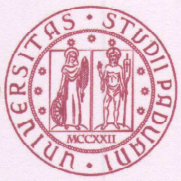

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova
Sede Consorziata: Università degli Studi di Trieste

Dipartimento di Ingegneria Industriale

SCUOLA DI DOTTORATO DI RICERCA IN: INGEGNERIA INDUSTRIALE
INDIRIZZO: INGEGNERIA ELETTROTECNICA
CICLO: XXV

INTEGRATED POWER SYSTEMS IN ALL ELECTRIC SHIPS: DEPENDABILITY ORIENTED DESIGN

Direttore della Scuola: Ch.mo Prof. Paolo Colombo

Coordinatore d'indirizzo: Ch.mo Prof. Giovanni Martinelli

Tutor: Ch.mo Prof. Giorgio Sulligoi

Co-tutor: Ch.mo Prof. Fabio Tosato

Co-tutor: Ch.mo Prof. Roberto Menis

Dottorando: Aldo da Rin

31 luglio 2014

Abstract.

English.

This work aims at providing a comprehensive and, as far as possible, standard and widely supported approach to a dependable design of all electric ship integrated power systems. The proposed approach is based upon latest development of dependability theory made recently available, from its founding lexicon and taxonomy to investigation tools and relevant international rules.

In its first part, this work analyses present rule requirements governing the discipline of designing an integrated power system serving an all electric ship. Analysis covers system definitions (what is what) in terms of taxonomy and associated concepts; system required performances both in terms of delivered services and in terms of reaction to anticipated reactions to predetermined fault scenarios.

In its second part, this work briefly presents latest developments in the theory and in the tools theory brings along: lexicon, taxonomy, system analysis, benchmarking and enforcing techniques. During this development, emphasis is posed on the fact that design documentation, be it owners' technical specification, classification society rule book or international standard, often recall dependability concepts, without fully exploiting the potential theory is promising, or the completeness of its definition corpus.

In its third part, this work applies dependability concepts to a real case scenario, an integrated power system installed on a recent cruise ship vessel. This application, albeit suffering from an important lack of information, due to copyrighting and industrial intellectual property rights, produces an informative example on the enquiring method and relevant deliverable: a system model, obtained in a strongly standardized way that permits a comprehensive and accurate dependability study, to be realized using tools and techniques defined in international standard. Results of this analysis are, as a consequence of method strong structure, repeatable and consistent, and allow quick verification of requirements. Analysis results, even though partial and superficial owing to already mentioned lack of accurate information, are offering some original view points. They are commented and classified according to indexes defined earlier.

In its fourth part, this works presents proposals to be applied to systems which exhibited low values of indexes. Such proposals are briefly analyzed in terms of index value variations; in doing this a quantification of improvement that could be obtained is given.

Finally, in its fifth part, this work shortly presents future research directions to improve investigation method.

This work reports elements of project management and maritime law as well, this in force of the multidisciplinary nature of dependability theory, and its repercussion on different sector of the marine industry, besides engineering. It is show how present method can fit the actual engineering process, and can provide a common language serving as substrate for various disciplines, like the ones mentioned.

Italiano.

Questo lavoro si prefigge lo scopo di definire in maniera quanto piu' possibile standardizzata e definita nel corpus delle regole internazionali la disciplina della progettazione volta alla fidatezza di impianti integrati di produzione, distribuzione ed utilizzo dell'energia elettrical a bordo di navi a propulsione elettrica. L'approccio proposto si fonda nei piu' recenti sviluppi della teoria della fidatezza, che coinvolgono il lessico, la tassonomia, fino agli strumenti di analisi e di quantificazione degli attributi. Tali sviluppi sono al vaglio della comunita' internazionale, ma gia' un importante consenso e' stato raggiunto.

La prima parte contiene un'analisi dettagliata dello stato normativo attualmente in vigore che disciplina la progettazione di un impianto elettrico integrato. I documenti normativi analizzati sono principalmente: la specifica tecnica armatoriale, i regolamenti delle societa' di classifica ed il corpus di regole degli enti internazionali. L'analisi si concentra sulla definizione dei sistemi, sia dal punto di vista tassonomico, funzionale e di requisiti in termini di reazione ad un predefinito insieme di condizioni di guasto.

La seconda parte riporta un breve sunto della teoria della fidatezza, nella sua piu' recente definizione. Si fa accenno al lessico, definito in maniera stringente, alla tassonomia ed alle tecniche di analisi e di sintesi della fidatezza. In questo contesto si attira l'attenzione sul fatto che i documenti analizzati nella parte precedente fanno sovente riferimento agli elementi della teoria della fidatezza, senza pero' considerarne appieno il significato e le ricadute che la teoria offre. La teoria funge da substrato che integra la documentazione, altrimenti frammentaria e priva della necessaria precisione, in un unico insieme autocontenuto.

La terza parte riporta un'applicazione dei concetti analizzati nella prima parte, rielaborati alla luce di quanto discusso nella seconda, ad un caso pratico: un impianto elettrico integrato di una nave da crociera di recente costruzione. L'applicazione, pur soffrendo di una importante mancanza d'informazioni, dovuta a vincoli di copyright e di protezione del know how aziendale, ha evidenziato la struttura del metodo e la sua esaustivita'. Il risultato dell'applicazione e' un modello che permette lo studio preventivo della fidatezza del sistema in fase di progettazione e il rapido controllo del rispetto dei limiti imposti in termini di reazione ai guasti previsti dalle norme. Nonostante i vincoli posti, il modello ed il relativo sistema di indagine hanno offerto spunti interessanti ed innovativi rispetto a componenti il cui comportamento in caso di guasto era stato erroneamente trascurato.

La quarta parte riprende i risultati ottenuti nella terza, ed offre implemetazioni alternative volte ad ottenere una maggiore fidatezza. Il raggiungimento di una maggiore fidatezza e' vincolato al calcolo del relativo indice pertinente alla nuova proposta. In tal guisa il metodo offre la possibilita' di comparare diverse archietture e di classificarle secondo un criterio univoco, ossia il valore dell'indice di fidatezza scelto.

La quinta parte, infine, offre spunti per indirizzare la ricerca futura. L'analisi dei sistemi e dei loro requisiti ha reso evidente la necessita' di muoversi su diversi fronti: dalla definizione sempre piu' stringente ed esaustiva dei termini, inseriti nel loro contesto, allo sviluppo di nuovi componenti atti a svolgere un servizio piu' completo, per quanto riguarda certi aspetti della loro fidatezza (rilevabilita').

