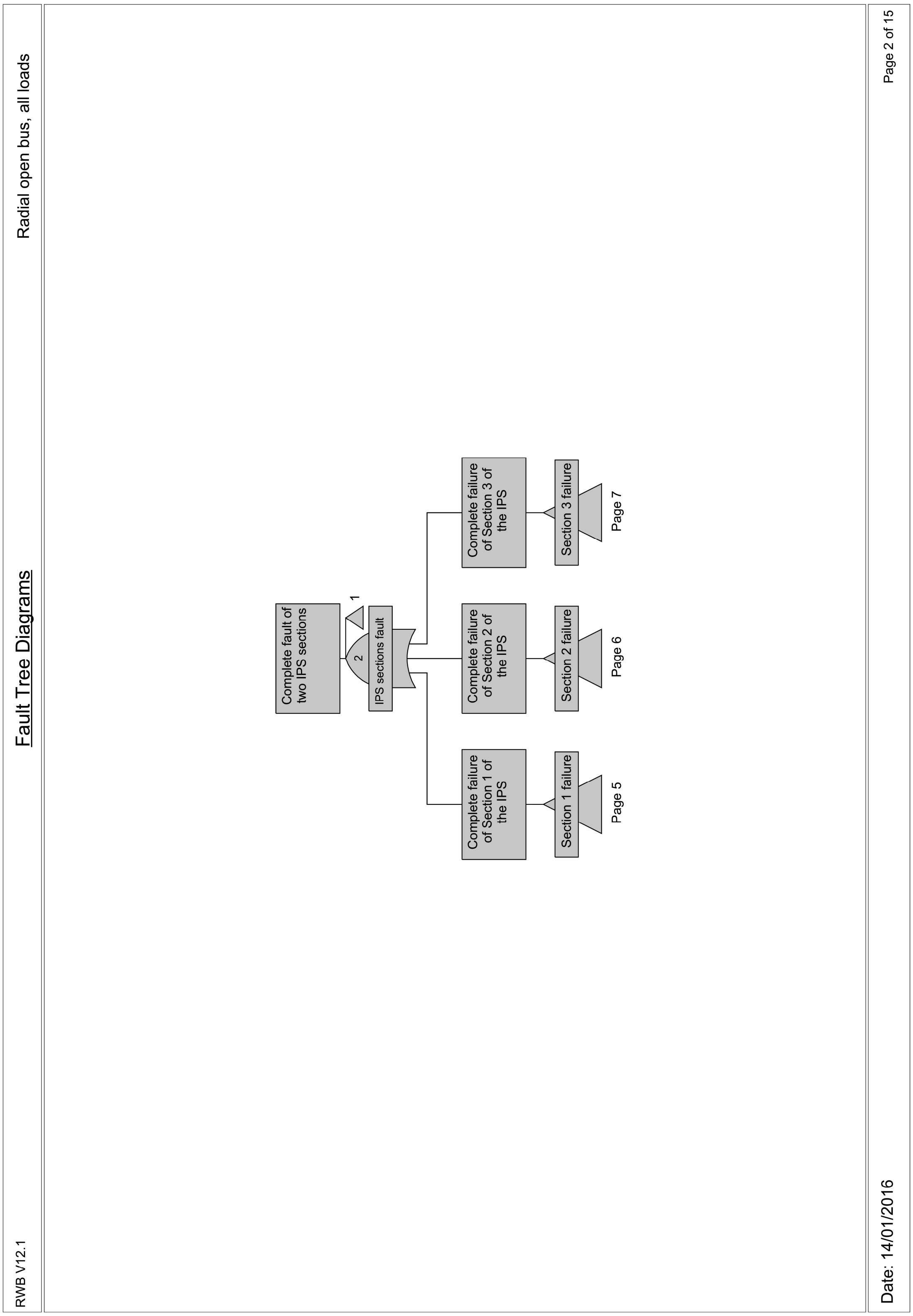

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Complete fault of two IPS sections
2
1
IPS sections fault
Complete failure of Section 1 of the IPS
Complete failure of Section 2 of the IPS
Complete failure of Section 3 of the IPS
Section 1 failure
Section 2 failure
Section 3 failure
Page 5
Page 6
Page 7
Date: 14/01/2016
Page 2 of 15

Figure 49 - Failure Tree, page 2/15

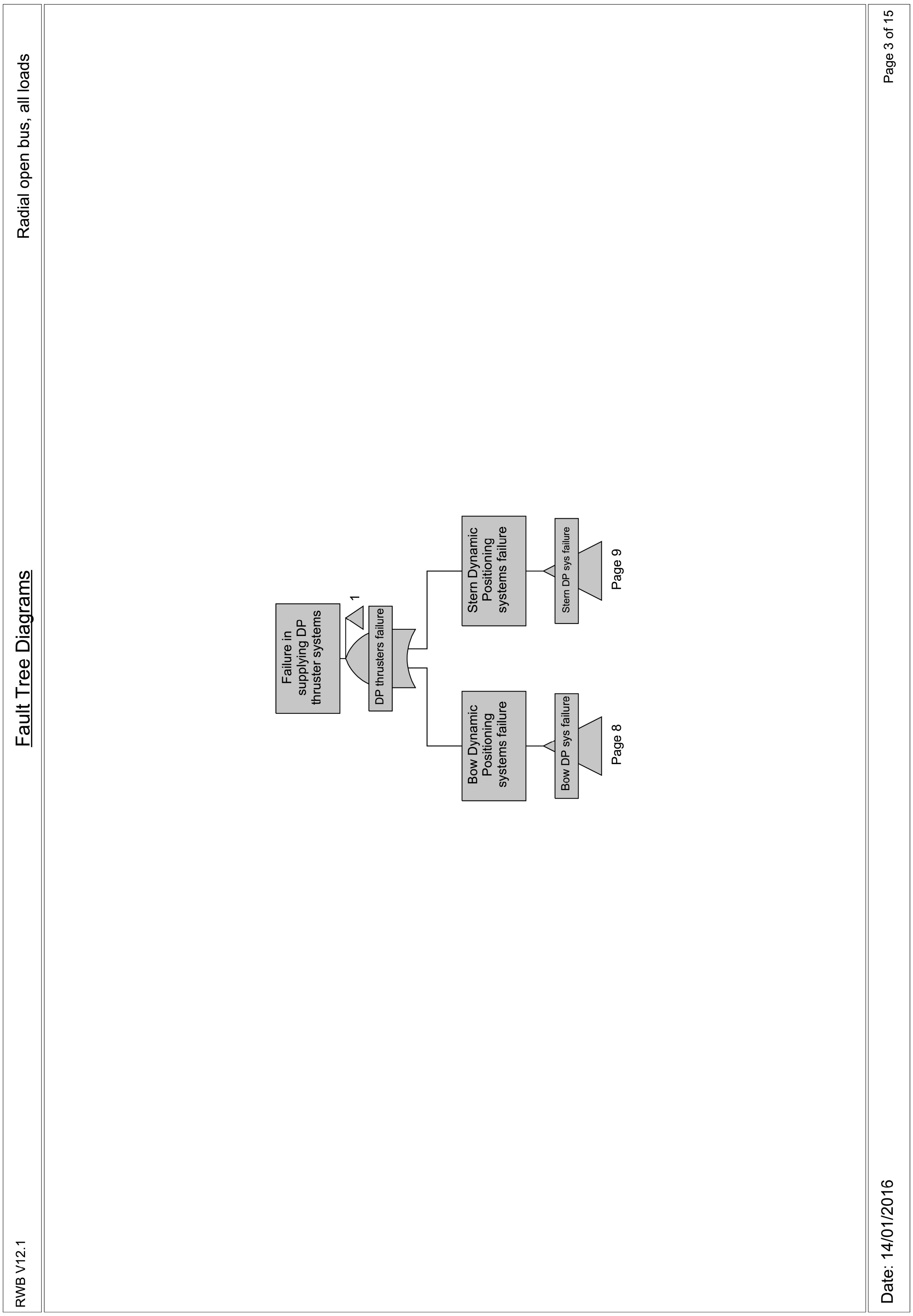

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Failure in supplying DP thruster systems
1
DP thrusters failure
Bow Dynamic Positioning systems failure
Stern Dynamic Positioning systems failure
Bow DP sys failure
Page 8
Stern DP sys failure
Page 9
Date: 14/01/2016
Page 3 of 15

Figure 50 - Failure Tree, page 3/15

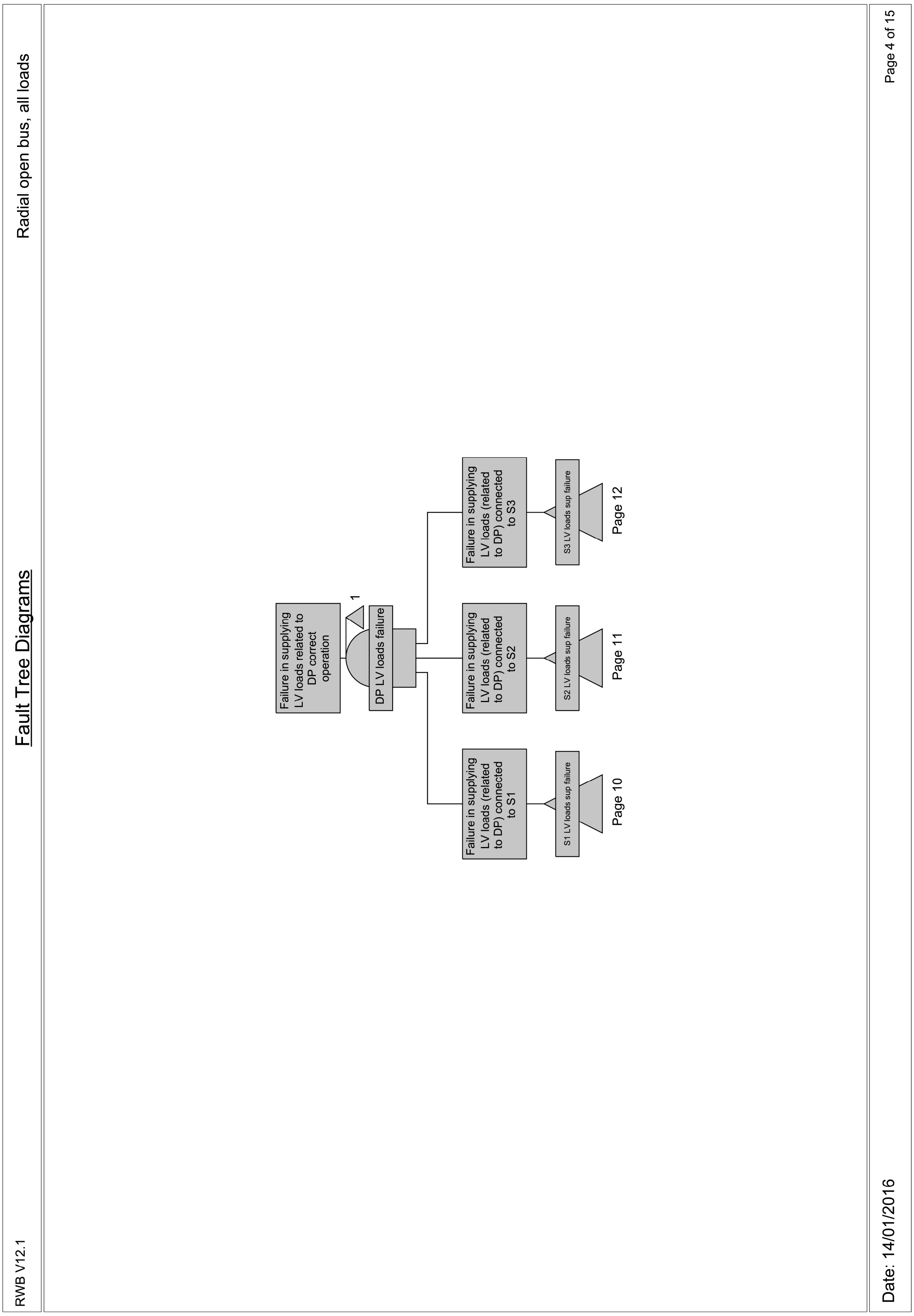

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Failure in supplying LV loads related to DP correct operation
1
DP LV loads failure
Failure in supplying LV loads (related to DP) connected to S1
Failure in supplying LV loads (related to DP) connected to S2
Failure in supplying LV loads (related to DP) connected to S3
S1 LV loads sup failure
S2 LV loads sup failure
S3 LV loads sup failure
Page 10
Page 11
Page 12
Date: 14/01/2016
Page 4 of 15

Figure 51 - Failure Tree, page 4/15

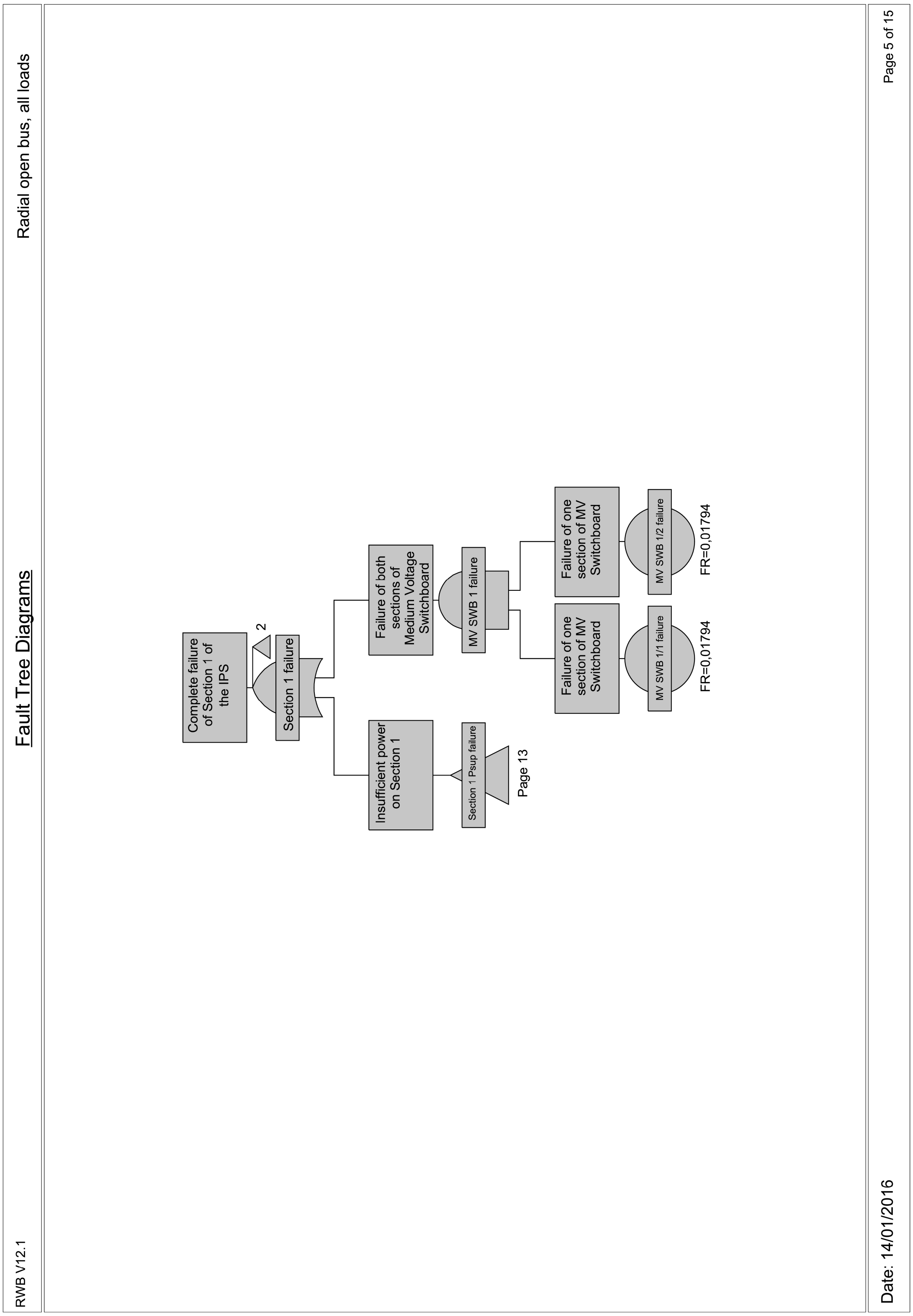

Fault Tree Diagrams
Radial open bus, all loads
RWB V12.1
Complete failure of Section 1 of the IPS
2
Section 1 failure
Insufficient power on Section 1
Section 1 Psup failure
Page 13
Failure of both sections of Medium Voltage Switchboard
MV SWB 1 failure
Failure of one section of MV Switchboard
MV SWB 1/1 failure
FR=0,01794
Failure of one section of MV Switchboard
MV SWB 1/2 failure
FR=0,01794
Date: 14/01/2016
Page 5 of 15

Figure 52 - Failure Tree, page 5/15

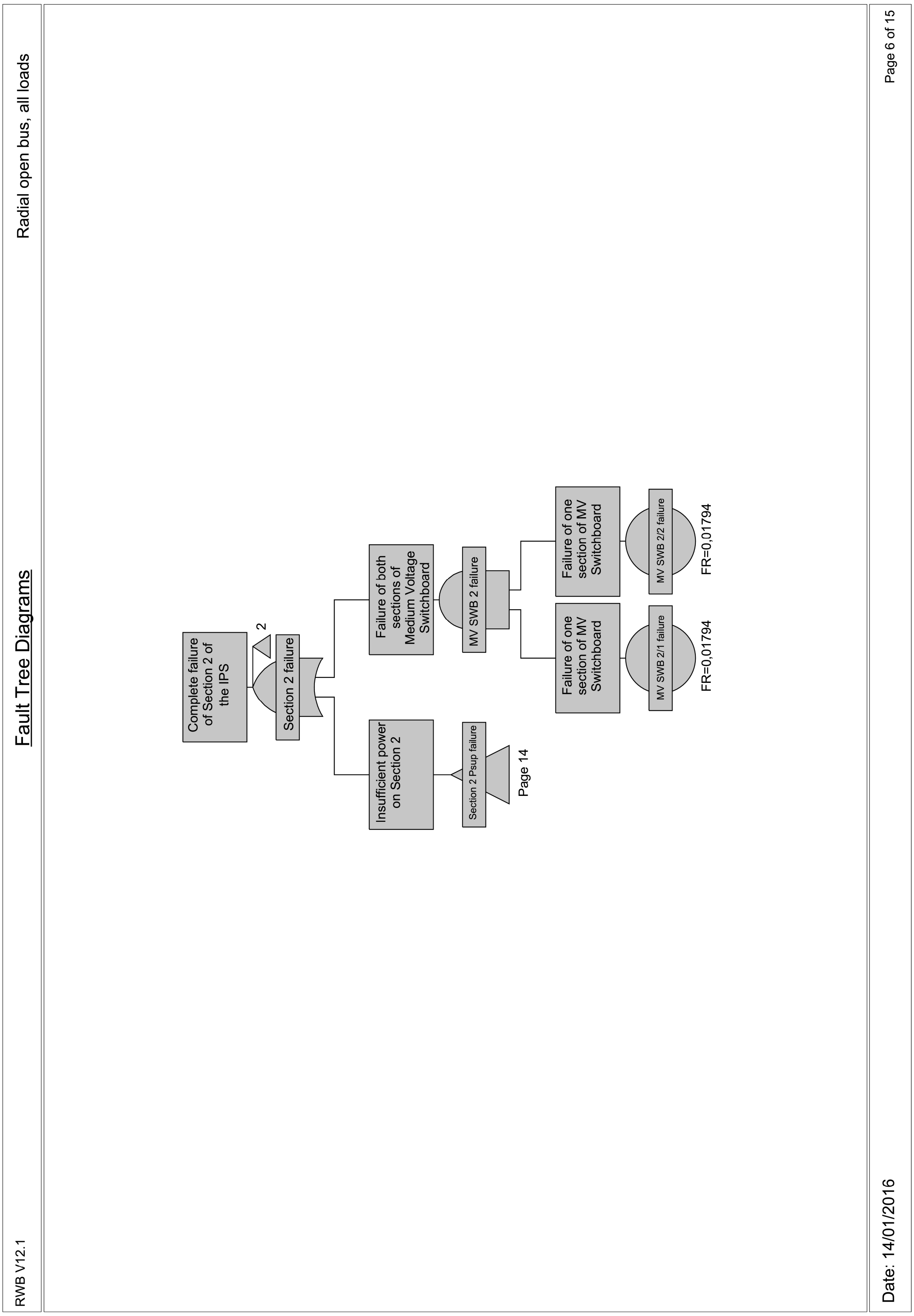

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Complete failure of Section 2 of the IPS
2
Section 2 failure
Insufficient power on Section 2
Section 2 Psup failure
Page 14
Failure of both sections of Medium Voltage Switchboard
MV SWB 2 failure
Failure of one section of MV Switchboard
MV SWB 2/1 failure
FR=0,01794
Failure of one section of MV Switchboard
MV SWB 2/2 failure
FR=0,01794
Date: 14/01/2016
Page 6 of 15

Figure 53 - Failure Tree, page 6/15

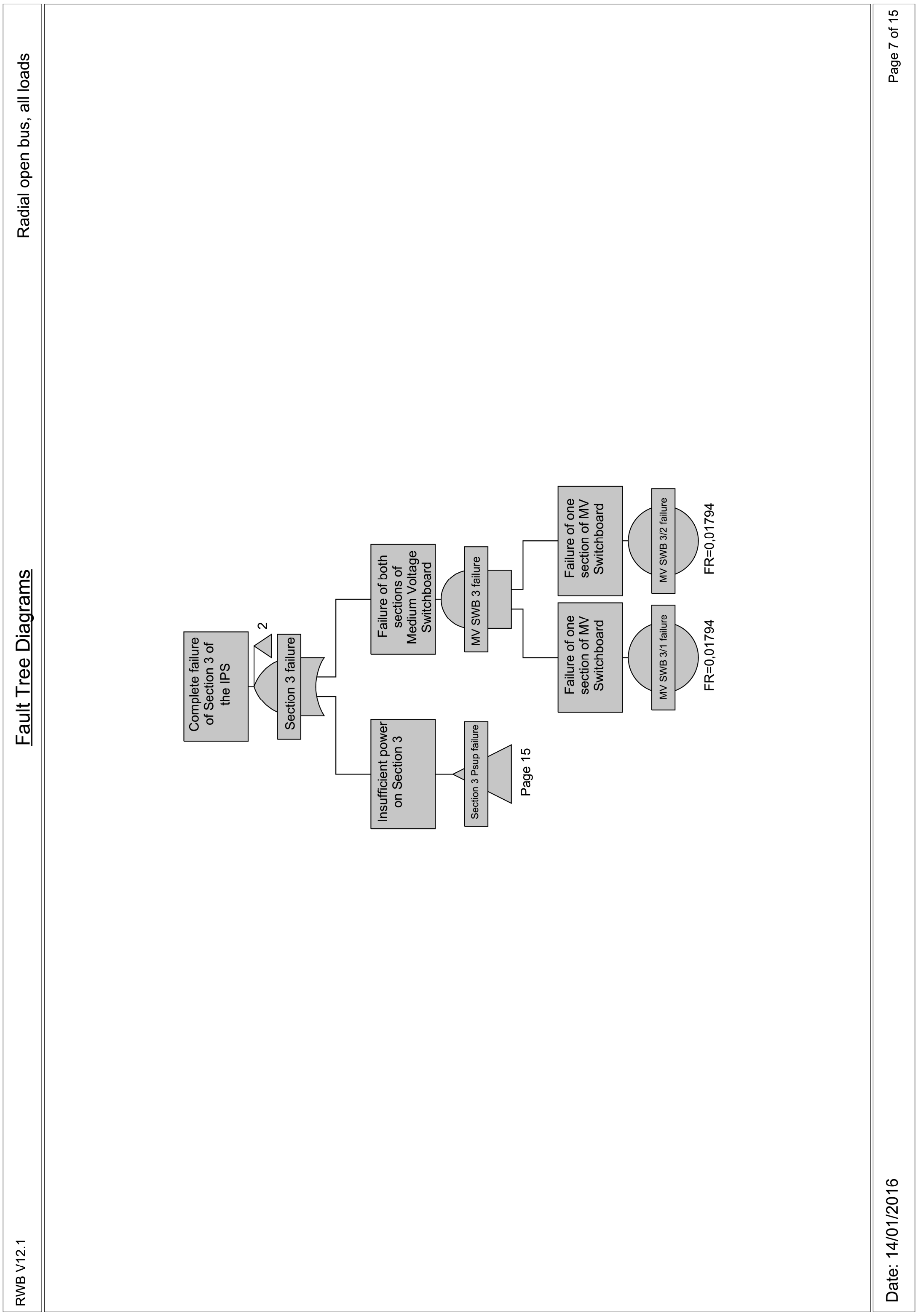
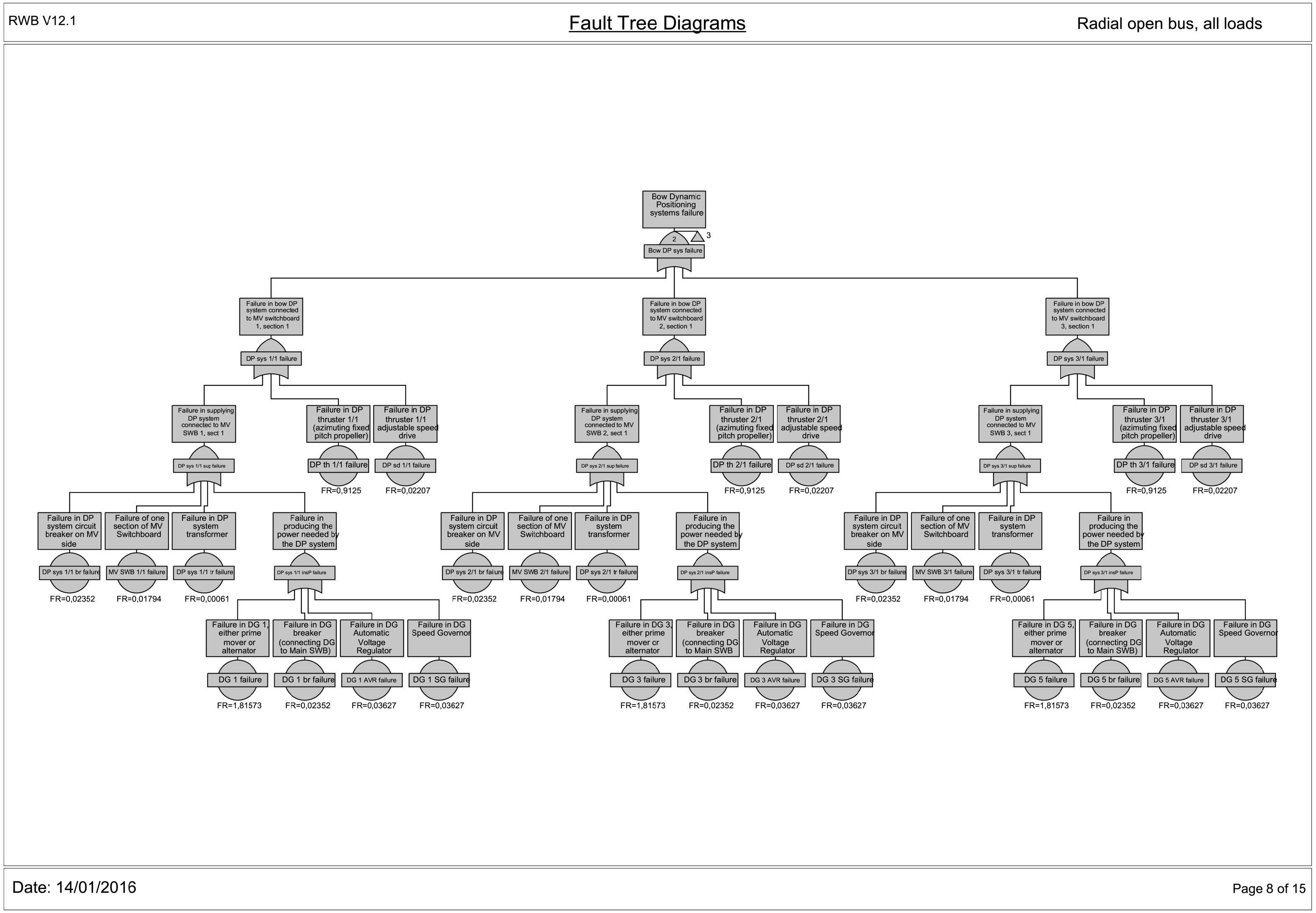

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Complete failure of Section 3 of the IPS
2
Section 3 failure
Insufficient power on Section 3
Section 3 Psup failure
Page 15
Failure of both sections of Medium Voltage Switchboard
MV SWB 3 failure
Failure of one section of MV Switchboard
MV SWB 3/1 failure
FR=0,01794
Failure of one section of MV Switchboard
MV SWB 3/2 failure
FR=0,01794
Date: 14/01/2016
Page 7 of 15

Figure 54 - Failure Tree, page 7/15



RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Bow Dynamic Positioning systems failure
2
3
Bow DP sys failure
Failure in bow DP system connected to MV switchboard 1, section 1
DP sys 1/1 failure
Failure in supplying DP system connected to MV SWB 1, sect 1
DP sys 1/1 sup failure
Failure in DP thruster 1/1 (azimuting fixed pitch propeller)
DP th 1/1 failure
FR=0,9125
Failure in DP thruster 1/1 adjustable speed drive
DP sd 1/1 failure
FR=0,02207
Failure in DP system circuit breaker on MV side
DP sys 1/1 br failure
FR=0,02352
Failure of one section of MV Switchboard
MV SWB 1/1 failure
FR=0,01794
Failure in DP system transformer
DP sys 1/1 tr failure
FR=0,00061
Failure in producing the power needed by the DP system
DP sys 1/1 insP failure
Failure in DG 1, either prime mover or alternator
DG 1 failure
FR=1,81573
Failure in DG breaker (connecting DG to Main SWB)
DG 1 br failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 1 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 1 SG failure
FR=0,03627
Failure in bow DP system connected to MV switchboard 2, section 1
DP sys 2/1 failure
Failure in supplying DP system connected to MV SWB 2, sect 1
DP sys 2/1 sup failure
Failure in DP thruster 2/1 (azimuting fixed pitch propeller)
DP th 2/1 failure
FR=0,9125
Failure in DP thruster 2/1 adjustable speed drive
DP sd 2/1 failure
FR=0,02207
Failure in DP system circuit breaker on MV side
DP sys 2/1 br failure
FR=0,02352
Failure of one section of MV Switchboard
MV SWB 2/1 failure
FR=0,01794
Failure in DP system transformer
DP sys 2/1 tr failure
FR=0,00061
Failure in producing the power needed by the DP system
DP sys 2/1 insP failure
Failure in DG 3, either prime mover or alternator
DG 3 failure
FR=1,81573
Failure in DG breaker (connecting DG to Main SWB
DG 3 br failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 3 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 3 SG failure
FR=0,03627
Failure in bow DP system connected to MV switchboard 3, section 1
DP sys 3/1 failure
Failure in supplying DP system connected to MV SWB 3, sect 1
DP sys 3/1 sup failure
Failure in DP thruster 3/1 (azimuting fixed pitch propeller)
DP th 3/1 failure
FR=0,9125
Failure in DP thruster 3/1 adjustable speed drive
DP sd 3/1 failure
FR=0,02207
Failure in DP system circuit breaker on MV side
DP sys 3/1 br failure
FR=0,02352
Failure of one section of MV Switchboard
MV SWB 3/1 failure
FR=0,01794
Failure in DP system transformer
DP sys 3/1 tr failure
FR=0,00061
Failure in producing the power needed by the DP system
DP sys 3/1 insP failure
Failure in DG 5, either prime mover or alternator
DG 5 failure
FR=1,81573
Failure in DG breaker (connecting DG to Main SWB)
DG 5 br failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 5 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 5 SG failure
FR=0,03627
Date: 14/01/2016
Page 8 of 15

Figure 55 - Failure Tree, page 8/15

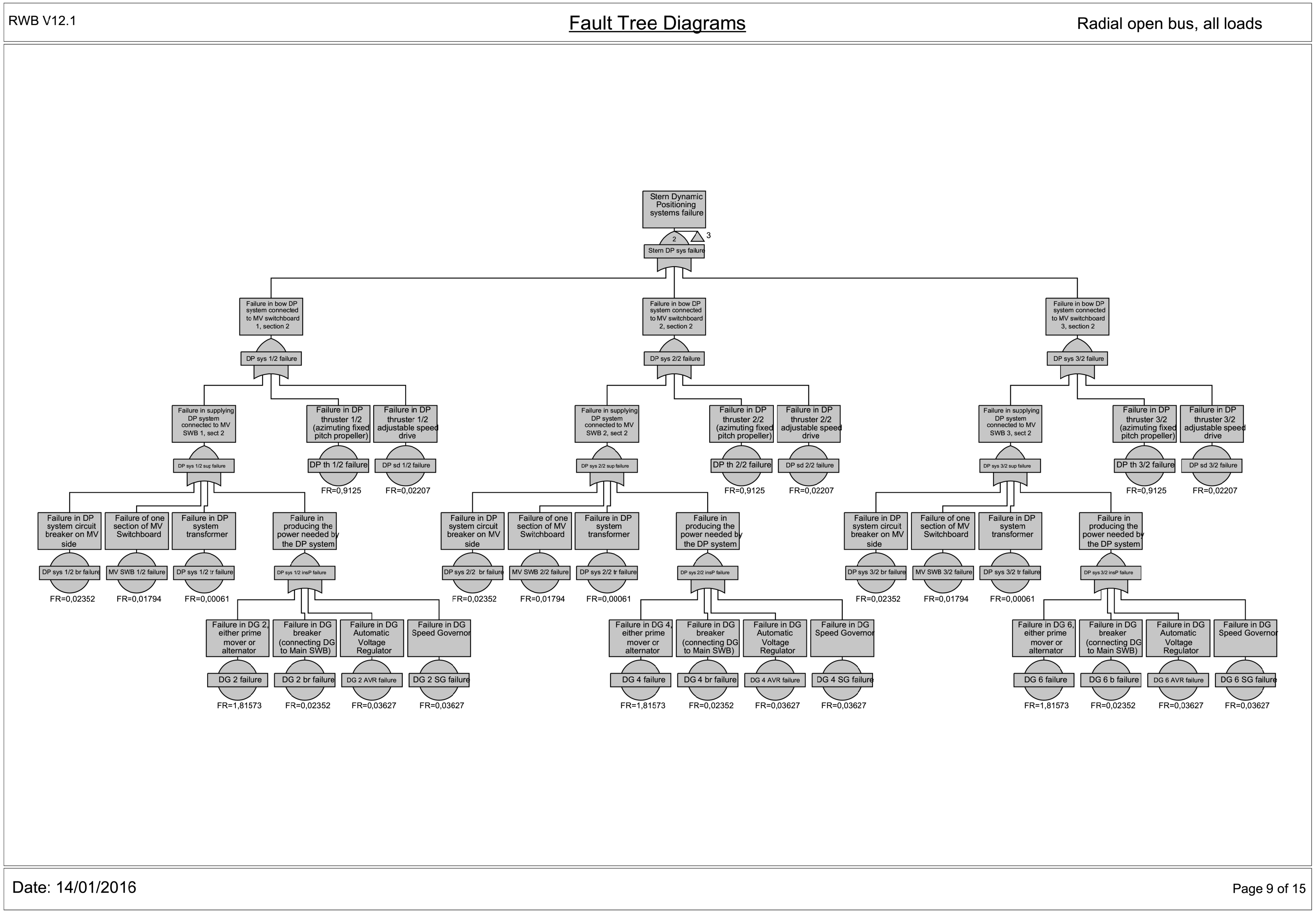

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Stern Dynamic Positioning systems failure
2
3
Stern DP sys failure
Failure in bow DP system connected to MV switchboard 1, section 2
DP sys 1/2 failure
Failure in supplying DP system connected to MV SWB 1, sect 2
DP sys 1/2 sup failure
Failure in DP thruster 1/2 (azimuting fixed pitch propeller)
DP th 1/2 failure
FR=0,9125
Failure in DP thruster 1/2 adjustable speed drive
DP sd 1/2 failure
FR=0,02207
Failure in DP system circuit breaker on MV side
DP sys 1/2 br failure
FR=0,02352
Failure of one section of MV Switchboard
MV SWB 1/2 failure
FR=0,01794
Failure in DP system transformer
DP sys 1/2 tr failure
FR=0,00061
Failure in producing the power needed by the DP system
DP sys 1/2 insP failure
Failure in DG 2, either prime mover or alternator
DG 2 failure
FR=1,81573
Failure in DG breaker (connecting DG to Main SWB)
DG 2 br failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 2 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 2 SG failure
FR=0,03627
Failure in bow DP system connected to MV switchboard 2, section 2
DP sys 2/2 failure
Failure in supplying DP system connected to MV SWB 2, sect 2
DP sys 2/2 sup failure
Failure in DP thruster 2/2 (azimuting fixed pitch propeller)
DP th 2/2 failure
FR=0,9125
Failure in DP thruster 2/2 adjustable speed drive
DP sd 2/2 failure
FR=0,02207
Failure in DP system circuit breaker on MV side
DP sys 2/2 br failure
FR=0,02352
Failure of one section of MV Switchboard
MV SWB 2/2 failure
FR=0,01794
Failure in DP system transformer
DP sys 2/2 tr failure
FR=0,00061
Failure in producing the power needed by the DP system
DP sys 2/2 insP failure
Failure in DG 4, either prime mover or alternator
DG 4 failure
FR=1,81573
Failure in DG breaker (connecting DG to Main SWB)
DG 4 br failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 4 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 4 SG failure
FR=0,03627
Failure in bow DP system connected to MV switchboard 3, section 2
DP sys 3/2 failure
Failure in supplying DP system connected to MV SWB 3, sect 2
DP sys 3/2 sup failure
Failure in DP thruster 3/2 (azimuting fixed pitch propeller)
DP th 3/2 failure
FR=0,9125
Failure in DP thruster 3/2 adjustable speed drive
DP sd 3/2 failure
FR=0,02207
Failure in DP system circuit breaker on MV side
DP sys 3/2 br failure
FR=0,02352
Failure of one section of MV Switchboard
MV SWB 3/2 failure
FR=0,01794
Failure in DP system transformer
DP sys 3/2 tr failure
FR=0,00061
Failure in producing the power needed by the DP system
DP sys 3/2 insP failure
Failure in DG 6, either prime mover or alternator
DG 6 failure
FR=1,81573
Failure in DG breaker (connecting DG to Main SWB)
DG 6 b failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 6 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 6 SG failure
FR=0,03627
Date: 14/01/2016
Page 9 of 15