Il lavoro riporta alcuni elementi di gestione dei progetti e di legislazione marittima che sono parte intergrante dell'ambiente in cui il progetto dei sistemi elettrici integrati si sviluppa. Cio' e' dovuto al fatto che la fidatezza e' un insieme di attributi e qualita' che travalica la pura ingegneria, ma sconfina nel campo della legislazione, dell'assicurazione dei rischi e financo nella gestione dei progretti. Si crede che il contesto creato dall'analisi di fidatezza possa costituire un comune sostrato per l'interazione di molteplici discipline, quali appunto la gestione di progetti, la legislazione e la gestione del rischio, tendente a favorire il dialogo e la reciproca comprensione.

Table of Contents

0. Forewords.

0.1 Classification Rules and Regulations.

In this work reference is made principally to *DNV-GL*, one of the main classification societies operating nowadays in the world of shipbuilding. Reason for this is threefold:

- Their collection of rules and requirements is freely available on the internet, without access restriction.
- They belong to *IACS*. This association gathers all main classification societies as *ABS*, *LRS* and *RINa*, to produce a set of harmonised requirements for the industry, applicable worldwide. Citing one *IACS* member rules is equivalent to citing all other.
- They include statutory interpretation of main marine international regulatory bodies, such as *SOLAS*, *MARPOL*, *ILO*, *IMO*, etc.

Only international rules relevant to system design are considered in this work, because they are functional to its purpose: promoting techniques to produce a design that embeds proven dependability, in addition to merely fulfilling technical specification in absence of disturbances. Local rules, produced by some port state authorities, have been ignored due to their limited application scope.

0.2 Owners Specification.

When references are made to such a document, no explicit citing is possible, as those documents are not available to public. Author refers to his personal experience with Carnival group of brands, which includes Carnival Criuse Line, Holland America Line, Costa Crociere, Princess Cruises, P&O Cruise Line, Cunard Lines, Seabourn Cruise Lines, Aida Cruises, etc., and several offshore operators, such as McDermott International, ENI, Jasper Offshore, SBM, Sealink, to name but a few.

0.3 List of Abbreviations.

Acronyms used in this work are hereunder listed, according to their order of appearance.

DNV-GL: Det Norske Veritas and Germaischer Lloyd.

IACS: or International Association of Classification Societies.

ABS: American Bureau of Shipping.

LRS: Lloyd's Register of Shipping.

RINa: Registro Italiano Navale.

SOLAS: International Convention on Safety of Human Life at Sea.

MARPOL: International Convention for the Prevention of Pollution from Ships.

ILO: International Labour Organization.

IMO: International Maritime Organization.

AC: Alternated Current.

EEMUA: Engineering Equipment and Materials Users' Association.

IPS: Integrated Power System.

PC: Process Computer.

PLC: Programmable Logic Controller.

AES: All Electric Ship.

UN: United Nations.

IEC: International Electrotechnical Commission.

PSV: Platform Supply Vessel.

DP: Dynamic Positioning.

HVSC: High Voltage Shore Connection.

LVSC: Low Voltage Shore Connection.

THD: Total Harmonic Distortion.

SCADA: Supervisory Control and Data Acquisition.

RTU: Remote Terminal Unit.

RIO: Remote Input Output Unit.

HMI: Human Machine Interface.

ECR: Engine Control Room.

OPC: Object Linking and Embedding for Process Control Foundation.

PID: Proportional, Integral and Derivative Control.

AVR: Automatic Voltage Regulator.

IAS: Integrated Automation System.

IAMCS: Integrated Automation, Monitoring and Control System.

ISA: International Society of Automation.

CPU: Central Processing Unit.

UPS: Uninterruptible Power Supply.

BCP: Battery Charger Panel.

R0: Redundancy without service interruption.

DGPS: Differential Global Positioning System.

I/O: Input/Output.

P&I Club: Protection and Indemnity Insurance Club. A P&I club is a mutual insurance association that provides cover for its members, who will typically be ship-owners, ship-operators or demise charterers.

PLSV: Pipe Lay Support Vessel.

MTTF: Mean Time to Failure.

MTTR: Mean Time to Repair.

FAT: Factory Acceptance Tests (or Trials).

HAT: Harbour Acceptance Tests (or Trials).

SAT: Sea Acceptance Tests (or Trials).

FMEA: Failure Mode and Effects Analysis.

FTA: Fault Tree Analysis.

DFTA: Dynamic Fault Tree Analysis.

RBD: Reliability Block Diagram.

DRBD: Dynamic Reliability Block Diagram.

ISO: International Standard Organisation.

ANSI: American National Standards Institute.

IEEE: Institute of Electrical and Electronic Engineers.

FMECA: Failure Mode, Effects, and Criticality Analysis.

RPN: Risk Priority Number.

BS: British Standards.

MSC: Maritime Safety Convention.

QoS: Quality of Service.

MTBF: Mean Time Between Failures. A conceptual extension of *MTTF* applied to repairable systems.

MTTD: Mean Time To Degradation.

GRT: Gross Registered Tonn.

SRtP: Safe Return to Port.

WBS: Work Breakdown Structure.

AFD: Arc Flash Detection.

DPDT: Double Pole, Double Thread.

DPCO: Double Pole Change Over.

1oo2: One out of Two.

2oo3: Two out of Three.

0.4 Use of Hyperlinks

Hyperlinks are widely used in this text, to highlight the importance of a stringent vocabulary. Accurate definitions produce accurate dependability studies, being these reliant on definitions.

1. Introduction.

1.1 Historical Outlines.

Ship borne power plants have undergone a substantial evolution in past years, with the appearance of electric propulsion and process automation. Before these solutions became a standard, production of electricity had been regarded as a bare ancillary system, devoted to serving accommodation loads, mainly lighting, cooking appliances and navigation aids. Most of engine room auxiliary was mechanically driven; air, steam or oil pressure actuation was standard. Pipe work was omnipresent, and so were leaks in need of being eliminated and filters in need of cleaning or replacing. Automatic control, where present, was realised by means of complex and sensitive mechanical equipment, unable to grant action repeatability, fast dynamic, high accuracy and long run without overhauling.