Figure 56 - Failure Tree, page 9/15

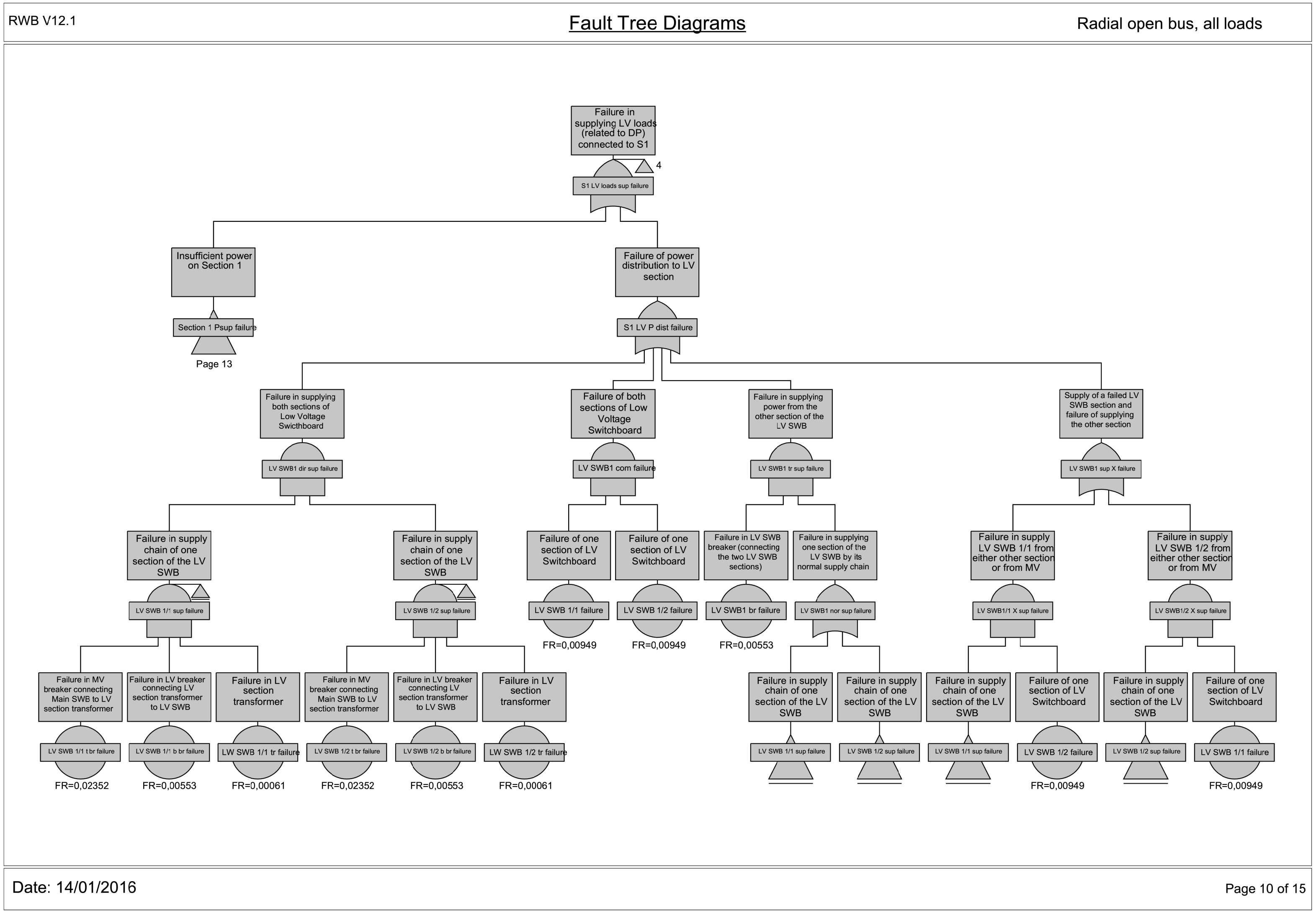

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Failure in supplying LV loads (related to DP) connected to S1
4
S1 LV loads sup failure
Insufficient power on Section 1
Section 1 Psup failure
Page 13
Failure of power distribution to LV section
S1 LV P dist failure
Failure in supplying both sections of Low Voltage Swicthboard
LV SWB1 dir sup failure
Failure of both sections of Low Voltage Switchboard
LV SWB1 com failure
Failure in supplying power from the other section of the LV SWB
LV SWB1 tr sup failure
Supply of a failed LV SWB section and failure of supplying the other section
LV SWB1 sup X failure
Failure in supply chain of one section of the LV SWB
LV SWB 1/1 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 1/2 sup failure
Failure of one section of LV Switchboard
LV SWB 1/1 failure
FR=0,00949
Failure of one section of LV Switchboard
LV SWB 1/2 failure
FR=0,00949
Failure in LV SWB breaker (connecting the two LV SWB sections)
LV SWB1 br failure
FR=0,00553
Failure in supplying one section of the LV SWB by its normal supply chain
LV SWB1 nor sup failure
Failure in supply LV SWB 1/1 from either other section or from MV
LV SWB1/1 X sup failure
Failure in supply LV SWB 1/2 from either other section or from MV
LV SWB1/2 X sup failure
Failure in MV breaker connecting Main SWB to LV section transformer
LV SWB 1/1 t br failure
FR=0,02352
Failure in LV breaker connecting LV section transformer to LV SWB
LV SWB 1/1 b br failure
FR=0,00553
Failure in LV section transformer
LW SWB 1/1 tr failure
FR=0,00061
Failure in MV breaker connecting Main SWB to LV section transformer
LV SWB 1/2 t br failure
FR=0,02352
Failure in LV breaker connecting LV section transformer to LV SWB
LV SWB 1/2 b br failure
FR=0,00553
Failure in LV section transformer
LW SWB 1/2 tr failure
FR=0,00061
Failure in supply chain of one section of the LV SWB
LV SWB 1/1 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 1/2 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 1/1 sup failure
Failure of one section of LV Switchboard
LV SWB 1/2 failure
FR=0,00949
Failure in supply chain of one section of the LV SWB
LV SWB 1/2 sup failure
Failure of one section of LV Switchboard
LV SWB 1/1 failure
FR=0,00949
Date: 14/01/2016
Page 10 of 15

Figure 57 - Failure Tree, page 10/15

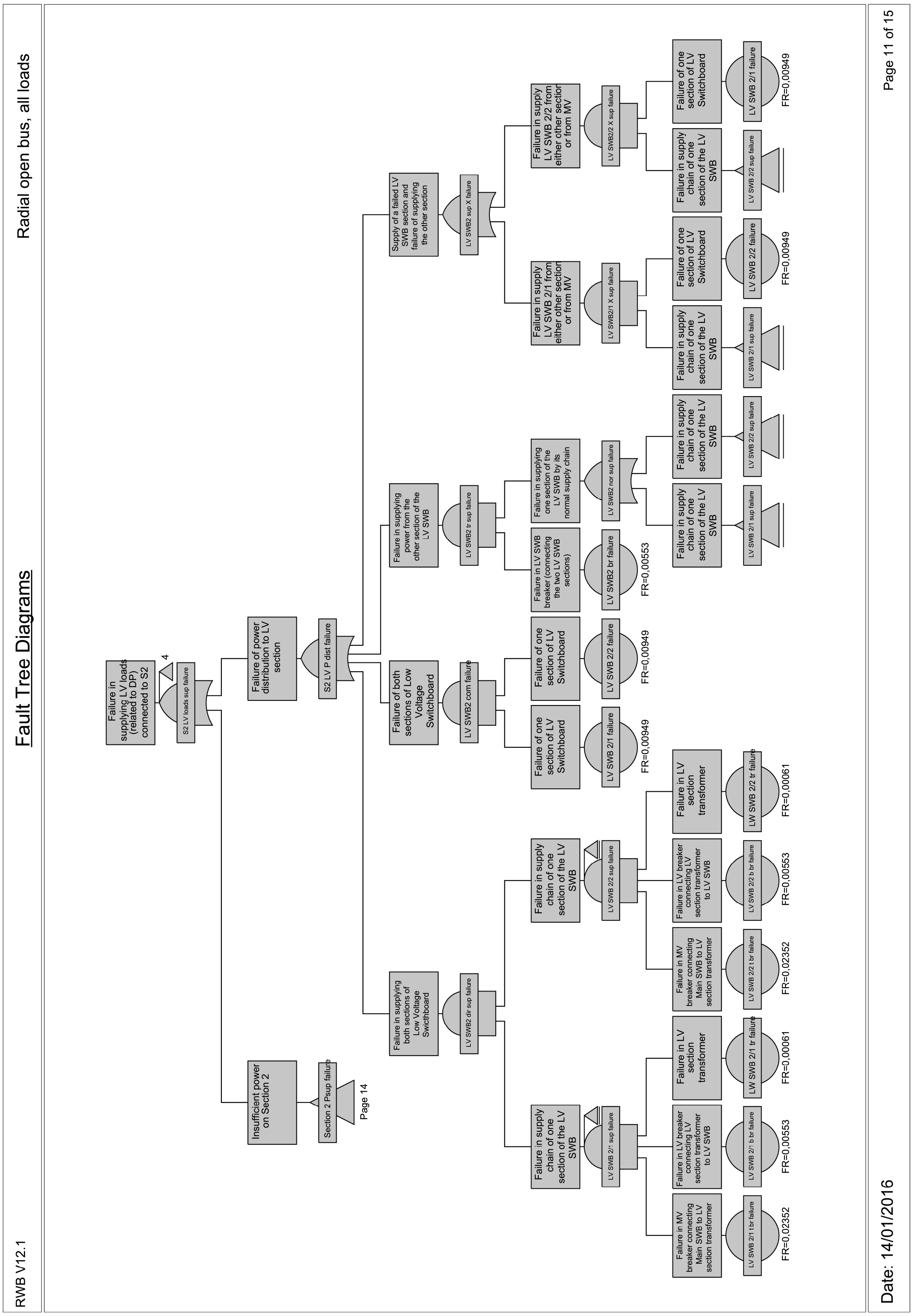

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Date: 14/01/2016
Page 11 of 15
Failure in supplying LV loads (related to DP) connected to S2
S2 LV loads sup failure
4
Insufficient power on Section 2
Section 2 Psup failure
Page 14
Failure of power distribution to LV section
S2 LV P dist failure
Failure in supplying both sections of Low Voltage Switchboard
LV SWB2 dir sup failure
Failure of both sections of Low Voltage Switchboard
LV SWB2 com failure
Failure in supplying power from the other section of the LV SWB
LV SWB2 tr sup failure
Supply of a failed LV SWB section and failure of supplying the other section
LV SWB2 sup X failure
Failure in supply chain of one section of the LV SWB
LV SWB 2/1 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 2/2 sup failure
Failure of one section of LV Switchboard
LV SWB 2/1 failure
FR=0,00949
Failure of one section of LV Switchboard
LV SWB 2/2 failure
FR=0,00949
Failure in LV SWB breaker (connecting the two LV SWB sections)
LV SWB2 br failure
FR=0,00553
Failure in supplying one section of the LV SWB by its normal supply chain
LV SWB2 nor sup failure
Failure in supply LV SWB 2/1 from either other section or from MV
LV SWB2/1 X sup failure
Failure in supply LV SWB 2/2 from either other section or from MV
LV SWB2/2 X sup failure
Failure in MV breaker connecting Main SWB to LV section transformer
LV SWB 2/1 t br failure
FR=0,02352
Failure in LV breaker connecting LV section transformer to LV SWB
LV SWB 2/1 b br failure
FR=0,00553
Failure in LV section transformer
LW SWB 2/1 tr failure
FR=0,00061
Failure in MV breaker connecting Main SWB to LV section transformer
LV SWB 2/2 t br failure
FR=0,02352
Failure in LV breaker connecting LV section transformer to LV SWB
LV SWB 2/2 b br failure
FR=0,00553
Failure in LV section transformer
LW SWB 2/2 tr failure
FR=0,00061
Failure in supply chain of one section of the LV SWB
LV SWB 2/1 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 2/2 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 2/1 sup failure
Failure of one section of LV Switchboard
LV SWB 2/2 failure
FR=0,00949
Failure in supply chain of one section of the LV SWB
LV SWB 2/2 sup failure
Failure of one section of LV Switchboard
LV SWB 2/1 failure
FR=0,00949

Figure 58 - Failure Tree, page 11/15

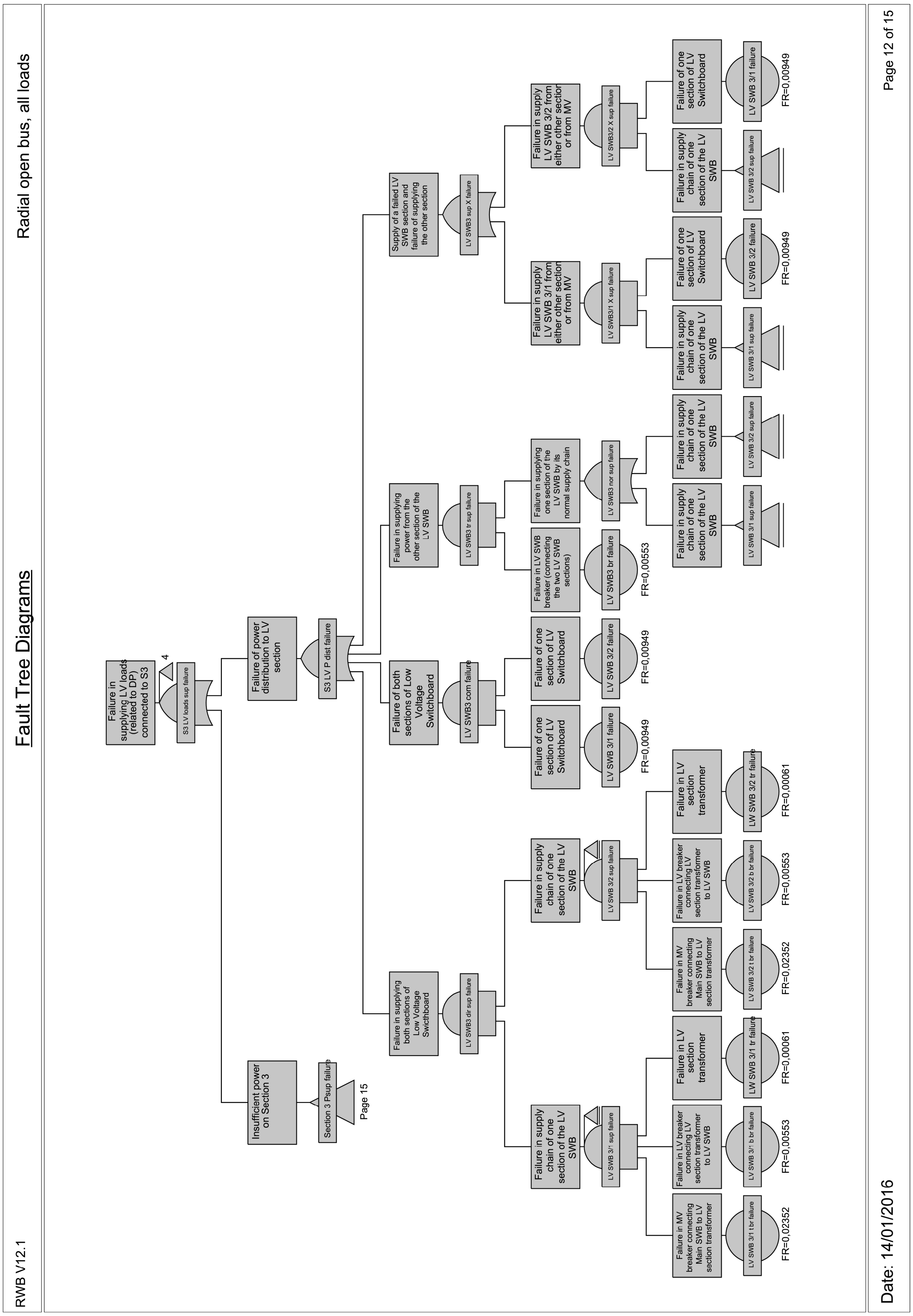

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Failure in supplying LV loads (related to DP) connected to S3
S3 LV loads sup failure
4
Insufficient power on Section 3
Section 3 Psup failure
Page 15
Failure of power distribution to LV section
S3 LV P dist failure
Failure in supplying both sections of Low Voltage Swichboard
LV SWB3 dir sup failure
Failure of both sections of Low Voltage Switchboard
LV SWB3 com failure
Failure in supplying power from the other section of the LV SWB
LV SWB3 tr sup failure
Supply of a failed LV SWB section and failure of supplying the other section
LV SWB3 sup X failure
Failure in supply chain of one section of the LV SWB
LV SWB 3/1 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 3/2 sup failure
Failure of one section of LV Switchboard
LV SWB 3/1 failure
FR=0,00949
Failure of one section of LV Switchboard
LV SWB 3/2 failure
FR=0,00949
Failure in LV SWB breaker (connecting the two LV SWB sections)
LV SWB3 br failure
FR=0,00553
Failure in supplying one section of the LV SWB by its normal supply chain
LV SWB3 nor sup failure
Failure in supply LV SWB 3/1 from either other section or from MV
LV SWB3/1 X sup failure
Failure in supply LV SWB 3/2 from either other section or from MV
LV SWB3/2 X sup failure
Failure in MV breaker connecting Main SWB to LV section transformer
LV SWB 3/1 t br failure
FR=0,02352
Failure in LV breaker connecting LV section transformer to LV SWB
LV SWB 3/1 b br failure
FR=0,00553
Failure in LV section transformer
LW SWB 3/1 tr failure
FR=0,00061
Failure in MV breaker connecting Main SWB to LV section transformer
LV SWB 3/2 t br failure
FR=0,02352
Failure in LV breaker connecting LV section transformer to LV SWB
LV SWB 3/2 b br failure
FR=0,00553
Failure in LV section transformer
LW SWB 3/2 tr failure
FR=0,00061
Failure in supply chain of one section of the LV SWB
LV SWB 3/1 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 3/2 sup failure
Failure in supply chain of one section of the LV SWB
LV SWB 3/1 sup failure
Failure of one section of LV Switchboard
LV SWB 3/2 failure
FR=0,00949
Failure in supply chain of one section of the LV SWB
LV SWB 3/2 sup failure
Failure of one section of LV Switchboard
LV SWB 3/1 failure
FR=0,00949
Date: 14/01/2016
Page 12 of 15

Figure 59 - Failure Tree, page 12/15

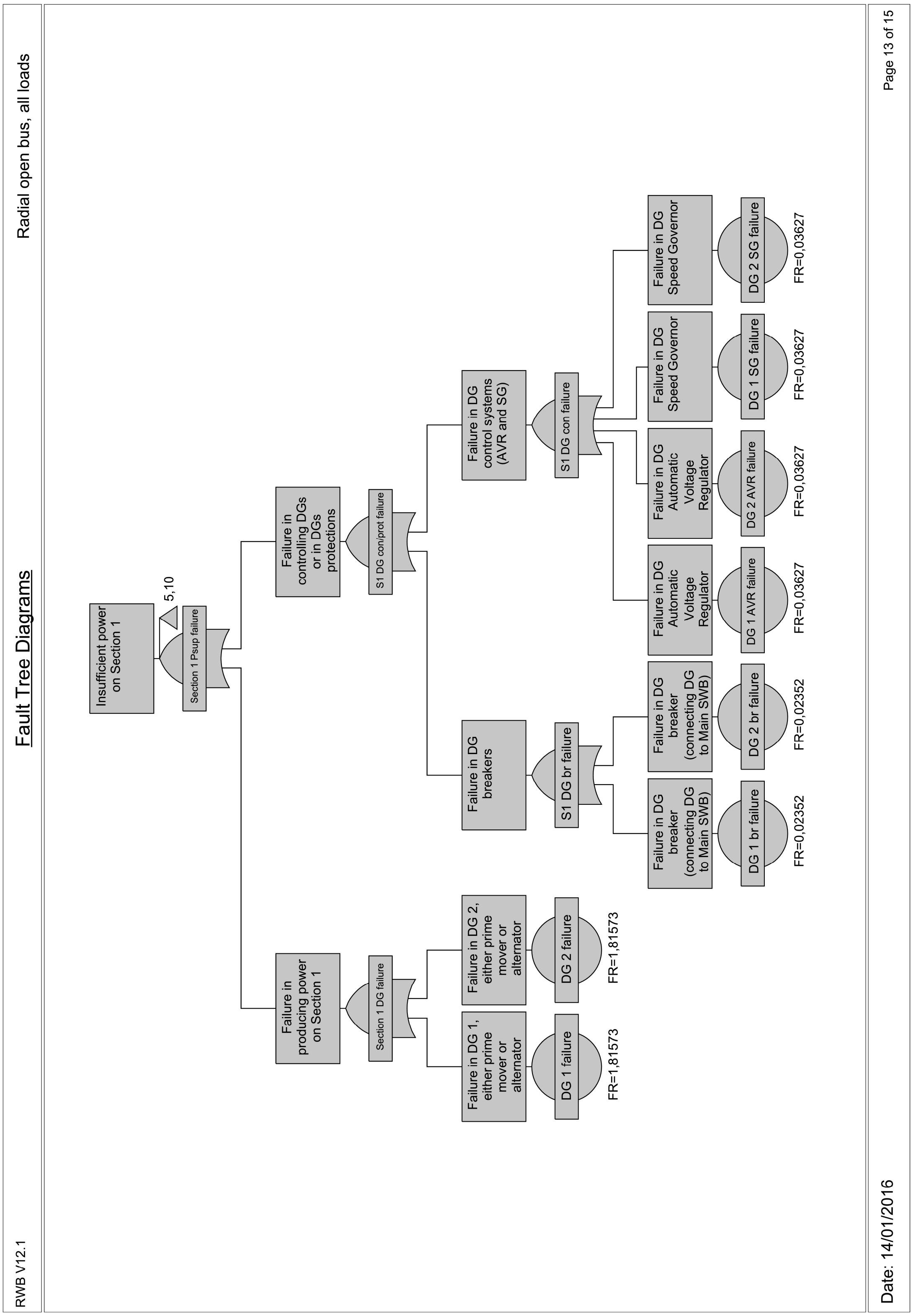

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Insufficient power on Section 1
Section 1 Psup failure
5,10
Failure in producing power on Section 1
Section 1 DG failure
Failure in DG 1, either prime mover or alternator
DG 1 failure
FR=1,81573
Failure in DG 2, either prime mover or alternator
DG 2 failure
FR=1,81573
Failure in controlling DGs or in DGs protections
S1 DG con/prot failure
Failure in DG breakers
S1 DG br failure
Failure in DG breaker (connecting DG to Main SWB)
DG 1 br failure
FR=0,02352
Failure in DG breaker (connecting DG to Main SWB)
DG 2 br failure
FR=0,02352
Failure in DG control systems (AVR and SG)
S1 DG con failure
Failure in DG Automatic Voltage Regulator
DG 1 AVR failure
FR=0,03627
Failure in DG Automatic Voltage Regulator
DG 2 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 1 SG failure
FR=0,03627
Failure in DG Speed Governor
DG 2 SG failure
FR=0,03627
Date: 14/01/2016
Page 13 of 15

Figure 60 - Failure Tree, page 13/15

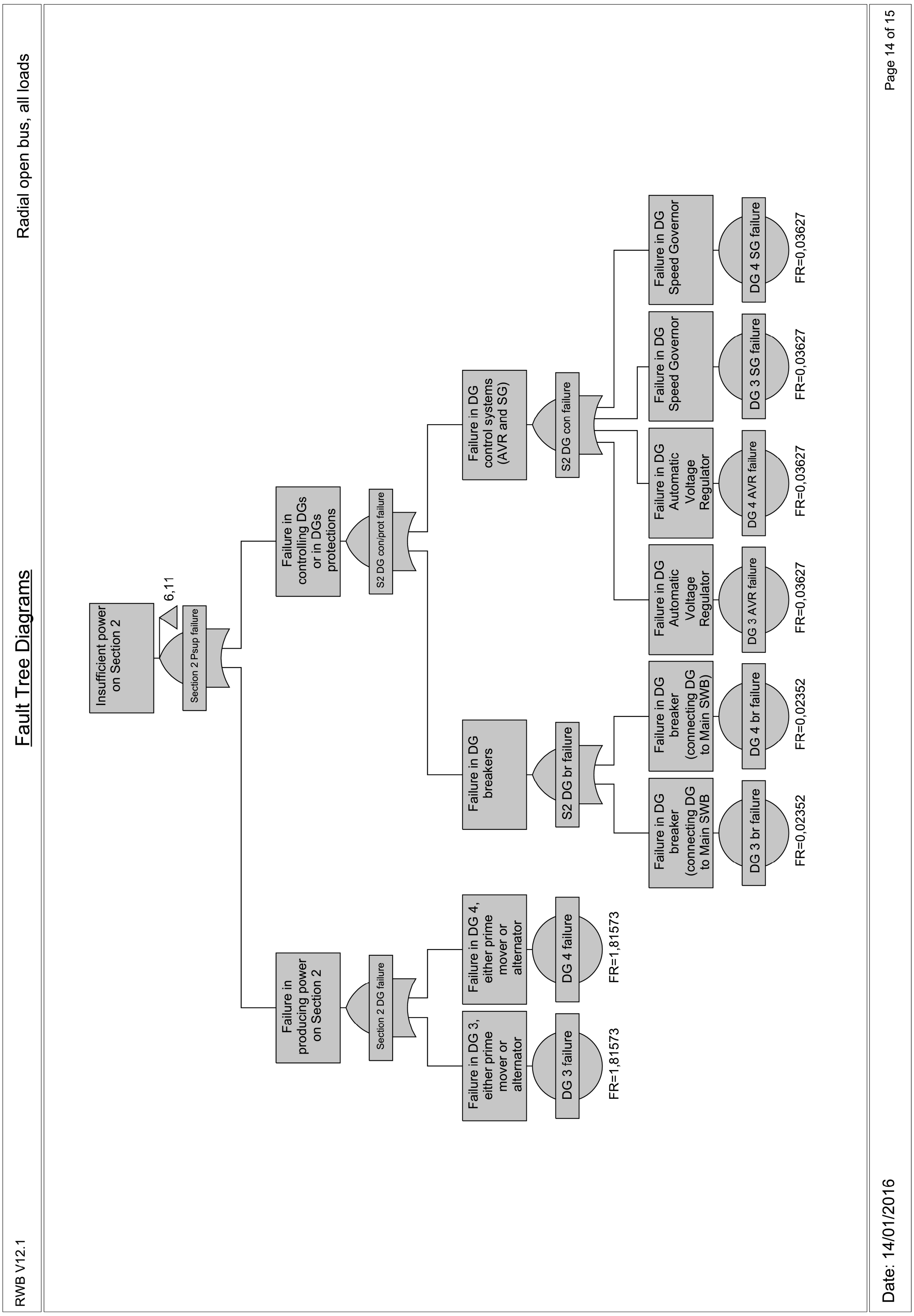

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Insufficient power on Section 2
Section 2 Psup failure
6,11
Failure in producing power on Section 2
Section 2 DG failure
Failure in DG 3, either prime mover or alternator
DG 3 failure
FR=1,81573
Failure in DG 4, either prime mover or alternator
DG 4 failure
FR=1,81573
Failure in controlling DGs or in DGs protections
S2 DG con/prot failure
Failure in DG breakers
S2 DG br failure
Failure in DG breaker (connecting DG to Main SWB
DG 3 br failure
FR=0,02352
Failure in DG breaker (connecting DG to Main SWB)
DG 4 br failure
FR=0,02352
Failure in DG control systems (AVR and SG)
S2 DG con failure
Failure in DG Automatic Voltage Regulator
DG 3 AVR failure
FR=0,03627
Failure in DG Automatic Voltage Regulator
DG 4 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 3 SG failure
FR=0,03627
Failure in DG Speed Governor
DG 4 SG failure
FR=0,03627
Date: 14/01/2016
Page 14 of 15

Figure 61 - Failure Tree, page 14/15

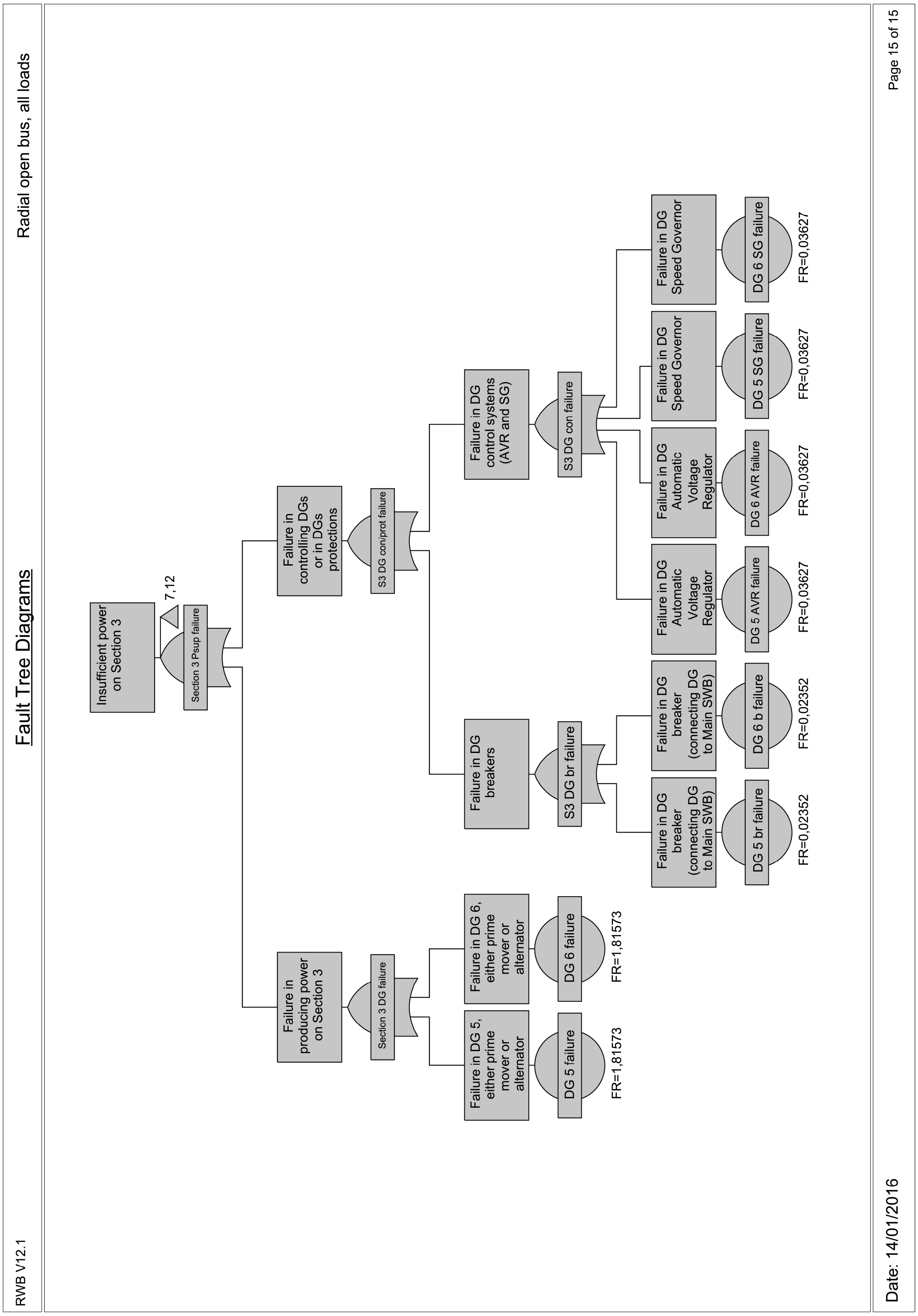

RWB V12.1
Fault Tree Diagrams
Radial open bus, all loads
Insufficient power on Section 3
Section 3 Psup failure
7,12
Failure in producing power on Section 3
Section 3 DG failure
Failure in controlling DGs or in DGs protections
S3 DG con/prot failure
Failure in DG 5, either prime mover or alternator
DG 5 failure
FR=1,81573
Failure in DG 6, either prime mover or alternator
DG 6 failure
FR=1,81573
Failure in DG breakers
S3 DG br failure
Failure in DG control systems (AVR and SG)
S3 DG con failure
Failure in DG breaker (connecting DG to Main SWB)
DG 5 br failure
FR=0,02352
Failure in DG breaker (connecting DG to Main SWB)
DG 6 b failure
FR=0,02352
Failure in DG Automatic Voltage Regulator
DG 5 AVR failure
FR=0,03627
Failure in DG Automatic Voltage Regulator
DG 6 AVR failure
FR=0,03627
Failure in DG Speed Governor
DG 5 SG failure
FR=0,03627
Failure in DG Speed Governor
DG 6 SG failure
FR=0,03627
Date: 14/01/2016
Page 15 of 15

Figure 62 - Failure Tree, page 15/15

Having built the Failure Tree, it is possible to apply the component's failure data previously shown to evaluate the several dependability attributes and figures depicted in Section 5.3 of Chapter 5 (page 106 ff.). The software used for the Fault Tree Analysis does such calculations automatically, starting from the fault events parameters depicted in Table 14 (page 125). The mathematical figures most relevant to the design process are:

- Unavailability;
- Frequency (of the fault);
- Fussell-Vesely Importance;
- Birnbaum Importance.

The results of the first two indices calculation is shown in Table 15, pointing out an entry for each component's failure model used during the analysis. In addition to that, in the same table are depicted the Failure Tree events associated to each failure model. The nomenclature here applied is coherent with the one used in the diagram, thus allowing associating these events data with their exact position in the FT.

It must be remarked that there is a difference between failure rate and failure frequency, which is also visible comparing the results calculated for the fault events (shown in Table 15) with the failure data depicted in Table 14 (page 125). In fact, failure rate assesses only the number of possible failures in a given time range, considering each faulted component as immediately repaired or changed. Conversely, fault frequency considers also MTTR, which is the time needed for the component repairing/substitution (obviously, in such time span the component cannot fail because it is already faulted). This leads to different results between failure rate and frequency especially for components with a high MTTR.

The failure frequency and unavailability figures are related (as shown in equation (**6.3**-**2**), page 124), thus it is sufficient to consider only one. The choice here done is to use failure frequency, because it is more immediate to understand, even by people with only basic knowledge about dependability theory. Analyzing the results, it is possible to highlight the components that have the highest failure frequency, which are:

- Diesel Generators;
- DP thrusters.

These are followed by other events with much less failure frequency. Due to that, it may be significant to assess the system's dynamic response to these two events through the simulation software.

Table 15 - Calculated Unavailability and Frequency for the fault events

ID	Associated events	Unavailability	Frequency [faults/year]
Adjustable Speed Drive failure	DP sd 1/1 failure, DP sd 2/1 failure, DP sd 3/1 failure, DP sd 1/2 failure, DP sd 2/2 failure, DP sd 3/2 failure	4,169e-5	0,02207
DG controls failure	DG 1 AVR failure, DG 3 AVR failure, DG 2 AVR failure, DG 4 AVR failure, DG 5 AVR failure, DG 6 AVR failure, DG 1 SG failure, DG 2 SG failure, DG 3 SG failure, DG 4 SG failure, DG 5 SG failure, DG 6 SG failure	3,095e-4	0,03626
Diesel Generator failure	DG 1 failure, DG 2 failure, DG 3 failure, DG 4 failure, DG 5 failure, DG 6 failure	5,172e-3	1,806
DP thruster failure	DP th 1/1 failure, DP th 2/1 failure, DP th 3/1 failure, DP th 1/2 failure, DP th 2/2 failure, DP th 3/2 failure	1,74e-2	0,8966
LV circuit breaker failure NO	LV SWB1 br failure, LV SWB 1/1 b br failure, LV SWB 1/2 b br failure, LV SWB 2/1 b br failure, LV SWB 2/2 b br failure, LV SWB2 br failure, LV SWB 3/1 b br failure, LV SWB 3/2 b br failure, LV SWB3 br failure	1,263e-6	0,00553
LV Switchboard failure	LV SWB 1/1 failure, LV SWB 1/2 failure, LV SWB 2/1 failure, LV SWB 2/2 failure, LV SWB 3/1 failure, LV SWB 3/2 failure	7,897e-6	0,00949
MV circuit breaker failure high current	DG 1 br failure, DG 3 br failure, DG 5 br failure, DG 2 br failure, DG 4 br failure, DG 6 br failure, DP sys 1/1 br failure, DP sys 2/1 br failure, DP sys 3/1 br failure, DP sys 1/2 br failure, DP sys 2/2 br failure, DP sys 3/2 br failure, LV SWB 1/1 t br failure, LV SWB 1/2 t br failure, LV SWB 2/1 t br failure, LV SWB 2/2 t br failure, LV SWB 3/1 t br failure, LV SWB 3/2 t br failure	3,974e-5	0,02352
MV Switchboard failure	MV SWB 1/1 failure, MV SWB 1/2 failure, MV SWB 2/1 failure, MV SWB 2/2 failure, MV SWB 3/1 failure, MV SWB 3/2 failure	4,649e-6	0,01794
MV/LV transformer failure	DP sys 1/1 tr failure, DP sys 2/1 tr failure, DP sys 3/1 tr failure, DP sys 1/2 tr failure, DP sys 2/2 tr failure, DP sys 3/2 tr failure, LW SWB 1/1 tr failure, LW SWB 1/2 tr failure, LW SWB 2/1 tr failure, LW SWB 2/2 tr failure, LW SWB 3/1 tr failure, LW SWB 3/2 tr failure	2,785e-7	0,00061

It must be remarked that the simulation of the dynamic IPS behavior may be done for each fault event, but such a practice will lead to a huge amount of both simulations to be done and related results to be evaluated. In the simplified case here shown the base fault events are eleven, which can combine in several different ways in order to lead to the top-event (combinations that can be deduced analyzing the fault tree). The simulation of all these events not only will take a high amount of time, but also will give results whose usefulness is not definable. In fact, to properly define which events are worth the investment of resources needed for the simulation and the evaluation of the results, the other two indices above mentioned are needed: FV and BB importance.

The calculated Fussell-Vesely (FV) and Birnbaum (BB) importance indices for each fault event and gate of the FT are shown in Table 16, sorted by FV (from high to low). Analyzing such results it is possible to define the events and the gates which have the most impact on the top-event, thus allowing the definition of the most useful place in which intervene with a redesign activity. This allows to focus the simulation activity only on the events and gates that are worth to be modified. (How FV and BB indices have to be evaluated has been explained in Section 5.3 of Chapter 5, page 106 ff.). The most impacting events are the ones with a high FV value, which are:

- DP thruster failures;
- DG failures;
- DG controls failures.

Among them, an evaluation of the BB index can be done, to assess if it is the case of improving the single component or the design of the overall system. In the case study here depicted, all the events have low values of the BB index, implying that the system design has been done well. The only viable option inferable by the dependability analysis is the improvement of the single component's dependability parameters. However, such an improvement it is not responsibility of the shipyard, but it is the result of a process that has to be done by the suppliers. Due to that, if no supplier worldwide is capable of offering a more dependable component/subsystem, nothing can be done also in this regard.