Electrification rendered ship design more flexible and open: new opportunities were explored and exploited. Many services, nowadays thought as normal in a ship, no matter the trade (refrigeration, just to mention one striking example), less than one century ago were simply not existent. This implied new trade possibilities, such as transportation of perishable goods, and additional comforts to existing ones, making them more attractive. Leaking pipe work was replaced by electrical cables, and complex mechanical control by electrical controls, lighter, faster, maintenance free (or almost) and more accurate. Automatic or remote control was applied to systems never automated before, such as temperature control, just to mention one.

Ship electrification and automation road map can be summarised[1] in some few milestones:

1878: first small electrical generators were installed on board a ship supplying lighting and some other small users. Regina Margherita, 1881, was the first italian ship with an electricity distribution plant

1901: E. A. Sperry filed his patent for the gyrocompass, a device that can be regarded as a main step forward to electricity used in navigational aids. At the end of II Word War wheelhouses had several electrical devices helping crew finding their way: radars, gyrocompasses, electrically controlled steering systems, and so forth.

1903: the first diesel electric ship was put in service (a Russian river tanker named: “Vandal”). An Italian electrical engineer, Cesidio del Proposto, patented a mixed mechanical/electrical propulsion system. This system provided reversing capabilities, by means of electrical machinery, to diesel engines [**1**].

1905: the first electrical ventilation system was installed on board

1915: battleships were equipped with turbo electric propulsion plant (USS New Mexico class)

1920: the first diesel electric ice breaker, the Sisu, was commissioned. Electric propulsion was chosen for the application owing to its high torque delivery at low rpm [**1**].

1929: m/v Viceroy of India was the first liner, belonging to P&O Cruises, equipped with a turbo-electric propulsion plant.

1931: m/v Victoria (launched in Trieste for Lloyd Triestino) was the first ship equipped with an electrically actuated air conditioning plant. The transatlantic Rex had a similar, but more powerful, system installed the following year.

1 Acknowledgments for these pieces of precious information must be given to Maurizio Eliseo, eminent marine historian and good friend.

1952: the Andrea Doria, first cruise ship equipped with *AC* power generation, started his service. This vessel was built by Ansaldo at Sestri shipyard.

1962: the Japanese cargo Kinkasan Maru started its trading service. This vessel is most likely the first with remote propulsion and ancillary commands installed. Contemporary to it, the NS Savannah, a nuclear powered cargo-passenger ship, mounted a similar system.

1980 - 1990: first *AC* drives were installed on ships. First ship automation systems were commissioned. Those systems covered engine room and marine appliances (thrusters, winches, steering gears, etc.) and had following basic functions:

- Monitoring
- Control
- Alarm/Event management according to *EEMUA* 191 directive.

1986: the Queen Elizabeth 2 was converted to diesel-electric. *AC* drives were used. This vessel can be considered to have the first *IPS*, with the introduction of the so called "Power Station Concept" [**1**].

1990: first podded cruise ship was launched. Pod mounted propulsion units are an ideal compliment to electric propulsion.

2000: first integrated automation system[2] proposed. Such system included engine room and marine systems, HVAC, and refrigeration management in one single infrastructure.

In about one century engine room layout completely changed: electricity became the preferred way of controlling and distributing power on board all kind of ships; automation and process control removed necessity for personnel to attend machinery locally, with tangible benefits in terms of health and safety, not to mention costs.

Nowadays commitment to electricity and process control is complete and pervasive: hydraulics have been gradually replaced and relegated to serving marginal subsystems, for which they are still convenient: side doors, hatches, watertight doors and very few others. Attempts are in progress to replace these systems too with electric counterparts, but yet not fully exploited. In any case, control of such system is quintessentially electrical, in nature[3].

Controls have followed strictly electrification, as one of the major advantage offered. Digital microprocessor based (*PC* or *PLC*) control and monitoring systems are widely diffused onboard ships of any trade; monitoring and alarm systems are part of regulatory bodies requests for certification.

Safety provisions rely almost completely on electrical power and digital control. Complex fire strategies are implemented, to control fire and give crew chances to evacuate passengers effectively; lighting is arranged

[2] From now on the generic term automation refers to the following functions: alarm management, monitoring, and automatic or remote control. Integration refers to the practice of conveying control of different systems, such as HVAC and engine room auxiliary into a common platform. Integration furthermore covers control systems that are stand alone, but have similar service that automation, albeit with reduced function (absent proprietary alarm management, for example).

[3] At present, electrically operated watertight doors have been used in several cruise ship projects already, like Costa Luminosa, for instance. Watertight doors used to be one of the systems that most effectively resisted electrification, owing to the fact that it must be operated when submerged and under a complete power loss. This tells how commitment to electrical power is strong among ship designers and owners

so that it is available in an occurrence of fire, fire detection makes use of network technologies to transmit alarm and integrated optoelectronic circuitry for fire detection, and so forth.

1.2 The "All Electric Ship" Concept.

Historically electrification on ship began outside the engine room, in the so called "accommodations", or living quarters, as illustrated in *1.1*. Lighting, cooking appliances (electric appliances were suitable for marine use, given the fact that there were no free flames employed, as well as no fuels stored), refrigeration and air conditioning were the first systems affected by the use of electrical power.

It has continued from there replacing at first mechanical (pneumatic and hydraulic) as actuating power for small control appliances, to the point of becoming the preferred power form for propulsion and steering, once considered as quintessential mechanical systems of a ship. At the same time, ship electrification has enabled a remarkable transfer of technology; many "land based" appliances has become "marine", increasing options in trading (from bananas to chemical tankers, carrying any sort of chemicals, just to mention as example).

Presently, nearly all system are electrically powered, monitored, actuated and controlled. From this fact derives the name *AES*. Needles to say, *IPS* is the founding block of an *AES*.

IPS concept, introduced in coincidence with the consolidation of electric propulsion as replacement for traditional propulsion, represents the final point in exploiting electrical architecture potential. Its introduction took place impacting the entire marine community, in different forms, no matter the sector: warships [**2**], trading vessels and cruiser embraced this new philosophy without distinction. In its most common meaning, *IPS* is the integration of electrical power supply, power distribution, power conversion, power management and propulsion functions into one single entity, from a design, procurement and support standpoint. Integration derives from the fact that auxiliary and propulsion now have common power source, instead of dedicated, as common in the past. It its more modern meaning, *IPS* concept includes the integration of controls into the previously defined set, to reclaim all possible synergic benefits. This widened meaning is inspiring this work. In fact automation and controls are an integral part in power generation and delivery process and more and more often key to optimal performances: they counteract *IPS* increased complexity, adding more accuracy and faster action.

Advantages of electrification are well known, and can be summarised as follows:

- Reduced number of prime mover and better exploitation. The necessity of propulsion and electrical power supply prime movers stands no longer, as the electrical power can be easily dispatched to either one or both functions, in different and controllable proportions.
- Freedom of positioning prime movers to achieve best ship's weight and space balance.
- Better noise and vibration performances.
- Freedom of using different kind of prime movers, such as gas or steam turbines, medium speed diesel engines, etc.
- Possibility to receive power from shore.
- Flexibility in dispatching power to essential/mission critical services.
- Ease of control.
- Hardware standardisation.

These advantages largely overcome disadvantages, such as:

- More equipment, and then more complexity
- Higher propulsion losses due to conversion.

Evolution of control system closely followed electrification; US Navy, a typical conservative customer when comes to innovation, rendered public data shown in Fig. 1 [**3**]:

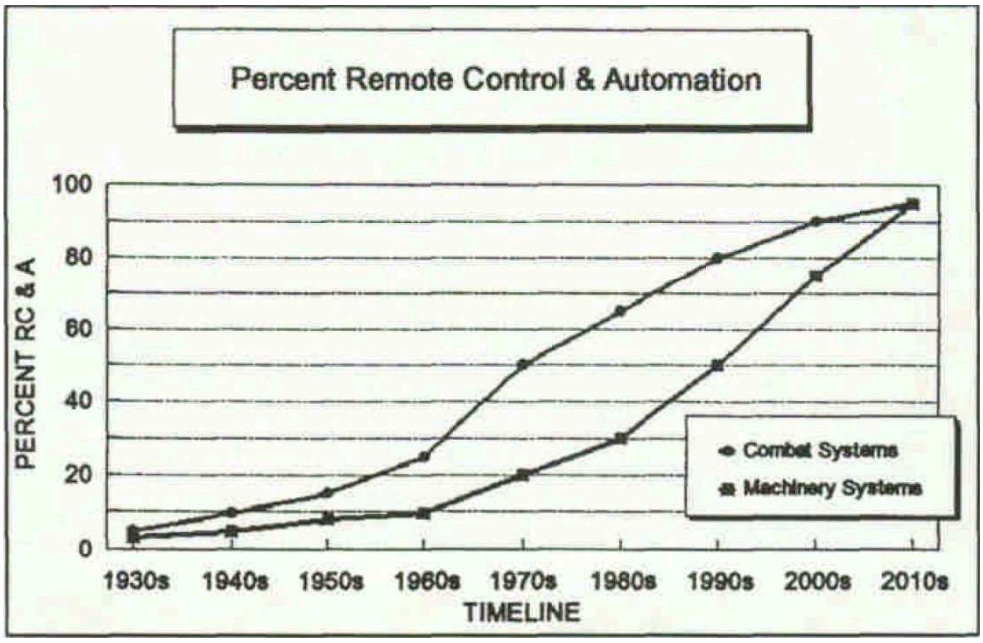

Fig. 1 Percent of Remotely Controlled or Automated Users vs. Time

In 80 years' time, nearly all ship design had changed in favour of automation and, in consequence, of electrical systems. Transition in merchant navy had been for certain faster.

By means of controls and communication techniques power intensive systems, such as propulsion, and more in general payload (cargo for merchant ships, weapons for military, HVAC or climate control for cruise ships, and so forth) are enable to coordinate actions with electrical power system in order to optimise results; by means of automation power can be managed to face the challenges of the moment.

A modern ship, no matter its service, heavily relies on its electrical system to grant safety of personnel, environment, and cargo. Electrical system is quintessential to personnel comfort, revenue making, or more in general to accomplish ship's function. From this simple set of considerations, reason and importance of *IPS*, in its extended meaning, appears.

1.3 All Electric Ship Present Situation.

Section *1.2* has illustrated ship systems dependency upon electrical power and control. This dependency calls for discipline, to safeguard human life, environment, cargo and, ultimately, vessel safety at sea. Several institutions supervise ship construction and operation, to ensure that life, environment, cargo and finally vessel are protected, with different degree of responsibility. Those institutions are:

- Port and flag state control authorities
- International regulatory bodies
- Ship owners

Port and flag state control authorities have legal jurisdiction on ships trading in respective state territorial waters, and are in charge of ensuring that ships under their control comply with the standards accepted by flag states under international law and conventions. Under international law, flag states are primarily responsible for ensuring compliance with international minimum standards [**4**].

Minimum standards port and flag control authorities are to enforce are prepared by international bodies under the aegis of the *UN*, such as *IMO*, *SOLAS*, *ILO*, *IEC*, classification societies, etc.

Classification societies have two main functions:

- Classify ships (private function). They set and maintain shipbuilding technical standards consolidating past experiences, statutory requirements and newest industrial and technological developments. They survey ship design, construction and commissioning to ensure standard compliance. They survey ships in operation to certify actual compliance is maintained. In this capacity, classification societies act as non-governmental associations and take limited liability for their omission ([**5**], Part 1, Chapter 1, Section 5, Paragraph A.100).
- Certify ships, on behalf of flag administrations (public function). They assess vessel compliance against international rules. In this capacity, classification societies represent government institutions; their advice has legal implications even though they are liable as before.

In both instances classification societies assess adherence to rules, either set by them or by other regulatory body.

Ship owners are legally forced, and carry liability for, to maintain ship seaworthiness, which basically means that ship is to be maintained in a fashion that permits compliance with rules set forth by port state control authorities. Ship owners have, in addition, different obligations due to their trading activities, such as:

- Business reputation. Owners rely on their vessel to deliver a service; the highest the dependability, or the trust clients can have in the fact that the service will be delivered up to the expectations (be they time or quality related), the highest the benefits on reputation.
- Return on investment. Owners rely on their vessels to deliver the service customers pay for in a reiterated, efficient and economical way. Long up time contributes to high revenues.
- Liability. Owners are legally liable for any damage their vessel produce on humans, environment, cargo and other vessels. Those liabilities can be a heavy burden and for certain insurance needs be instated. Owners rely on their vessel not to incur in such expenditures, which can cause, in the worst case, bankruptcy.