Table 16 - Calculated Fussell-Vesely and Birnbaum importance indices for each FT gate and event

ID	Event description	FV importance	BB importance
DP th 3/2 failure	Failure in DP thruster 3/2 (azimuting fixed pitch propeller)	0,2341	4,663e-2
DP th 1/2 failure	Failure in DP thruster 1/2 (azimuting fixed pitch propeller)	0,2341	4,663e-2
DP th 2/2 failure	Failure in DP thruster 2/2 (azimuting fixed pitch propeller)	0,2341	4,663e-2
DP th 3/1 failure	Failure in DP thruster 3/1 (azimuting fixed pitch propeller)	0,2341	4,663e-2
DP th 1/1 failure	Failure in DP thruster 1/1 (azimuting fixed pitch propeller)	0,2341	4,663e-2
DP th 2/1 failure	Failure in DP thruster 2/1 (azimuting fixed pitch propeller)	0,2341	4,663e-2
DG 1 failure	Failure in DG 1, either prime mover or alternator	0,08698	5,829e-2
DG 4 failure	Failure in DG 4, either prime mover or alternator	0,08698	5,829e-2
DG 6 failure	Failure in DG 6, either prime mover or alternator	0,08698	5,829e-2
DG 3 failure	Failure in DG 3, either prime mover or alternator	0,08698	5,829e-2
DG 5 failure	Failure in DG 5, either prime mover or alternator	0,08698	5,829e-2
DG 2 failure	Failure in DG 2, either prime mover or alternator	0,08698	5,829e-2
DG 4 AVR failure	Failure in DG Automatic Voltage Regulator	0,005205	5,829e-2
DG 1 AVR failure	Failure in DG Automatic Voltage Regulator	0,005205	5,829e-2
DG 3 AVR failure	Failure in DG Automatic Voltage Regulator	0,005205	5,829e-2
DG 2 AVR failure	Failure in DG Automatic Voltage Regulator	0,005205	5,829e-2

ID	Event description	FV importance	BB importance
DG 1 SG failure	Failure in DG Speed Governor	0,005205	5,829e-2
DG 2 SG failure	Failure in DG Speed Governor	0,005205	5,829e-2
DG 5 AVR failure	Failure in DG Automatic Voltage Regulator	0,005205	5,829e-2
DG 6 AVR failure	Failure in DG Automatic Voltage Regulator	0,005205	5,829e-2
DG 5 SG failure	Failure in DG Speed Governor	0,005205	5,829e-2
DG 6 SG failure	Failure in DG Speed Governor	0,005205	5,829e-2
DG 3 SG failure	Failure in DG Speed Governor	0,005205	5,829e-2
DG 4 SG failure	Failure in DG Speed Governor	0,005205	5,829e-2
DG 2 br failure	Failure in DG breaker (connecting DG to Main SWB)	0,0006683	5,829e-2
DG 4 br failure	Failure in DG breaker (connecting DG to Main SWB)	0,0006683	5,829e-2
DG 6 br failure	Failure in DG breaker (connecting DG to Main SWB)	0,0006683	5,829e-2
DG 3 br failure	Failure in DG breaker (connecting DG to Main SWB	0,0006683	5,829e-2
DG 5 br failure	Failure in DG breaker (connecting DG to Main SWB)	0,0006683	5,829e-2
DG 1 br failure	Failure in DG breaker (connecting DG to Main SWB)	0,0006683	5,829e-2
DP sd 3/1 failure	Failure in DP thruster 3/1 adjustable speed drive	0,000561	4,663e-2
DP sd 1/2 failure	Failure in DP thruster 1/2 adjustable speed drive	0,000561	4,663e-2
DP sd 2/1 failure	Failure in DP thruster 2/1 adjustable speed drive	0,000561	4,663e-2
DP sd 1/1 failure	Failure in DP thruster 1/1 adjustable speed drive	0,000561	4,663e-2

ID	Event description	FV importance	BB importance
DP sd 3/2 failure	Failure in DP thruster 3/2 adjustable speed drive	0,000561	4,663e-2
DP sd 2/2 failure	Failure in DP thruster 2/2 adjustable speed drive	0,000561	4,663e-2
DP sys 3/1 br failure	Failure in DP system circuit breaker on MV side	0,0005346	4,663e-2
DP sys 1/2 br failure	Failure in DP system circuit breaker on MV side	0,0005346	4,663e-2
DP sys 2/1 br failure	Failure in DP system circuit breaker on MV side	0,0005346	4,663e-2
DP sys 2/2 br failure	Failure in DP system circuit breaker on MV side	0,0005346	4,663e-2
DP sys 1/1 br failure	Failure in DP system circuit breaker on MV side	0,0005346	4,663e-2
DP sys 3/2 br failure	Failure in DP system circuit breaker on MV side	0,0005346	4,663e-2
MV SWB 2/2 failure	Failure of one section of MV Switchboard	6,255E-05	4,663e-2
MV SWB 3/1 failure	Failure of one section of MV Switchboard	6,255E-05	4,663e-2
MV SWB 3/2 failure	Failure of one section of MV Switchboard	6,255E-05	4,663e-2
MV SWB 1/1 failure	Failure of one section of MV Switchboard	6,255E-05	4,663e-2
MV SWB 1/2 failure	Failure of one section of MV Switchboard	6,255E-05	4,663e-2
MV SWB 2/1 failure	Failure of one section of MV Switchboard	6,255E-05	4,663e-2
DP sys 1/2 tr failure	Failure in DP system transformer	3,748E-06	4,663e-2
DP sys 2/2 tr failure	Failure in DP system transformer	3,748E-06	4,663e-2
DP sys 3/2 tr failure	Failure in DP system transformer	3,748E-06	4,663e-2
DP sys 1/1 tr failure	Failure in DP system transformer	3,748E-06	4,663e-2
DP sys 2/1 tr failure	Failure in DP system transformer	3,748E-06	4,663e-2
DP sys 3/1 tr failure	Failure in DP system transformer	3,748E-06	4,663e-2

ID	Event description	FV importance	BB importance
S3 LV P dist failure*	Failure of power distribution to LV section*	0	1,455e-12
S2 LV P dist failure*	Failure of power distribution to LV section*	0	1,455e-12
S1 LV P dist failure*	Failure of power distribution to LV section*	0	1,455e-12

The dependability analysis of the system highlighted most frequent failures in the designed system, and the components/subsystems on which is most convenient to intervene from a dependability point of view. However, from the results shown above, the most frequent faults are related to components that are installed in the system with a design that already takes into account their high failure frequency. The lack of evident impacting events is mainly due to the heavy simplification in system here applied, done with the aim of easing the demonstration of the applicability of the proposed process. Nevertheless, also in such a simplified dependability analysis some events worth to be taken into account can be defined. As an example, the Diesel Generator's failure has proven to be one of the most frequent onboard. Its impact on the system's dependability is high, as shown by the FV index, but no intervention can be easily done to lower its impact since the design is already sufficiently robust, as shown by the BB index. In fact, the best improvement will be the increase of component's failure rate. However, such parameter is not modifiable by the designer, being pertaining to DG supplier. This may seem an impasse situation, but a relevant concept about FTA has to be remarked: the analysis is totally dependent on the selected top-event. In this case the top-event was the loss of the DP capability, which is unaffected by a single DG failure. However, if another top-event is selected, a single DG failure can became critical. It is the case of a top-event defined as follows: the capability of supplying all the onboard loads foreseen by the electric loads balance. In this case, the loss of a DG will lower the power generation capabilities of its related IPS section, down to a level below the quota of loads to be supplied by each MV switchboard in the considered operating condition. Due to that, one of the IPS sections may lose its capability to supply all its connected loads, leading to the top-event. This example remarks the need of clearly define all the hypotheses used during the dependability analysis, in order to not deduce wrong conclusions from the analysis results (which are exact, but limited in application area by the starting hypotheses). Due to these considerations, the fault to be simulated in the following design steps will be the failure of a single DG in the abovementioned operating conditions.

6.4.3 Electromechanical transients simulation

The dependability analysis and the evaluation of its quantitative results, shown above, were the first two steps of the innovative design process. In order to perform the following two design steps it is necessary to simulate the selected fault scenarios and propose solutions to possible issues. The dependability analysis results evaluation has led to the decision of simulating the dynamic behavior of the IPS following the fault of a DG, because such a failure has been deemed as the most representative case, able to highlight the advantages that a dynamic simulation can give to design process.

The dynamic simulation of the system (electromechanical transients and steady-state) is performed using an ensemble of mathematical models of the various system components built in Matlab® Simulink® software environment. The system's model has been built using as foundations those shown in [103], [100], and [102], applying the modifications needed in order to represent the IPS of the case study drillship. The overall Simulink® model is shown in Figure 63, while an explanation of the single blocks is not in the scope of this thesis work. In case of need, reference can be done to the above mentioned literature.

The main system parameters have been depicted in Section 6.3.1 of this Chapter, while specific components parameters have been set using default data taken from experience. This has been done due to the absence of most of these parameters in the case study data, which refers to a ship which is still in preliminary design phase. However, the goal of the case study is not to accurately simulate a particular vessel's IPS, but to demonstrate the applicability of the proposed innovative design process, thus making irrelevant the accuracy of the parameters. Due to that, simulation result are shown in relative representation (per-unit) to highlight the difference in respect to rated values, thus ignoring their absolute values. The system's state before the fault can be inferred by the previous sections. In fact, the hypotheses stated in Section 6.4.1 are still valid, thus leading to the simulation of the IPS in the following conditions:

- Operation in normal drilling, normal marine conditions configuration;
- Open bus condition (the three MV switchboards are separated);
- Simulated fault condition → failure of one DG (modeled in the software as a sudden opening of the generator's breaker).

The results of the simulation are shown in Figure 64, Figure 65, Figure 66, Figure 67, and Figure 68. These show respectively: remaining DG frequency and voltage; active and reactive powers supplied by the DGs connected to the MV switchboard in which the fault is simulated; voltage on the MV switchboard in which the fault is simulated.

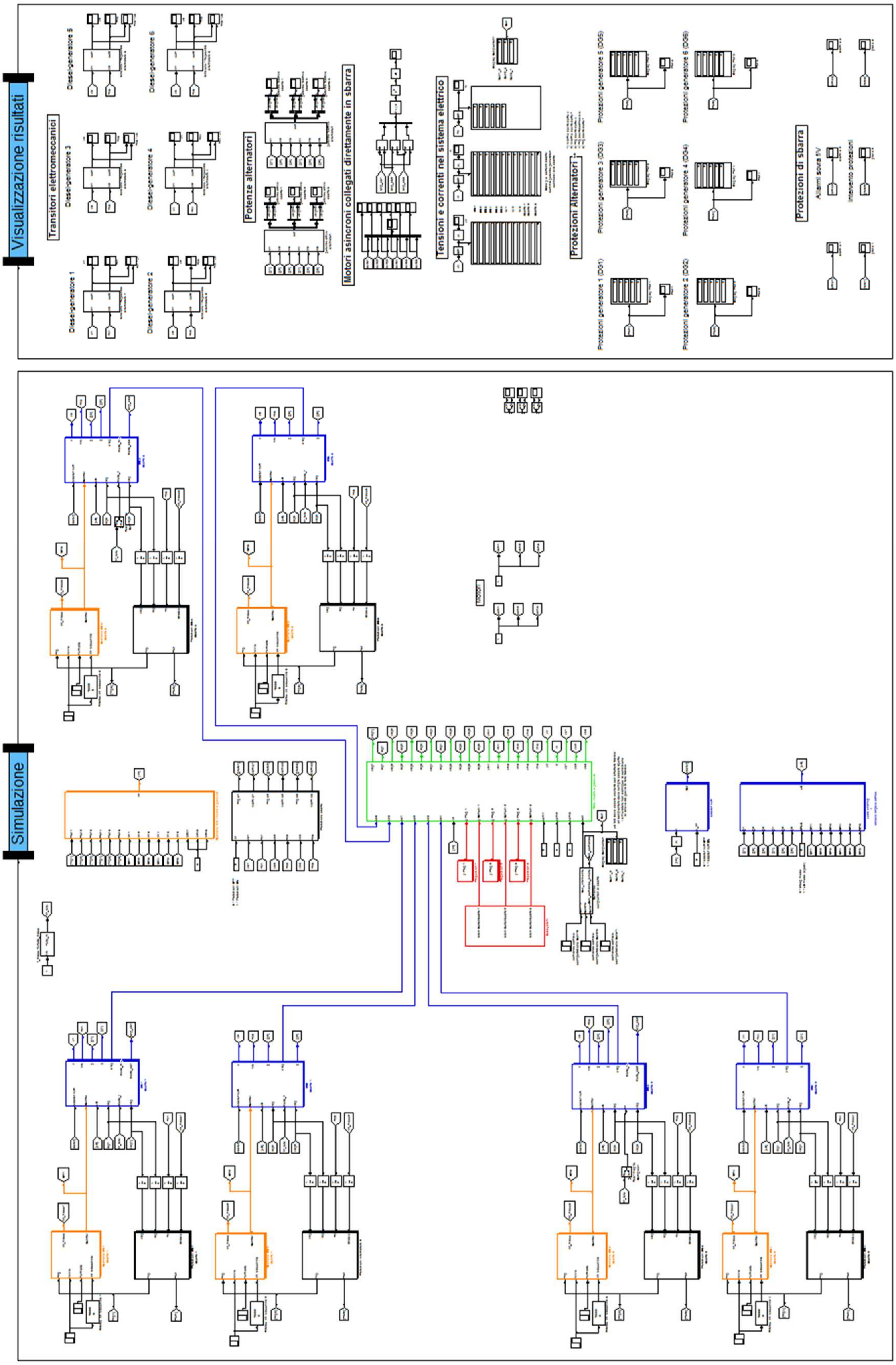

Visualizzazione risultati
Transitori elettromeccanici
Dieselgeneratore 1
Dieselgeneratore 2
Dieselgeneratore 3
Dieselgeneratore 4
Dieselgeneratore 5
Dieselgeneratore 6
Potenze alternatori
Motori asincroni collegati direttamente in sbarra
Tensioni e correnti nel sistema elettrico
Protezioni Alternatori
Protezioni generatore 1 (DG1)
Protezioni generatore 2 (DG2)
Protezioni generatore 3 (DG3)
Protezioni generatore 4 (DG4)
Protezioni generatore 5 (DG5)
Protezioni generatore 6 (DG6)
Protezioni di sbarra
Intervento protezioni
Simulazione

Figure 63 - Matlab® Simulink® model of the IPS for electromechanical transients' simulation

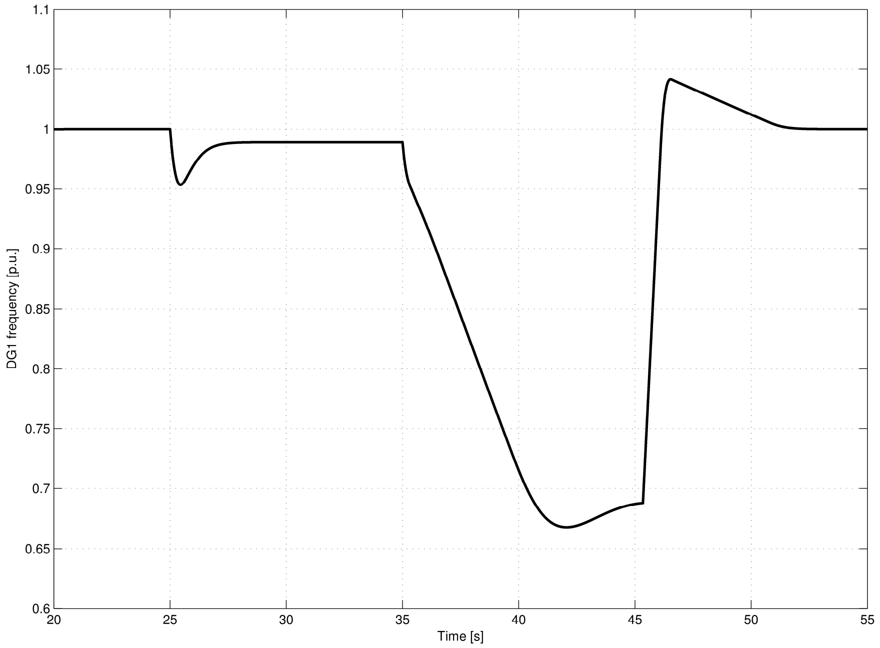


Figure 64 - Simulated DG fault, frequency of the remaining DG

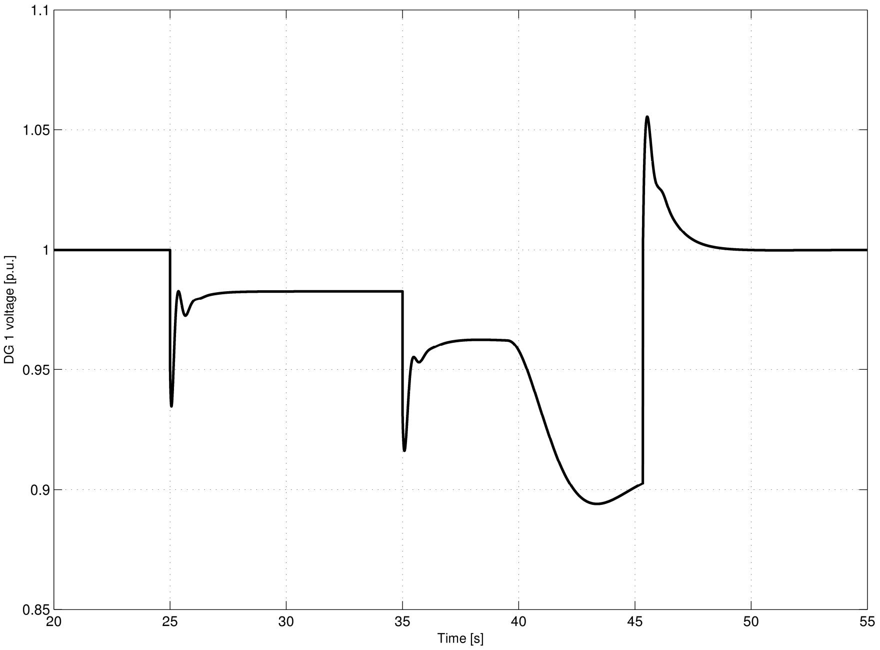


Figure 65 - Simulated DG fault, voltage of the remaining DG

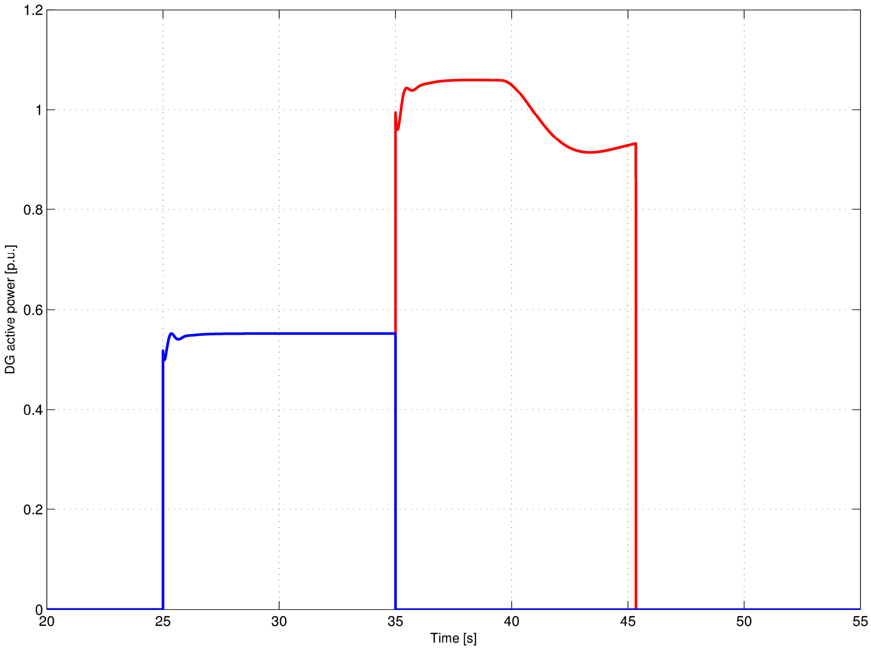


Figure 66 – Simulated DG fault, active power of the DGs (red - remaining DG; blue - failed DG)

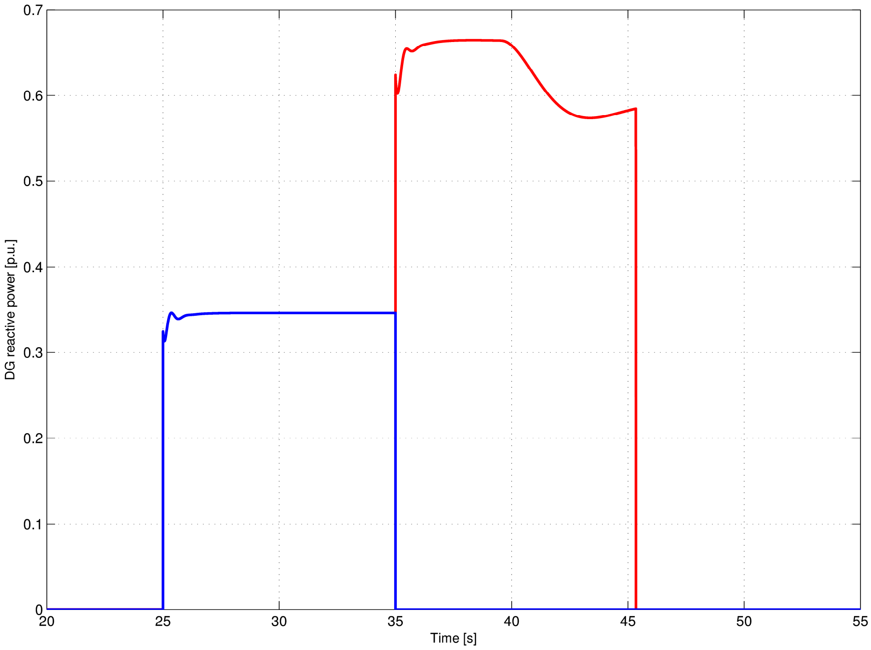


Figure 67 – Simulated DG fault, reactive power of the DGs (red - remaining DG; blue - failed DG)