All these requirements concur to define ship electrical system resilience to an agreed range of anticipated faults or, in a different perspective, ability to deliver the expected service in potentially unfavourable conditions, for the longest possible period of time. They focus primarily on so called **main functions**, or systems essential to ensure safety of human life, environment, cargo and, ultimately, the vessel. Those functions are recognised to be ([**5**], Part 1, Chapter 1, Section 1, Paragraph A.220):

- Hull strength
- weather tight and watertight integrity
- electrical power supply

- propulsion
- steering
- drainage and bilge pumping
- ballasting
- anchoring

Those functions are considered as inherent in the concept of ship, in the sense that every ship has those functions. Ships differ then when comes to considering **accessory functions**: those may characterise ship's service, trade, etc.

It is easy observing at least four main functions (electrical power supply, propulsion, steering and anchoring) nowadays are electrically actuated and controlled, one, weather and water tightness, is increasingly becoming electrically actuated, being already electrically controlled[4]; this reiterates the fact that electrical systems are integral part of nowadays marine world.

Aim of this study is analysing all electric ship integrated power system **dependability**, or the ability to provide the expected service with acceptable trust, or, in a different perspective, the ability to avoid service failures that are more frequent or more severe than accepted [**6**]. This analysis is centred on design phase, as first stage of project execution, so able to impact all following phases. As explained already, dependability is a highly desirable propriety all electric ship integrated power system should have, and, as will be shown in the following, is included, even though not specifically mentioned, in many instances of documents influencing modern ship design.

Reason for this study is easily found in the importance of *IPS*, so stressed to generate the acronym *AES*.

1.3.1 Electrical Power Supply System.

As anticipated, most recognised classification rules list this system (or module, in the *IPS* framework set forth in [**2**]) as a main function. To enforce this vision, they set a vast corpus of rules governing the discipline. Owners as well include requirements, in order to suit vessel for their trading purpose. Typically, owners' requirements integrate class requirements to form a **technical specification**, describing the project in a level of detail that enables a successful design.

Basic and most common requirements defining the electrical power supply system in terms of performance, architecture and behaviour in presence of failures[5] are presented in this section.

Electrical power supply system is required to be built as the set of four interconnected, interacting and independent sub-systems, termed ***main*, *emergency*, *transitional* and *external* (or shore) electrical power supply systems**, according to their use.

[4] One of the first installations with electrically actuated watertight doors was the cruise ship Costa Luminosa, commissioned during 2009.

[5] Failure in the rule context is a sudden event or deterioration causing loss of function ([**5**], Part 4, Chapter 1, Section 1, Paragraph B.102).

- Main power supply system is to be capable of keeping the vessel in normal[6] and habitable[7] conditions.
- Emergency power supply system is to be used only when main fails to supply emergency services listed in Table 1.
- Transitional power supply system is to be used from the moment main failed to the moment emergency is online (this time frame shall not exceed 45 sec., if emergency system is fully operational), to supply systems listed in Table 2.
- External electrical power supply system is used when ship is alongside for a longer period of time (typically in excess of 4 hours, [**7**], Sec.1, Page 5 refers), and is to replace main system in its active functions in that specific situation.

More in details, systems that have to be supplied from emergency power supply are listed in Table 1.

System	Duration
Emergency lighting.	18 hours
Navigation lights.	18 hours
Fire pumps.	18 hours
Steering gear	½ hour
Watertight doors and hatches	18 hours
Internal and external communication systems	18 hours
Navigation systems	18 hours
Transitional Power Supply System	18 hours

Table 1: List of Systems That Have to Be Supplied from Emergency Power Supply.

Users required for dead ship re-starting (starting air compressors, pre-lubrication pumps, heaters, etc.) need only to have the possibility of being supplied from emergency power supply; they can be left deactivated during emergency till main power supply system is ready for restart.

Systems that have to be supplied from transitional power supply are listed in Table 2.

Electrical power supply system shall be arranged as an *AC* three wire, with insulated or earthed neutral, but without hull return (unless this is not necessary for some other reasons, such as insulation monitoring, hull cathodic protection and intrinsic safety circuitry). Three phase four wires and single phase arrangements are accepted if voltage is lower or equal to 500V, subject to confirmation hull return is not used.

[6] A ship is said to be in normal condition when main functions are fully operational. Main functions relevant to *IPS* are: power generation, propulsion, steering, power supply and control for ballasting, anchoring, drainage and bilge pumping. Normal operation for propulsion can be retained when a speed of 7 knots in calm waters, and ability to maintain position in Beauforts 8 with associated sea state conditions is achieved. [**5**], Part 1, Ch. 1, Sect. 1, Paragraph A.220 refers. Presence of personnel require safety systems, therefore normal condition is said to be achieved when all main functions and safety provisions are functioning normally. [**5**], Part 4, Chapter 8, Section 13, Paragraph A.201.

[7] Additionally, all systems required to achieve designed comfortable conditions for habitability, shall be functioning normally. Those latter systems include: cooking, heating, domestic refrigeration, mechanical ventilation, sanitary and fresh water. All utility systems for the listed functions shall be included. [**5**], Part 4, Chapter 8, Section 13, Paragraph A.201.

System	Duration
Emergency Lighting	½ hour
Navigation Lights	½ hour
Watertight doors and hatches	½ hour
Internal and external communication systems	½ hour
Fire detection and Alarm System	½ hour
Gas Detection and Alarm System	½ hours
General Alarm System	½ hours

Table 2: List of Systems That Have to Be Supplied from Transitional Power Supply

Electrical power supply system shall operate at specified voltage and frequency levels, within specified tolerances, indicated in the following table, derived from *IEC* 60092-201[8]:

Nominal Voltage	Tolerance (on nominal value)	Nominal Frequency	Tolerance (on nominal value)	Use
11kV AC	±2,5% Steady state -15% / +20% Transient	50/60Hz	±5% Steady State ±10% Transient	Power Supply, Power Supply
6,6kV AC	±2,5% Steady state -15% / +20% Transient	50/60Hz	±5% Steady State ±10% Transient	Electrical power supply, Power Supply
690V AC	±2,5% Steady state -15% / +20% Transient	50/60Hz	±5% Steady State ±10% Transient	Electrical power supply, Power Supply
440V AC	±2,5% Steady state -15% / +20% Transient	60Hz	±5% Steady State ±10% Transient	Electrical power supply, Power Supply Control
400V AC	±2,5% Steady state -15% / +20% Transient	50Hz	±5% Steady State ±10% Transient	Electrical power supply, Power Supply Control
230V AC	±2,5% Steady state -15% / +20% Transient	50/60Hz	±5% Steady State ±10% Transient	Power Supply Control
230V DC	-15% / +30% Cyclic variation < 5% Ripple < 10%	N/A	N/A	Power Supply Control
120V AC	±2,5% Steady state -15% / +20% Transient	60Hz	±5% Steady State ±10% Transient	Power Supply Control

[8] This rule unifies voltage levels belonging to different systems; 690V belongs to 50Hz series but can fit 60Hz considering that it can be thought of a 660V + 4.5%, so within tolerance.

Nominal Voltage	Tolerance (on nominal value)	Nominal Frequency	Tolerance (on nominal value)	Use
120VDC	-15% / +30% Cyclic variation < 5% Ripple < 10%	N/A	N/A	Control
48V DC	-15% / +30% Cyclic variation < 5% Ripple < 10%	N/A	N/A	Power Supply Control
24V DC	-15% / +30% Cyclic variation < 5% Ripple < 10%	N/A	N/A	Power Supply Control

Table 3: Voltage and Frequency Level, Together With Associated Tolerances.

Electrical power supply system shall operate keeping maximum *THD* level below 8%, with no single harmonic exceeding 5%.

Users shall be arranged in compliance with following requirements ([**5**], Part 4, Chapter 8):

- The failure of any single circuit or bus bar section shall not endanger the services necessary for the vessel's manoeuvrability. The failure of any single circuit shall not cause important services to be out of action for long periods. Any single failure shall not render duplicated consumers serving essential[9] or important[10] services inoperable.
- When the secondary distribution is arranged as two separate systems each fed from one transformer or converter, duplicated essential or important consumers shall be divided between the two systems.
- Each transformer required to ensure component redundancy for main sources of power, transformers and power converters in the main power supply system, shall be installed as a separate unit, with a separate enclosure.
- Where the main source of electrical power is necessary for propulsion of the ship, and for high voltage distribution systems, the main bus bar shall be subdivided into at least two parts which shall normally be connected by circuit breakers or other approved means; so far as is practicable, the connection of generating sets and other duplicated equipment shall be equally divided between the parts.
- Electrical discriminative protection against over-current shall be insured. Low voltage systems shall be protected against over-voltage.

[9] Essential (primary essential) services are those services that need to be in continuous operation for maintaining the vessel's manoeuvrability in regard to propulsion and steering. [**5**], Part 4, Chapter 8, Section 13, Paragraph A.300 refers.

[10] Important (secondary essential) services are those services that need not necessarily be in continuous operation for maintaining for the vessel's manoeuvrability, but which are necessary for maintaining the vessels functions. [**5**], Part 4, Chapter 8, Section 13, Paragraph A.302 refers.

1.3.1.1 Main Electrical Power Supply System.

Main electrical power supply system shall be designed to ensure electrical power supply to the vessel in normal conditions[6].

System shall be arranged in such a fashion that there shall be component redundancy for main sources of power, transformers and power converters so that with any source, transformer or power converter out of operation, it shall be capable of supplying power to following services:

- Those services necessary to provide normal operational conditions for propulsion and safety. This requirement substantially dictates that propulsion service is to be maintained even in case of one generator (or transformer, or converter; but those pieces of equipment do not belong to scope of analysis, as will be shown) being out of service,
- Starting the largest essential or important electric motor on board, except auxiliary thrusters, without the transient voltage and frequency variations exceeding the limits specified in *1.3.1*,
- Ensuring minimum comfortable conditions of habitability which shall include at least adequate services for cooking, heating, domestic refrigeration (except refrigerators for air conditioning), mechanical ventilation, sanitary and fresh water

Furthermore, it shall be designed in a way that a single failure does not disable propulsion permanently.

To that extent main electrical power supply is to consist of at least two identical and independent (i.e. not sharing components or services) **power stations**, interconnected by at least one **interconnecting line**.

A power station is defined as the set constituted by at least one **generator** and a **main switchboard incoming cubicle**.

A generator is defined as the set consisting of a **prime mover** and an **alternator**; a main switchboard incoming cubicle is a switchboard **section** including a **cable** and a **breaker compartment**. Breaker compartment contains its relevant circuit breaker, which forms part of the set. Terms section, and compartment are defined in *IEC* EN 60439, part 1.

An **interconnecting line** is the set constituted by one or two switchboard sections, containing each a cable and a breaker compartment, fitted with its circuit breaker, one at each power entering end, and interconnecting cabling or bus bars[11]. Examples can be found in the following pictures (Fig. 2, Fig. 3, Fig. 4 and Fig. 5).

Fig. 2 and Fig. 3 show details of main electrical power supply system; Fig. 2 shows the 11kV and Fig. 3 the 690V level. Power stations can be identified by the circled numbers in Fig. 2. In this case main switchboard is said to be formed by two components: high voltage switchboard and low voltage switchboard, shown in Fig. 3. High and low voltage switchboards are interconnected by three transformers, two in use, one for each low voltage switchboard, and the third as reserve[12].

[11] [**5**], Part4, Chapter 8, Section 12, Paragraph A.401 b confirms this architecture.

[12] In this paragraph classification and owners' requirements are not separated; in fact the need of two power stations is a class requirement, whist the use of a third HV/LV transformer is an owner request. Picture in subject exemplify the implementation of rules and requirements, produced by different entities, into one specification.