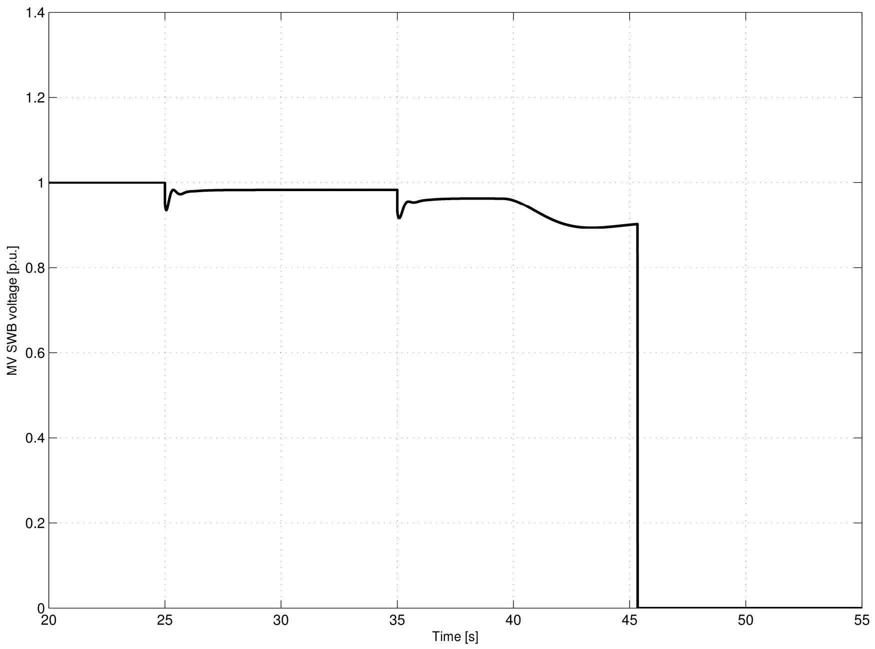


Figure 68 – Simulated DG fault, voltage on the MV Switchboard

The simulation results show different events happening at well-defined time instants:

- t = 25 s application of the full load to the system;
- t = 35 s failure of one DG (sudden disconnection from the MV SWB);
- t > 45 s IPS section black-out (loss of power supply on MV SWB).

Evaluating the simulation outcomes, it is evident that the simulated fault condition is not bearable by the single IPS section (while the other two sections remain fully operative thanks to the open bus configuration). In fact, the load applied on the single section is higher than the remaining generator's active power capability, thus leading to its disconnection due to either under-frequency protection or overload protection (depending on which acts faster). In this condition the IPS is not able to supply its correct service to the users.

As mentioned during dependability analysis, the single IPS section black-out caused by the fault event is not an issue if the given top-event is considered (*DP failure*). This happens due to the presence of the other two independent IPS sections. However, a black-out is still a condition that must be avoided in an AES, even if partial. Due to that, a possible solution able to prevent such a harmful outcome has been conceived: the application of a load shedding algorithm. In practice, when the frequency of a MV switchboard drops below a fixed limit (here set at 0.8 p.u.), some loads are disconnected to allow keeping the generator into its power capability limits. The loads that can be removed are to be defined clearly, because they should be loads whose impact on the system operation is minimal. In particular, in the case of a DP vessel the loads to be shed must not be related to the DP operation, thus leaving a limited amount of possibilities. The loads selected for the disconnection in case of need are:

- Drilling system (assuring at least one mud pump in operation, to avoid getting the drill stuck in the well);
- HVAC systems (down to the minimum ventilation needed to avoid buildup of carbon monoxide in the ship locals);
- Accommodation loads (assuring only essential systems, such as light and sanitary systems).

This load shedding allows reducing the power of the loads connected to one MV switchboard from 9354 kW absorbed in normal condition down to 3660 kW, which is a power level bearable by a single DG (which rated power is 7700 kW). To demonstrate the effectiveness of such a solution another simulation has been performed, implementing the load-shedding algorithm. The results are shown in Figures spanning from Figure 69 to Figure 73 in the same order as before. As can be easily seen, the load shedding intervention allows recovering the frequency on the remaining DG due to the lowering in the supplied loads. This in turn avoids the occurrence of a black out, demonstrating the effectiveness of the proposed solution.

However, this leaves the system in a configuration which is not supposed to last forever: a degraded service. In fact, after the application of an emergency action a new configuration has to be achieved, which must be able to supply the system in the normal condition once again (correct service). Several different solutions can be applied to recover a normal operating conditions. Some examples are:

- Connection of the redundant unities, present on the two healthy switchboards, in place of the unities disconnected by the emergency action;
- Use of an operating configuration with lower power requirements;
- Reconfiguration of the network as a closed bus, to allow reconnecting the loads disconnected by the emergency action.

The definition of the action to be applied is up to the designer, which have to found a solution able to be compliant with the requirements. As an example, the closed bus solution is not applicable if the designed IPS is not able to correctly function in such a condition (due to either protections inadequacy, or absence of a PMS able to withstand the different needs of a closed bus operation). Conversely, an operating configuration with lower power requirements may be not feasible, leading to a stop of the drilling operations (with related penalties).

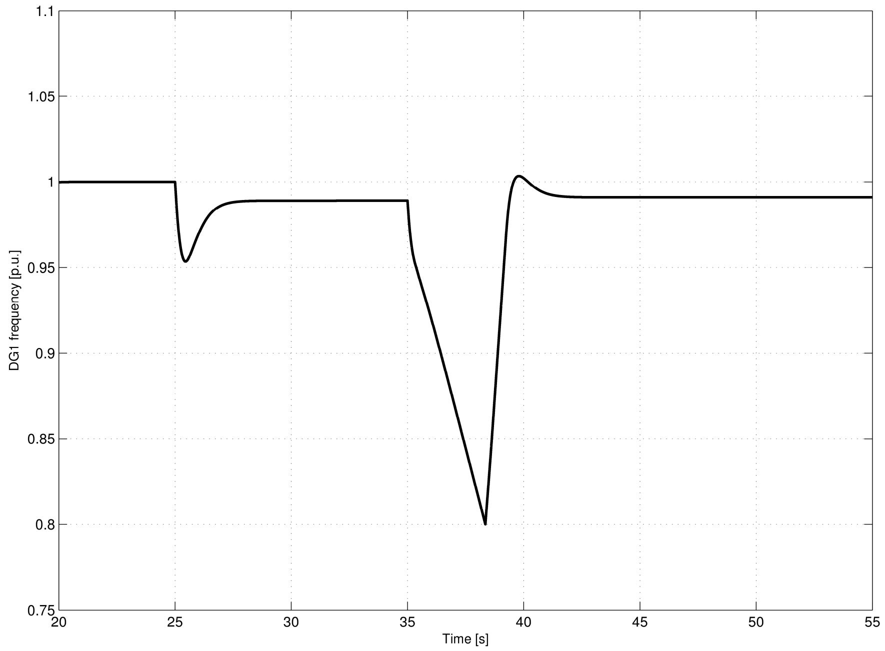


Figure 69 - Simulated DG fault and load shedding, frequency of the remaining DG

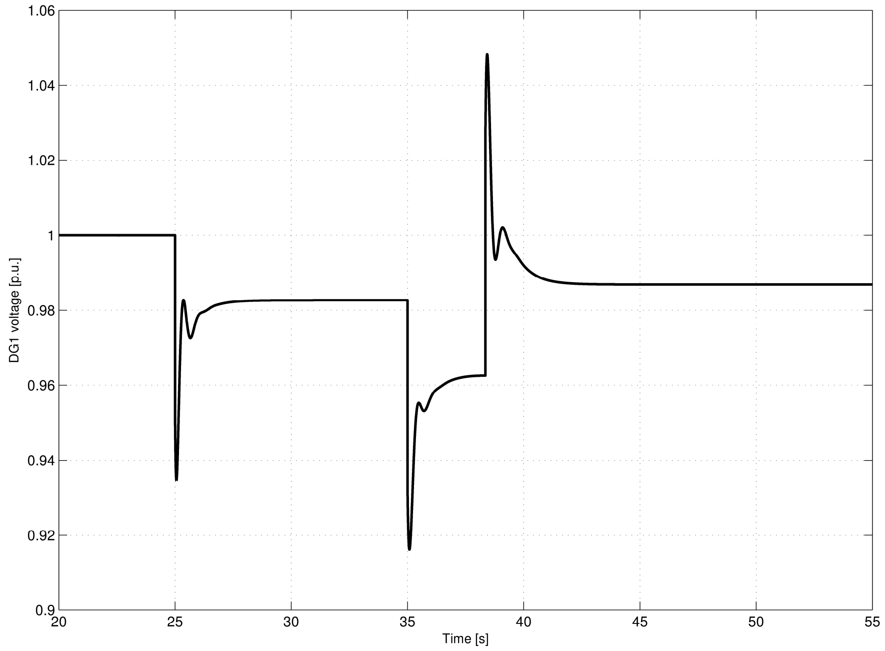


Figure 70 - Simulated DG fault and load shedding, voltage of the remaining DG

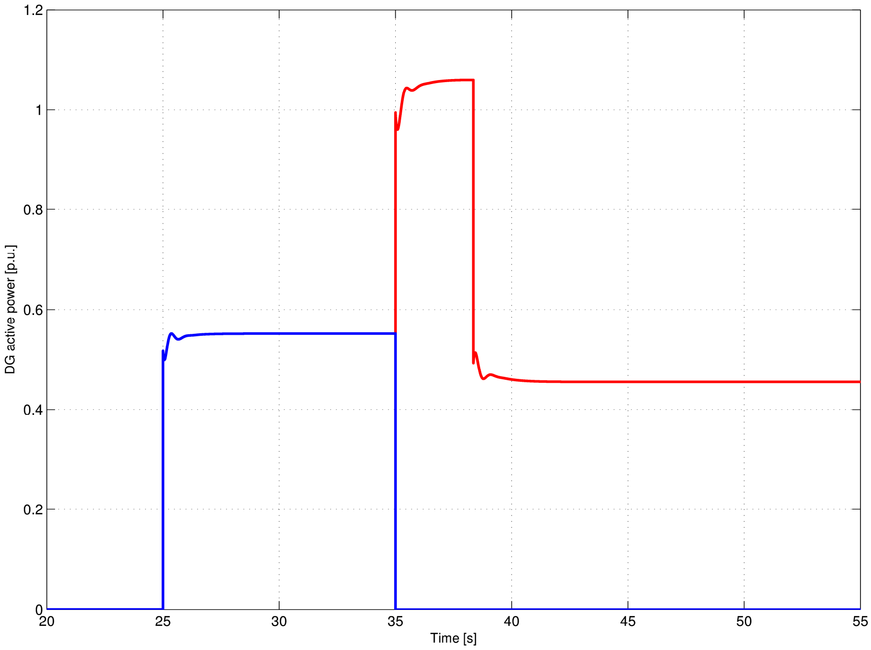


Figure 71 – Simulated DG fault and load shedding, active power of the DGs (red - remaining DG; blue - failed DG)

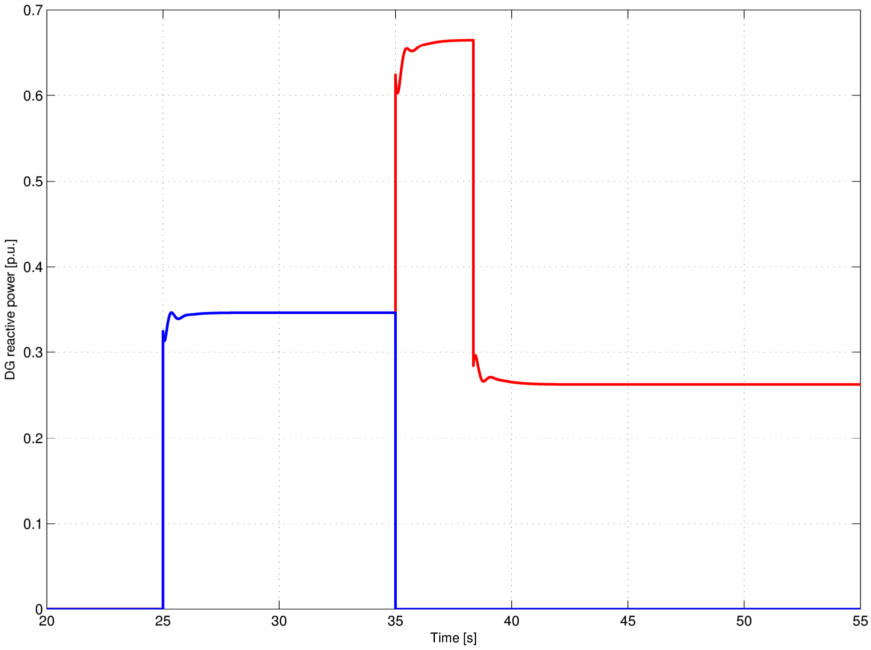


Figure 72 – Simulated DG fault and load shedding, active power of the DGs (red - remaining DG; blue - failed DG)

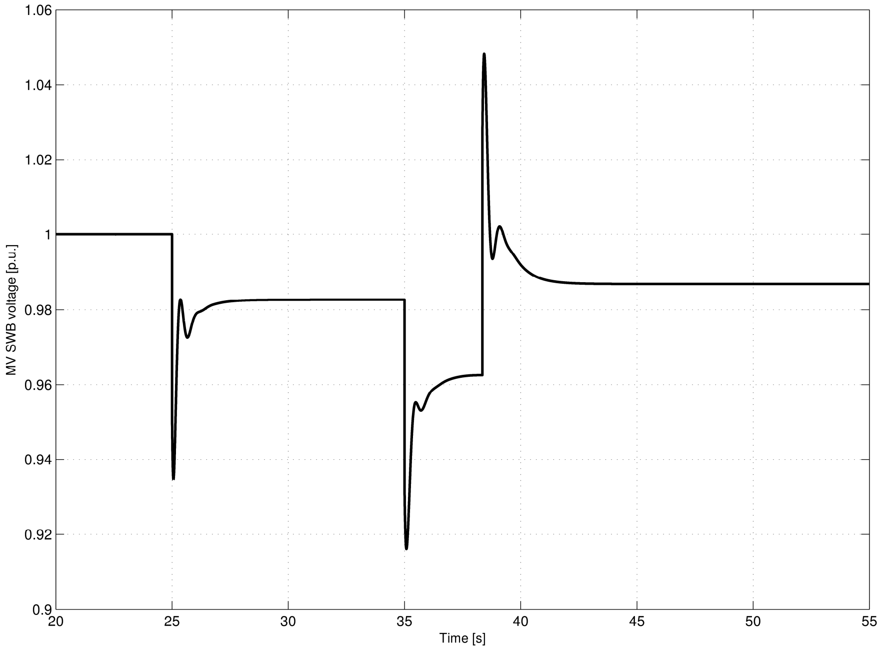


Figure 73 - Simulated DG fault and load shedding, voltage on the MV Switchboard

The definition of the actions to be taken after the emergency response to a fault can be done with the aid of the software simulator, similarly to what has been done for defining the emergency action itself. Simulations allow trying several different solutions to select the most suited on the base of its outcomes. In this case study, it has been supposed the design of an IPS able to operate correctly also in closed bus condition. Due to that, the selected recovery action to be implemented after the emergency load shedding imply the use of the closed bus. Indeed, the defined recovery action operates as follows:

- Wait until frequency of the remaining DG is stabilized;
- Start of the MV SWBs synchronization;
- Close the tie-breaker between two MV SWBs when the angle difference between their voltages phasors (calculated through Park transformation [109]) is under 5 degrees;
- Wait 10 s to allow running DGs active and reactive load sharing stabilization;
- Reconnect the loads removed by the load shedding action.

The result of the supplication of such a recovery action is shown in figures spanning from Figure 74 to Figure 78, with the same order as before. To allow appreciate the entire automatic fault response action, the simulation results will show the system's variables evolution starting from the DG fault event.

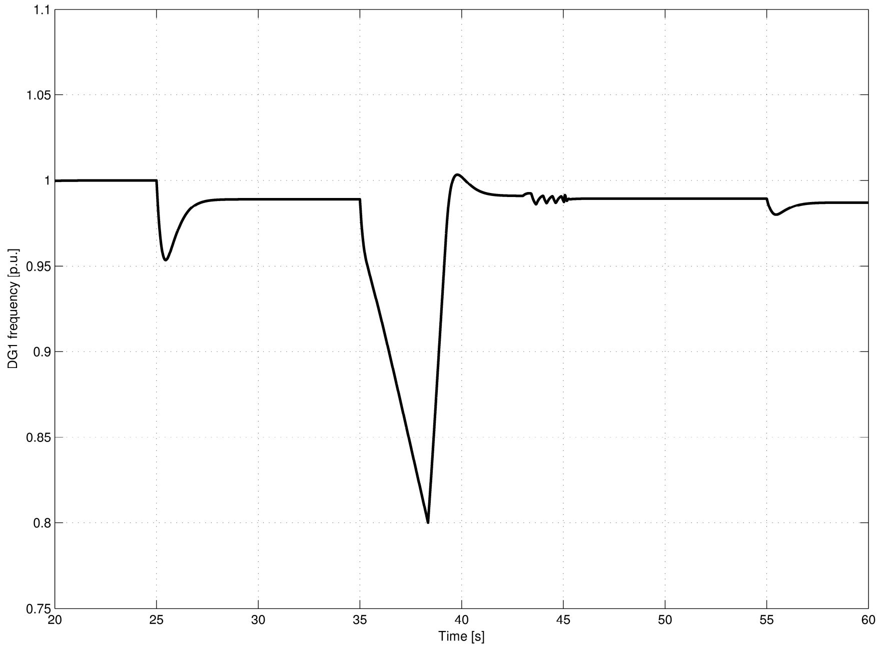


Figure 74 - Simulated DG fault and automatic recovery action, frequency of the remaining DG

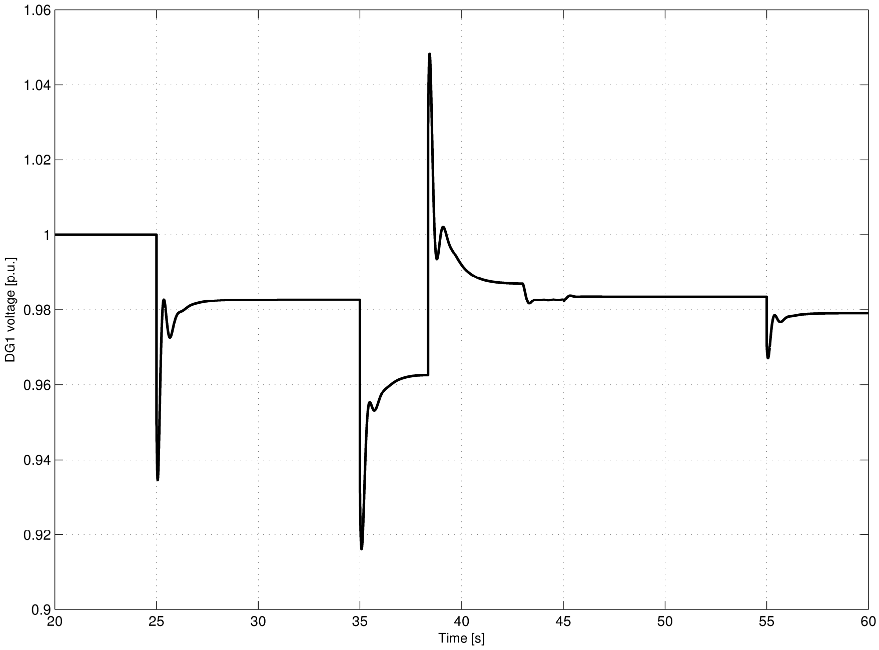


Figure 75 - Simulated DG fault and automatic recovery action, voltage of the remaining DG