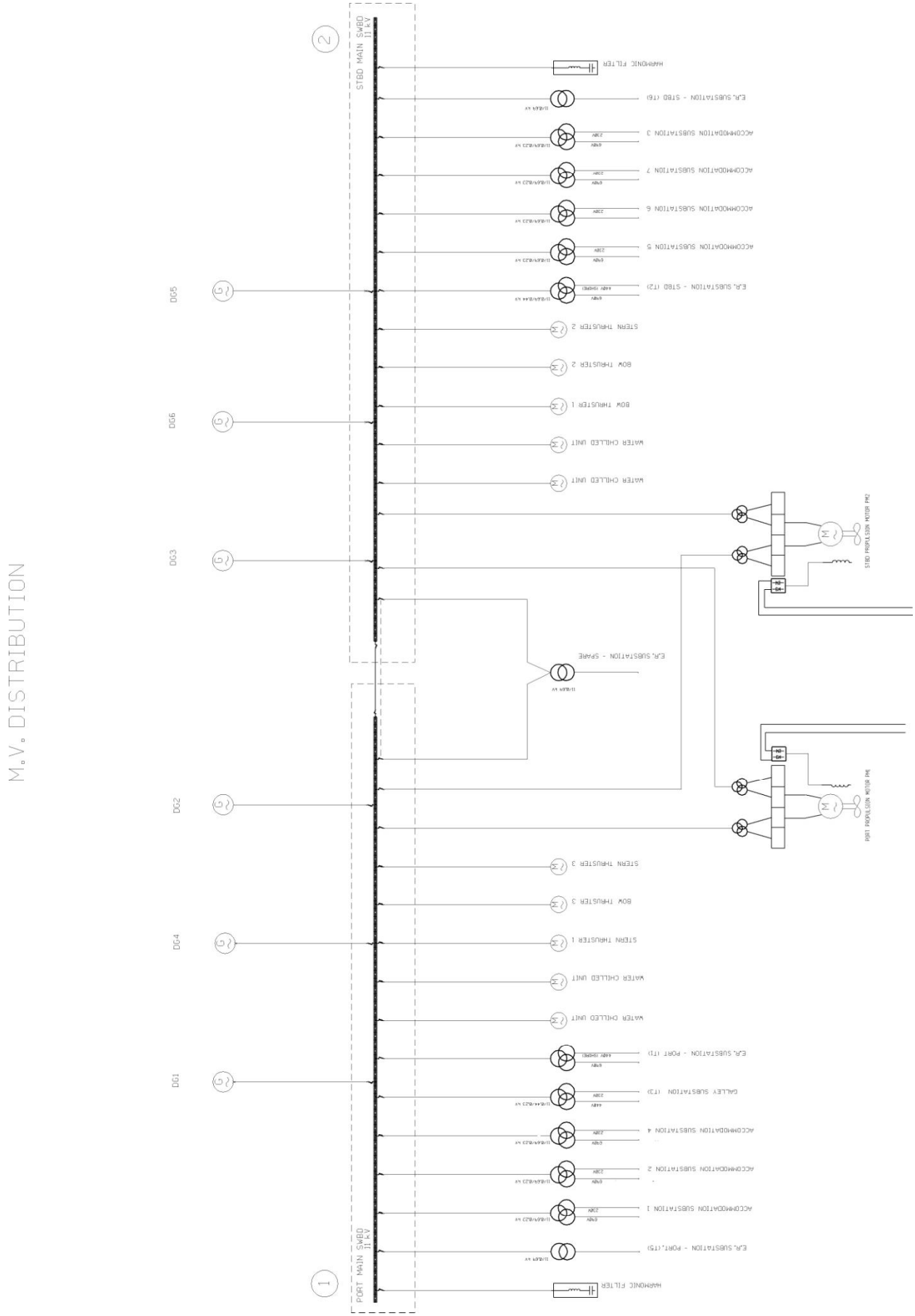

Fig. 2: *IPS* Layout, High Voltage Electrical power supply, Distribution and Electrical Propulsion. Cruise Ship Application

Non duplicated services mentioned above shall be then supplied by both power stations, with change over arrangements (automatic, manual) where necessary; duplicated shall supplied from different power stations.

Propulsion system is a typical duplicated system, as one shaft line satisfies criteria set forth in *1.3.1*; the two shaft lines are then to be supplied from different power stations. In fact, Fig. 2 shows a little bit more complicated situation, fruit of a specific interpretation. In that figure the entity "shaft line" is constituted by two converters, but connected to different shafts. In the end, whatever the failure, two converters are to remain, generating the same thrust one complete shaft line would, and with the advantage that resulting thrust is balanced because exerted over two shafts. An owners' request (cross connection) has been merged with a class request.

Emergency electrical power supply system is interconnected to main so that emergency generator is not demanded to run continuously. Interconnection is automatically discontinued in case of failure, in order to preserve independency ([**5**], Part 4, Chapter 8, Section 2, Paragraph C.105) and continuity of supply.

Transitional electrical power supply system is shown as interconnected to the emergency power supply, 230V section (Fig. 3). In normal condition this system is just an aggregated load for the emergency power supply, which is in turn an aggregate load for the main power supply; in an emergency the three sub-systems discontinue their interconnection and act as independent supplies of electrical power.