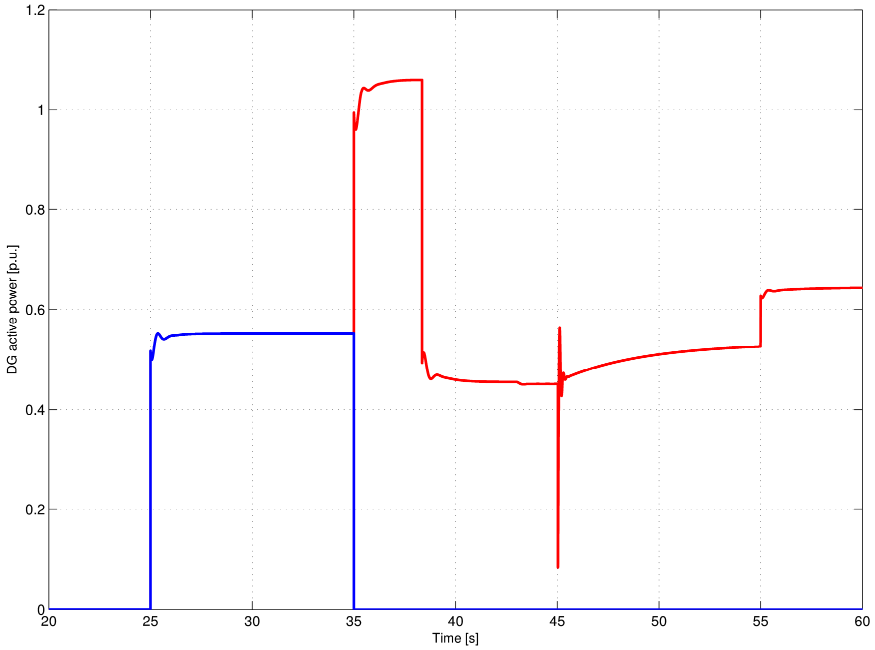


Figure 76 - Simulated DG fault and automatic recovery action, active power of the DGs (red - remaining DG; blue - failed DG)

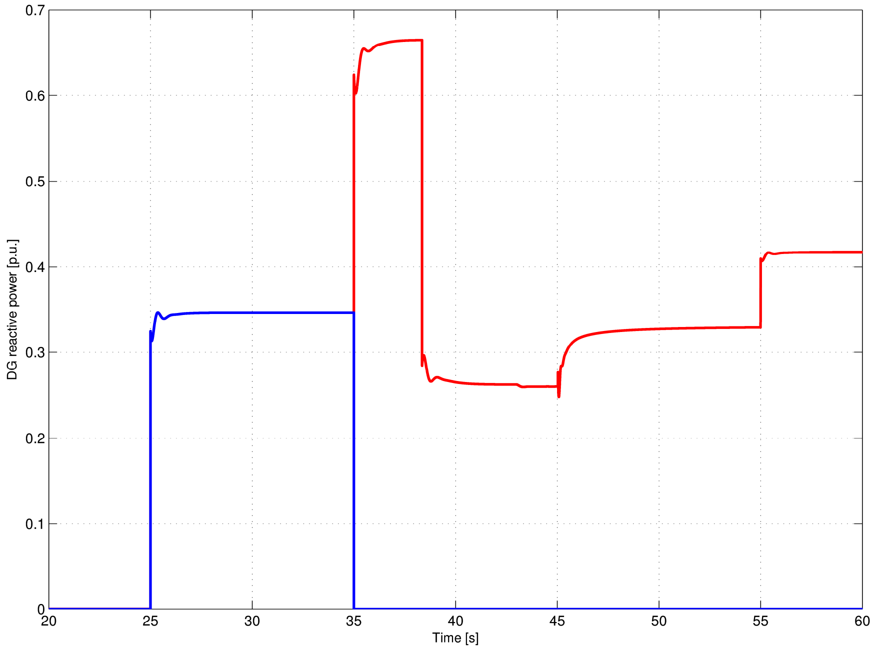


Figure 77 - Simulated DG fault and automatic recovery action, reactive power of the DGs (red - remaining DG; blue - failed DG)

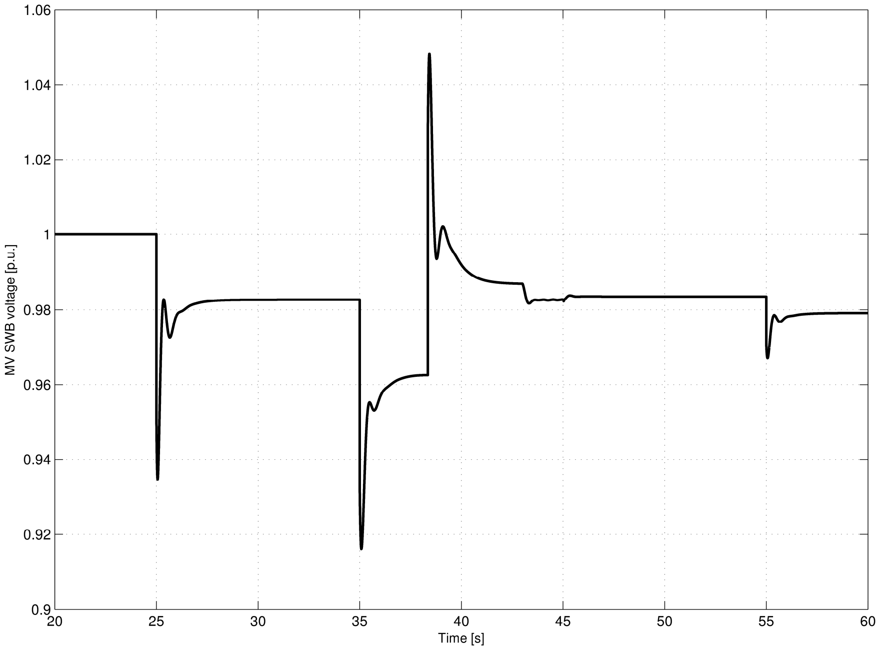


Figure 78 - Simulated DG fault and automatic recovery action, voltage on the MV switchboard

As can be seen from the simulation results, the proposed recovery action allows recovering the capability of supplying the full load foreseen by the electric loads balance in nearly 20 seconds after the fault event. Obtaining such a result has been simple using the software simulator, which allowed applying various recovery solutions to the IPS in order to select the best one. Moreover, the use of the simulator allowed lowering as much as possible the response times of the recovery action (although keeping a safety margin), limiting the time in which the IPS give a degraded service to the users.

The definition of both emergency and recovery actions is commonly done “on the paper” in conventional design. This practice not only is incapable of optimizing the response times, but also imply the possibility of verifying the correctness of the designed actions only on the real-system. This demonstrate the possible improvements in design achievable using a software simulator, which impact in terms of both computational and time resources is nowadays limited. In addition to that, it as to be highlighted the fact that the closed bus operation, used in this case study to recover correct service, require demonstration of equivalent integrity of power operation (3/1 from ABS Guide on DP Systems). Such a demonstration can be easily done through the application of both dependability analysis and software simulations, thus rendering the proposed design process useful also for this particular case.

6.4.4 Dependability evaluation of the proposed solutions

To conclude the demonstration of the proposed design process, a dependability analysis of the system with the proposed design solutions embedded has to be done. However, such a process imply the construction of a Failure Tree for each different possible solution, with the proper top-event, and the consequent comparison of the achieved dependability attributes. The main problem in this regard is due to the different top-events that may be considered while studying each possible solution. In fact, as frequently repeated above, both the FTA and its outcomes depend directly on the selected top-event. In this case, it is evident that no comparisons can be made through dependability.

To clarify the above affirmation, an example can be done: if the selected top-event is the avoidance of a black out in case of one DG loss (in the above-mentioned conditions), each proposed solution is valid. Moreover, a paradox can be highlighted: if such a top-event is selected, the solution implying the recovery of the correct service may have even worse dependability attributes than the simple load shedding action. This could happen because the application of the recovery solution implies the intervention of more components than simple load-shedding (controls, protections and tie-breakers) and a change in system structure (from open bus to closed bus). Due to that, even if the recovery appears clearly as the best solution to the designers, it may be worse from the point of view of system's fault behavior. Conversely, if the top-event selected for the analysis is the maintenance of the correct service, only the recovery action solution will present modified attributes in respect to the base design, because the other actions lead only to a degraded service condition. This remarks the need of clearly defining all the hypotheses to be used during the analysis, and never forgot them when evaluating both the system and the analyses outcomes.

In the case study, the top-event was the loss of the capability to keep the position using DP systems. As was clear at the end of the Section 6.4.2 of this Chapter, the fault imposed in the simulation does not affect such a top-event. This removes the need of building another Failure Tree, because no changes are to be expected from the proposed load shedding solution. However, the recovery solution changes the system configuration, thus leading to possible different dependability analysis outcomes for the system after the recovery action intervention. Such an analysis could be easily done using FTA, leading to a discussion similar to what has been done above. Since the purpose of this thesis is not to compare different design concepts, such analysis has not been done.

7 Conclusion

Nowadays, IPSs are becoming more and more complex, due to both the onboard installation of increasing rates of electronic power converters and the use of innovative subsystems never applied before on ships. In fact, such a trend is driven by different requirements: the ship owners want to achieve higher performance, or require the same performance at a reduced cost; while regulatory bodies are showing an increasingly interest in the system's behavior in case of faults. While this trend is still in its infancy in common merchant ship applications (as an example, cruise ships fully compliant with SRtP regulation are yet to be delivered), both naval and dynamic positioning vessels are pioneers in this direction.

Designing such complex systems is difficult, due to two main issues: the classic ship design process has been conceived when ships were simpler, thus it is becoming inadequate to address the design of modern complex ships; and the proposal of new distribution systems and components imply designing the IPS having no previous knowledge on which to base.

Due to that, the aim of this thesis was to present an innovative design process, applicable to the All Electric Ships' (AESs) Integrated Power System (IPS), able to address the issues given by both the conventional design process and the desire to install on board new subsystems and components.

To reach such a goal a wide review of the state of the art have been done, with the aim of allowing to understand the context, why the innovative process is needed, and which innovative techniques can be used as an aid in design. Each point have been discussed focusing on the aim of this thesis, thus presenting topics, bibliography, and personal evaluations tailored to direct the reader to comprehend the impact of the proposed design process.

The proposed design process makes extended use of innovative tools, able to aid the designers in decision-making activities related to the ship design process. In particular, to develop the innovative process have been applied the dependability theory concepts and techniques and the software simulation of the system's dynamic behavior. The former has proved to be able to give a systematic approach in assessing the impact of the single components' faults on the overall system. Indeed, dependability techniques allow pinpointing both the most critical components in system's dependability point of view, and subsystems/components on which it is possible to save money through a relaxation of either components' parameters or subsystem design. The Fault Tree Analysis has been chosen as the best-suited technique for this application, due to the possibility to achieve both qualitative and quantitative analysis. For what concerns the software simulation, it has been used to evaluate the dynamic transients that lead the system to the failure in the cases highlighted by the dependability analysis. This allowed proposing solutions tailored on the particular ship in course of design, and demonstrating the effectiveness of such solutions even before the construction of the system.

To demonstrate the applicability of the proposed design process, a case study has been presented: the IPS of a Dynamic Positioning Drilling Ship classified in class DPS-3 following ABS rules. Such a case study has been selected due to the stringent requirements DPS-3 vessels have, whose impact on system design is significant. A simplified study of the preliminary design of the ship in study has been done, to highlight how the proposed design process is supposed to be applied and the results it is able to give. The results of such a case study proved the possibility to apply the innovative process with a bearable effort by designers, and explained the possible improvements that are achievable through the application of the innovative design tools and the proposed design process.

Bibliography

[1] G. Sulligoi, "All electric ships: present and future after 20 years of research and technical achievements," *Electrical Engineering Research Report,* 2011.

[2] J. Hansen and F. Wendt, "History and State of the Art in Commercial Electric Ship Propulsion, Integrated Power Systems, and Future Trends," *Proceedings of the IEEE,* vol. 103, no. 12, pp. 2229-2242, Dec. 2015.

[3] 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 Electrification Magazine,* vol. 3, no. 2, pp. 49-65, june 2015.

[4] M. Cupelli, F. Ponci, G. Sulligoi, A. Vicenzutti, C. Edrington, T. El-mezyani and A. Monti, "Power Flow Control and Network Stability in an All-Electric Ship," *Proceedings of the IEEE,* vol. 103, no. 12, pp. 2355-2380, Dec. 2015.

[5] E. Skjong, E. Rodskar, M. Molinas, T. Johansen and J. Cunningham, "The Marine Vessel's Electrical Power System: From its Birth to Present Day," *Proceedings of the IEEE,* vol. 103, no. 2, pp. 2410-2424, Dec. 2015.

[6] R. Hepburn, "Why a naval architect likes an electric ship," in *Power Electronics, Electrical Drives, Automation and Motion, 2008. SPEEDAM 2008. International Symposium on*, Ischia, Italy, 11-13 June 2008.

[7] T. McCoy, "Integrated Power Systems—An Outline of Requirements and Functionalities for Ships," *Proceedings of the IEEE,* vol. 103, no. 12, pp. 2276-2284, Dec. 2015.

[8] International Maritime Organization, SOLAS Consolidated Edition, IMO, 2014.

[9] C. Craig and M. Islam, "Integrated Power System Design for Offshore Energy Vessels and Deepwater Drilling Rigs," *Industry Applications, IEEE Transactions on,* vol. 48, no. 4, pp. 1251-1257, July-Aug 2012.

[10] G. Lipardi, L. Piva, L. Piegari, E. Tironi, R. Lamedica, A. Ruvio, G. Sulligoi and A. Vicenzutti, "Electric loads characterization in an aircraft carrier with ring-bus distribution system," in *Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on*, Aachen, DE, March 2015.

[11] "IEEE Recommended Practice for Electric Installations on Shipboard," *IEEE Std 45-2002*, pp. 1-272, Oct. 9 2002.

[12] "Electrical installations in ships," *IEC 60092.*

[13] "Part 6: Control, Electrical, Refrigeration and Fire," *Lloyd's Register, Rules and Regulations for the Classification of Ships,* July 2015.

[14] T. Lauvdal, "Power Management System With Fast Acting Load Reduction For DP Vessels," in *Dynamic Positioning Conference*, 17-18 Oct. 2000.

[15] D. E. Wilkes, "Power Management and Blackout Prevention," in *Dynamic Positioning Conference*, 18-19 Sept. 2001.

[16] M. Al-Mulla and N. Seeley, "Distributed generation control in islanded industrial facilities: A case study in power management systems," in *PCIC Europe 2010 Conference Record*, San Antonio, TX, USA, 15-17 June 2010.

[17] K. Nicholson, R. Doughty, L. Mane, G. Miranda and F. Pulaski, "Cost effective strategies for industrial electric power management systems," in *Petroleum and Chemical Industry conference, 1998. Industry Applications Society 45th Annual*, 28-30 Sep 1998.

[18] D. E. Wilkes, "Dynamic Positioning Incidents Resulting From Inadequate Power Systems Analysis," in *Dynamic Positioning Conference*, 17-18 Sept. 2002.

[19] N. Doerry, J. Amy and C. Krolick, "History and the Status of Electric Ship Propulsion, Integrated Power Systems, and Future Trends in the U.S. Navy," *Proceedings of the IEEE,* vol. 103, no. 12, pp. 2243-2251, Dec. 2015.

[20] H. Shatto and D. Phillips, "Reliability and Risk Analysis - Failure Modes and Effects Analysis (FMEAs)," in *Dynamic Positioning Conference*, 21-22 Oct. 1997.

[21] R. B. Andersen and I. Haukaas, "Challenges of Protection and Control System Verification on DP3 vessels with Focus on Ride Through Fault and Blackout," in *Dynamic Positioning Conference*, 15-16 Oct. 2013.

[22] "Guide for Dynamic Positioning Systems," *American Bureau of Shipping,* November 2013 (Updated July 2014).

[23] "Rules for Classification of Ships - Part 6 Chapter 7 - Newbuilding - Special equipment and systems - Additional class: Dynamic Positioning Systems," *Det Norske Veritas,* July 2013.

[24] "MSC/Circ. 645 - Guidelines for Vessels with Dynamic Positioning Systems," *International Maritime Organization - IMO,* 6 June 1994.

[25] A. Kallah, "Electrical Power Plant and Thruster Systems Design Considerations for Dynamically Positioned Vessels," in *Dynamic Positioning Conference*, 21-22 Oct. 1997.

[26] "Rules for Building and Classing Mobile Offshore Drilling Units - Part 4 - Machinery and Systems," *American Bureau of Shipping,* 2015.

[27] T. Nordtun, "Machinery Systems for DP Vessels with Increased Efficiency and Reliability," in *Dynamic Positioning Conference*, 7-8 Oct. 2008.

[28] B. Cheater, P. Lammers and J. v. Keep, "Low Loss Concept Comparison Study," in *Dynamic Positioning Conference*, 12-13 Oct. 2010.

[29] International Group of Authorities (Editor: Thomas Lamb), Ship Design and Construction, The Society of Naval Architects and Marine Engineers, 2003.

[30] M. Baret, C. Ferrero, D. Giulivo, A. Vicenzutti, D. Bosich, G. Sulligoi, M. Giuliano and L. Piva, "Amerigo Vespucci: Retrofitting of propulsion and generation systems on the italian training's tall ship," in *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2014 International Symposium on*, Ischia, IT, 18-20 June 2014.

[31] M. Altosole, M. Figari, C. Ferrero, V. Giuffra and L. Piva, "Propulsion retrofitting of the tall ship Amerigo Vespucci: Automation design by simulation," in *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2014 International Symposium on*, Ischia, IT, 18-20 June 2014.

[32] V. Bucci, A. Marinò and I. Juricic, "Integrated ship design: Automated Generation of Production Deliverables with New Generation Shipbuilding CAD Systems," in *Conference on Computer Applications and Information Technology in the Maritime Industries*, Hamburg, DE, April 2013.

[33] J. Chalfant, "Early-Stage Design for Electric Ship," *Proceedings of the IEEE,* vol. 103, no. 12, pp. 2252-2266, Dec. 2015.

[34] J. Chalfant, M. Ferrante and C. Chryssostomidis, "Design of a notional ship for use in the development of early-stage design tools," in *Electric Ship Technologies Symposium (ESTS), 2015 IEEE,* Old Town Alexandria, VA, USA, 21-24 June 2015.

[35] C. C. P. Mandel, "A Design Methodology for Ships and other Complex Systems," *Philosophical Transactions of the Royal Society A,* vol. 273, no. 1231, pp. 85-98, 5 Sept. 1972.

[36] G. Buja, A. da Rin, R. Menis and G. Sulligoi, "Dependable design assessment of Integrated Power Systems for All Electric Ships," in *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS), 2010*, Bologna, IT, 19-21 Oct. 2010.

[37] J. Warwick, "Electrical Systems Analysis," in *Dynamic Positioning Conference*, 21-22 Oct. 1997.

[38] J. Prousalidis, P. Mouzakis, E. Sofras, D. Muthumuni and O. Nayak, "On studying the power supply quality problems due to thruster start-ups," in *Electric Ship Technologies Symposium, 2009. ESTS 2009. IEEE*, Baltimore, MD, USA, 20-22 April 2009.

[39] G. Sulligoi, A. Vicenzutti, M. Chiandone, D. Bosich and V. Arcidiacono, "Generators electromechanical stability in shipboard grids with symmetrical layout: Dynamic interactions between voltage and frequency controls," in *3-5 Oct. 2013*, Palermo, IT, AEIT Annual Conference, 2013.

[40] C. Rivetta, G. Williamson and A. Emadi, "Constant power loads and negative impedance instability in sea and undersea vehicles: statement of the problem and comprehensive large-signal solution," in *Electric Ship Technologies Symposium, 2005 IEEE*, 25-27 July 2005.

[41] A. Rahimi, G. Williamson and A. Emadi, "Loop-Cancellation Technique: A Novel Nonlinear Feedback to Overcome the Destabilizing Effect of Constant-Power Loads," *Vehicular Technology, IEEE Transactions on,* vol. 59, no. 2, pp. 650-661, Feb. 2010.

[42] G. Sulligoi, D. Bosich, G. Giadrossi, L. Zhu, M. Cupelli and A. Monti, "Multiconverter Medium Voltage DC Power Systems on Ships: Constant-Power Loads Instability Solution Using Linearization via State Feedback Control," *Smart Grid, IEEE Transactions on,* vol. 5, no. 5, pp. 2543-2552, Sept. 2014.

[43] A. Kwasinski and C. Onwuchekwa, "Dynamic Behavior and Stabilization of DC Microgrids With Instantaneous Constant-Power Loads," *Power Electronics, IEEE Transactions on,* vol. 26, no. 3, pp. 822-834, March 2011.

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

[45] K.-N. Areerak, S. Bozhko and G. Asher, "Stability analysis and modelling of AC-DC system with mixed load using DQ-transformation method," in *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on*, June 30 2008-July 2 2008.

[46] A. Emadi, "Modeling of power electronic loads in AC distribution systems using the generalized State-space averaging method," *Industrial Electronics, IEEE Transactions on,* vol. 52, no. 5, pp. 992-1000, Oct. 2004.

[47] P. Heskes, J. Myrzik and W. Kling, "Power electronic loads with negative differential impedance in a low voltage distribution system," in *Electricity Distribution - Part 1, 2009. CIRED 2009. 20th International Conference and Exhibition on*, 8-11 June 2009.

[48] B. Wen, D. Boroyevich, P. Mattavelli, Z. Shen and R. Burgos, "Experimental verification of the Generalized Nyquist stability criterion for balanced three-phase ac systems in the presence of constant power loads," in *Energy Conversion Congress and Exposition (ECCE), 2012 IEEE*, 15-20 Sept. 2012.

[49] R. Burgos, D. Boroyevich, F. Wang, K. Karimi and G. Francis, "On the Ac stability of high power factor three-phase rectifiers," in *Energy Conversion Congress and Exposition (ECCE), 2010 IEEE*, 12-16 Sept. 2010.

[50] G. Sulligoi, A. Vicenzutti, V. Arcidiacono and Y. Khersonsky, "Voltage Stability in Large Marine Integrated Electrical and Electronic Power Systems," in *Petroleum and Chemical Industry Technical Conference (PCIC), 2015 IEEE*, Houston, TX, USA, 5-7 Oct. 2015.

[51] D. F. Phillips, "Classic Single Point Failures of Redundant DP Systems," in *Dynamic Positioning Conference*, 13-14 Oct. 1998.

[52] S. Leeb, J. Kirtley, W. Wichakool, Z. Remscrim, C. Tidd, J. Goshorn, K. Thomas, R. Cox and R. Chaney, "How Much DC Power Is Necessary?," *Journal of the American Society of Naval Engineers,* vol. 122, no. 2, pp. 79-92, 2010.

[53] N. Doerry and J. Amy, "Functional decomposition of a medium voltage DC integrated power system," in *ASNE Shipbuilding in Support of the Global War on Terrorism Conference*, Biloxi, MS, USA, 14-17 April 2008.

[54] A. Vicenzutti, D. Bosich and G. Sulligoi, "MVDC power system voltage control through feedback linearization technique: Application to different shipboard power conversion architectures," in *Electric Ship Technologies Symposium (ESTS), 2013 IEEE*, Arlington, VA, USA, 22-24 April 2013.

[55] D. Bosich, "Medium Voltage DC integrated power systems for large all electric ships. [Ph.D. thesis]," 2014.

[56] T. Ericsen, "The ship power electronic revolution: Issues and answers," in *Petroleum and Chemical Industry Technical Conference, 2008. PCIC 2008. 55th IEEE*, Cincinnati, OH, USA, 22-24 Sept. 2008.

[57] "IEEE Standard for Power Electronics Open System Interfaces in Zonal Electrical Distribution Systems Rated Above 100 kW," *IEEE Std 1826-2012,* June 2012.

[58] J. Momoh and L. Mili, Operation and Control of Electric Energy Processing Systems, IEEE Press Series on Power Engineering, Wiley, 2010.

[59] G. Sulligoi, A. Vicenzutti, E. Tironi, M. Corti, R. Lamedica, A. Ruvio, G. Lipardi and L. Piva, "Naval smart grid: Integrated Power System for all electric naval vessels with control and reliability characteristics," in *AEIT Annual Conference - From Research to Industry: The Need for a More Effective Technology Transfer (AEIT), 2014*, Trieste, IT, 18-19 Sept. 2014.

[60] "Clad in Controversy," *IEEE Spectrum,* vol. 8, 2013.

[61] D. Witt, D. Helfers and Y. Young, "Comparative Study of Power Generation and Energy Storage Modules for Support of High Energy Weapons," *Naval Engineers Journal,* vol. 124, no. 2, pp. 74-77, 2012.

[62] Y. Khersonsky, M. Islam and K. Peterson, "Challenges of Connecting Shipboard Marine Systems to Medium Voltage Shoreside Electrical Power," *Industry Applications, IEEE Transactions on,* vol. 43, no. 3, pp. 838-844, May-june 2007.

[63] K. Peterson, P. Chavdarian, M. Islam and C. Cayanan, "Tackling ship pollution from the shore," *Industry Applications Magazine, IEEE,* vol. 15, no. 1, pp. 56-60, Jan.-Feb. 2009.

[64] G. Sulligoi, D. Bosich, R. Pelaschiar, G. Lipardi and F. Tosato, "Shore-to-Ship Power," *Proceedings of the IEEE,* vol. 103, no. 12, pp. 2381-2400, Dec. 2015.

[65] "IEC/ISO/IEEE Utility Connections in Port--Part 1: High Voltage Shore Connection (HVSC) Systems--General requirements," *IEC/ISO/IEEE 80005-1:2012,* July 2012.

[66] A. Vicenzutti, F. Tosato, G. Sulligoi, G. Lipardi and L. Piva, "High voltage ship-to-shore connection for electric power supply support in landing operations: An analysis," in *Electric Ship Technologies Symposium (ESTS), 2015 IEEE*, Old Town Alexandria, VA, USA, 21-24 June 2015.

[67] "Short-circuit currents in d.c. auxiliary installations in power plants and substations - Part 1: Calculation of short-circuit currents," *IEC 61660-1:1997,* 1997.

[68] A. Vicenzutti, E. De Din and G. Sulligoi, "Transient short circuit analysis in DC on-board distribution systems fed by synchronous generators through 6-pulse diode rectifiers," in *Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on*, Aachen, DE, 3-5 March 2015.

[69] A. Vicenzutti, F. Tosato, E. De Din and G. Sulligoi, "Studies on asymmetrical short circuit currents in shipboard medium voltage direct current distribution systems fed by AC generators," in *Electric Ship Technologies Symposium (ESTS), 2015 IEEE*, Old Town Alexandria, VA, USA, 21-24 June 2015.

[70] J. L. Ramseur, "Deepwater Horizon Oil Spill: Recent Activities and Ongoing Developments," Congressional Research Service, April 17, 2015.

[71] V. Nelson, "Fault-tolerant computing fundamental concepts," *Computer,* vol. 23, no. 7, pp. 19-25, June 1990.

[72] N. Leveson, Safeware - System Safety and Computers, Addison-Wesley, 1995.

[73] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *Dependable and Secure Computing, IEEE Transactions on,* vol. 1, no. 1, pp. 11-33, Jan.-March 2004.

[74] M. Al-Kuwaiti, N. Kyriakopoulos and S. Hussein, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability," *Communications Surveys & Tutorials, IEEE,* vol. 11, no. 2, pp. 106-124, Second Quarter 2009.

[75] E. O. S. Hansen, "DP Dependability," in *Dynamic Positioning Conference*, 11-12 Oct. 2011.

[76] "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems," *IEEE Std 493-2007,* June 2007.

[77] A. Chowdhury and D. Koval, Power Distribution Systems Reliability – practical methods and applications, IEEE Press Series on Power Engineering - Wiley, 2009.

[78] 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 *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS), 2012*, Bologna, IT, 16-18 Oct. 2012.

[79] R. Eriksen, J. Harms and R. McDonnell, "Assessing the reliability of DP systems for deepwater drilling vessels," in *Dynamic Positioning Conference*, 12-13 Oct. 1999.

[80] "Guidance on Failure Modes & Effects Analyses (FMEAs)," IMCA - The International Marine Contractors Association, April 2002.

[81] M. D. Quilici, "DP System Reliability - Quantitative vs. Qualitative Analysis," in *Dynamic Positioning Conference*, 12-13 Oct. 1999.

[82] W. Lee, D. Grosh, F. Tillman and C. Lie, "Fault Tree Analysis, Methods, and Applications - A Review," *Reliability, IEEE Transactions on,* Vols. R-34, no. 3, pp. 194-203, Aug. 1985.

[83] Y.-Y. Hong, L.-H. Lee and H.-H. Cheng, "Reliability Assessment of Protection System for Switchyard Using Fault-Tree Analysis," in *Power System Technology, 2006. PowerCon 2006. International Conference on*, 22-26 Oct. 2006.

[84] U.S. Nuclear Regulatory Commission, "NUREG-0492 - Fault Tree Handbook".

[85] SAE, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," *Std. ARP4761.*

[86] U.S.A. Department of Defense, "Electronic Reliability Design Handbook," *Military Handbook MIL-HDBK-338B.*

[87] "Fault Tree Analysis (FTA)," *IEC 61025,* 2006-12.

[88] R. Menis, A. da Rin, A. Vicenzutti and G. Sulligoi, "All electric ship dependable design: integrated power system analysis using dynamic reliability block diagram," in *IMaeEST Marine Electrical and Control Systems Safety Conference (MECSS)*, Amsterdam, NL, 9 Oct. 2013.

[89] F. Crawley and B. Tyler, HAZOP: Guide to best practice - Guidelines to best practice for the process and chemical industries, Elsevier, 2015.

[90] "Hazard and operability studies (HAZOP studies) - Application guide," *IEC 61882:2001,* 2001.

[91] A. Munn, "Common Problems and Recent Trends with HAZOPs," in *IChemE Symposium Series n° 155*, 2009.

[92] A. da Rin, "Integrated Power Systems in All Electric Ships: Dependability Oriented Design. [Ph.D. thesis]," 2014.

[93] A. Mokashi, J. Wang and A. Vermar, "A study of reliability-centered maintenance in maritime operations," *Elsevier - Marine Policy,* 2002.

[94] C. M. Milkie and A. N. Perakis, "Statistical Methods for Planning Diesel Engine Overhauls in the U. S. Coast Guard," *Naval Engineers Journal,* vol. 116, no. 2, pp. 31-42, 2004.

[95] C. Dong, C. Yuan, Z. Liu and X. Yan, "Marine Propulsion System Reliability Research Based on Fault Tree Analysis," *Advanced Shipping and Ocean Engineering,* vol. 2, no. 1, pp. 27-33, March 2013.

[96] R. Cornes and T. R. Stockton, "FMEA as an Integral Part of Vessel Design and Construction: Producing a Fault Tolerant DP Vessel," in *Dynamic Positionong Conference,* 13-14 OCt. 1998.

[97] R. Menis, A. da Rin, G. Sulligoi and A. Vicenzutti, "All electric ships dependable design: Implications on project management," in *AEIT Annual Conference - From Research to Industry: The Need for a More Effective Technology Transfer (AEIT), 2014*, Trieste, IT, 18-19 Sept. 2014.

[98] M. Chiandone, A. da Rin, R. Menis, G. Sulligoi and A. Vicenzutti, "Dependable oriented design of complex integrated power systems on ships," in *Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on*, Aachen, DE, 3-5 March 2015.

[99] "Mobile and fixed offshore units - Electrical installations - Part 5: Mobile units," *IEC 61892-5.*

[100] G. Sulligoi, D. Bosich, T. Mazzuca and L. Piva, "The FREMM simulator: A new software tool to study electro-mechanic dynamics of the shipboard integrated power system," in *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS), 2012*, Bologna, IT, 16-18 Oct. 2012.

[101] T. A. Johansen and A. J. Sørensen, "Experiences with HIL Simulator Testing of Power Management Systems," in *Dynamic Positioning Conference*, 13-14 Oct. 2009.

[102] 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 *Electric Ship Technologies Symposium (ESTS), 2013 IEEE*, Arlington, VA, USA, 22-24 April 2013.

[103] D. Bosich, M. Filippo, D. Giulivo, G. Sulligoi and A. Tessarolo, "Thruster motor start-up transient in an all-electric cruise-liner: Numerical simulation and experimental assessment," in *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS), 2012,* Bologna, IT, 16-18 Oct. 2012.

[104] T. Lauvdal, "Optimizing and Evaluating the Performance of Power and Thruster Plant in DP Vessels with an Integrated Vessel Simulator," in *Dynamic Positioning Conference,* 17-18 Oct. 2000.

[105] J. Langston, M. Sloderbeck, M. Steurer, D. Dalessandro and T. Fikse, "Role of hardware-in-the-loop simulation testing in transitioning new technology to the ship," in *Electric Ship Technologies Symposium (ESTS), 2013 IEEE*, Arlington, VA, USA, 22-24 April 2013.

[106] M. Cupelli, M. de Paz Carro and A. Monti, "Hardware in the loop implementation of linearizing state feedback on MVDC ship systems and the significance of longitudinal parameters," in *Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on*, Aachen, DE, 3-5 March 2015.

[107] M. Cupelli, M. de Paz Carro and A. Monti, "Hardware in the Loop implementation of a disturbance based control in MVDC grids," in *Power & Energy Society General Meeting, 2015 IEEE*, 26-30 July 2015.

[108] M. Andrus, M. Steurer, C. Edrington, F. Bogdan, H. Ginn, R. Dougal, E. Santi and A. Monti, "Real-time simulation-based design of a power-hardware-in-the-loop setup to support studies of shipboard MVDC issues," in *Electric Ship Technologies Symposium, 2009. ESTS 2009. IEEE*, 20-22 April 2009.

[109] R. Marconato, Electric Power Systems, Milan: CEI - Italian Electrotechnical Committee, 2002.

[110] K. Marouani, H. Guendouz, B. Tabbache, F. Khoucha and A. Kheloui, "Experimental investigation of an emulator "Hardware In the Loop" for electric naval propulsion system," in *Control & Automation (MED), 2013 21st Mediterranean Conference on*, 25-28 June 2013.

[111] M. van der Borst and H. Schoonakker, "An overview of PSA importance measures," *Elsevier Reliability Engineering & System Safety*, vol. 72, pp. 241-245, 2001.

[112] The Maersk group, "Maersk Energy," [Online]. Available: http://www.maersk.com/en/industries/energy. [Accessed 06 01 2016].

[113] Center for Catastrophic Risk Management (CCRM), University of California - Berkeley, "Final Report on the Investigation of the Macondo Well Blowout," Deepwater Horizon Study Group, March 1, 2011.

Papers

[3] 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 Electrification Magazine,* vol. 3, no. 2, pp. 49-65, june 2015.

[5] M. Cupelli, F. Ponci, G. Sulligoi, A. Vicenzutti, C. Edrington, T. El-mezyani and A. Monti, "Power Flow Control and Network Stability in an All-Electric Ship," Proceedings of the IEEE, vol. 103, no. 12, pp. 2355-2380, Dec. 2015.

[10] G. Lipardi, L. Piva, L. Piegari, E. Tironi, R. Lamedica, A. Ruvio, G. Sulligoi and A. Vicenzutti, "Electric loads characterization in an aircraft carrier with ring-bus distribution system," in Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on, Aachen, DE, March 2015.

[30] M. Baret, C. Ferrero, D. Giulivo, A. Vicenzutti, D. Bosich, G. Sulligoi, M. Giuliano and L. Piva, "Amerigo Vespucci: Retrofitting of propulsion and generation systems on the italian training's tall ship," in Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2014 International Symposium on, Ischia, IT, 18-20 June 2014.

[39] G. Sulligoi, A. Vicenzutti, M. Chiandone, D. Bosich and V. Arcidiacono, "Generators electromechanical stability in shipboard grids with symmetrical layout: Dynamic interactions between voltage and frequency controls," in 3-5 Oct. 2013, Palermo, IT, AEIT Annual Conference, 2013.

[50] G. Sulligoi, A. Vicenzutti, V. Arcidiacono and Y. Khersonsky, "Voltage Stability in Large Marine Integrated Electrical and Electronic Power Systems," in Petroleum and Chemical Industry Technical Conference (PCIC), 2015 IEEE, Houston, TX, USA, 5-7 Oct. 2015.

[54] A. Vicenzutti, D. Bosich and G. Sulligoi, "MVDC power system voltage control through feedback linearization technique: Application to different shipboard power conversion architectures," in Electric Ship Technologies Symposium (ESTS), 2013 IEEE, Arlington, VA, USA, 22-24 April 2013.

[59] G. Sulligoi, A. Vicenzutti, E. Tironi, M. Corti, R. Lamedica, A. Ruvio, G. Lipardi and L. Piva, "Naval smart grid: Integrated Power System for all electric naval vessels with control and reliability characteristics," in AEIT Annual Conference - From Research to Industry: The Need for a More Effective Technology Transfer (AEIT), 2014, Trieste, IT, 18-19 Sept. 2014.

[66] A. Vicenzutti, F. Tosato, G. Sulligoi, G. Lipardi and L. Piva, "High voltage ship-to-shore connection for electric power supply support in landing operations: An analysis," in Electric Ship Technologies Symposium (ESTS), 2015 IEEE, Old Town Alexandria, VA, USA, 21-24 June 2015.

[68] A. Vicenzutti, E. De Din and G. Sulligoi, "Transient short circuit analysis in DC on-board distribution systems fed by synchronous generators through 6-pulse diode rectifiers," in Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on, Aachen, DE, 3-5 March 2015.

[69] A. Vicenzutti, F. Tosato, E. De Din and G. Sulligoi, "Studies on asymmetrical short circuit currents in shipboard medium voltage direct current distribution systems fed by AC generators," in Electric Ship Technologies Symposium (ESTS), 2015 IEEE, Old Town Alexandria, VA, USA, 21-24 June 2015.

[78] 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 Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS), 2012, Bologna, IT, 16-18 Oct. 2012.

[88] R. Menis, A. da Rin, A. Vicenzutti and G. Sulligoi, "All electric ship dependable design: integrated power system analysis using dynamic reliability block diagram," in IMaeEST Marine Electrical and Control Systems Safety Conference (MECSS), Amsterdam, NL, 9 Oct. 2013.

[97] R. Menis, A. da Rin, G. Sulligoi and A. Vicenzutti, "All electric ships dependable design: Implications on project management," in AEIT Annual Conference - From Research to Industry: The Need for a More Effective Technology Transfer (AEIT), 2014, Trieste, IT, 18-19 Sept. 2014.

[98] M. Chiandone, A. da Rin, R. Menis, G. Sulligoi and A. Vicenzutti, "Dependable oriented design of complex integrated power systems on ships," in Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles (ESARS), 2015 International Conference on, Aachen, DE, 3-5 March 2015.

[102] 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 Electric Ship Technologies Symposium (ESTS), 2013 IEEE, Arlington, VA, USA, 22-24 April 2013.