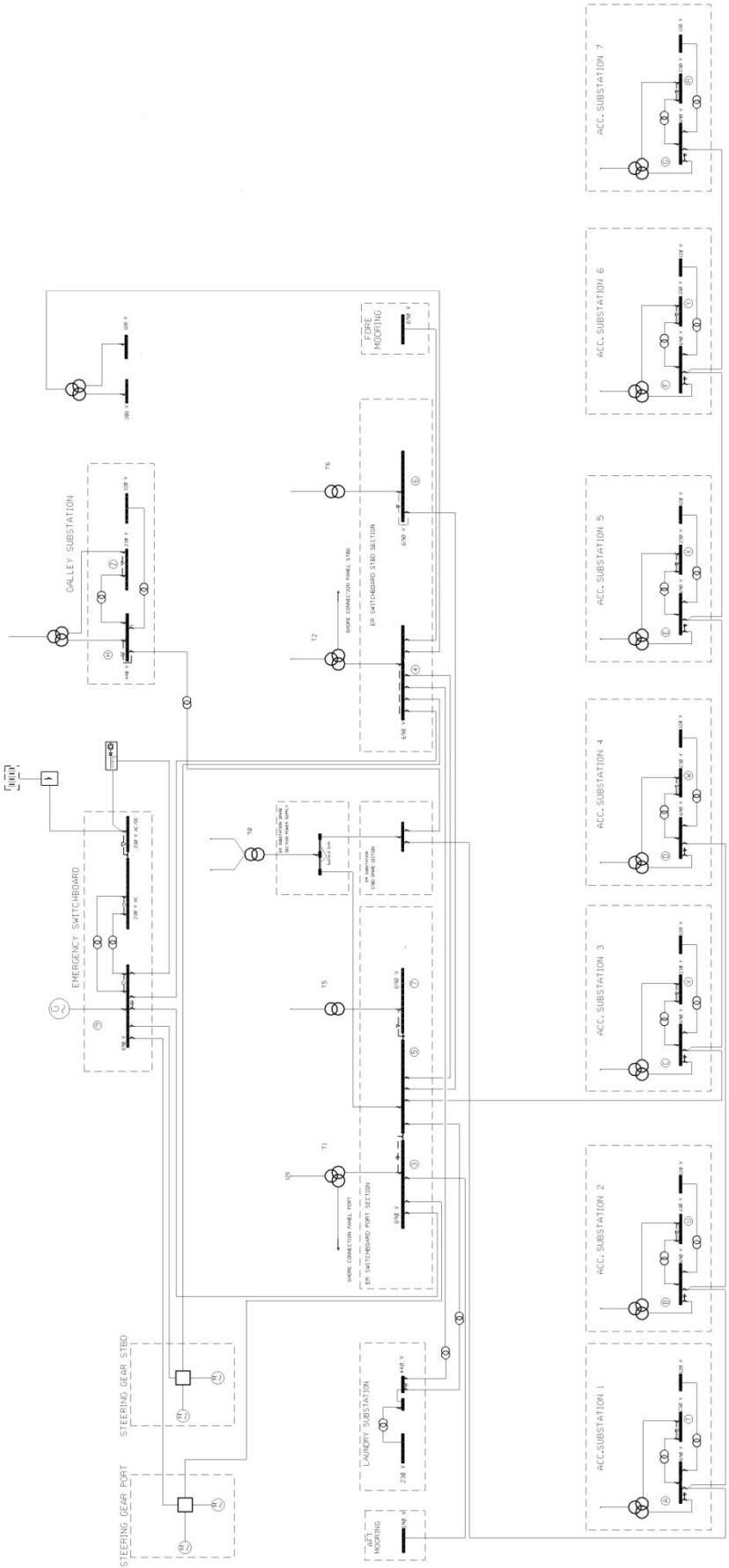

Fig. 3: *IPS* Layout, Low Voltage Distribution. Cruise Ship Application

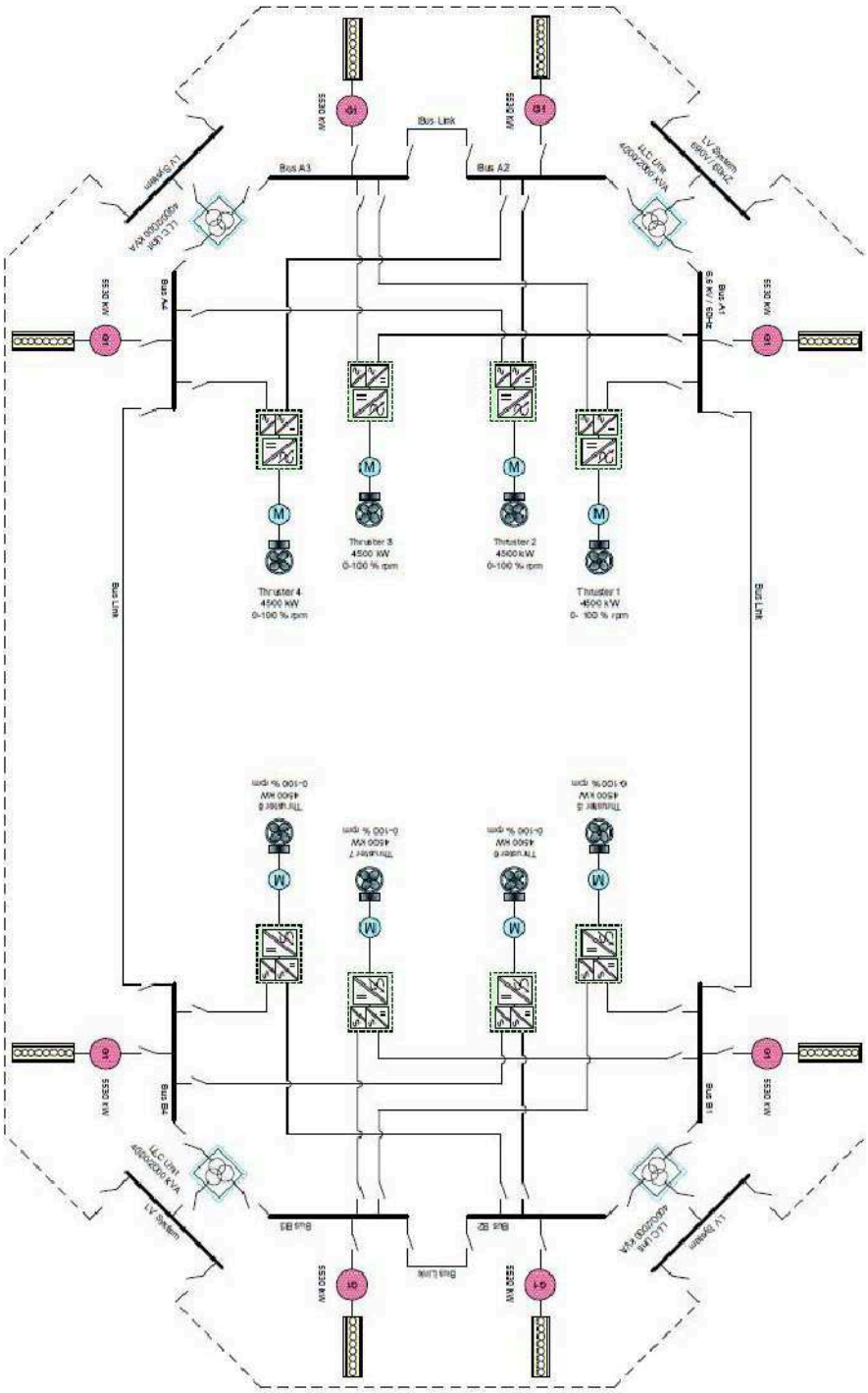

Fig. 4: *IPS* Layout, *DP3* Vessel Application

Fig. 4 and Fig. 5 are topologically similar to Fig. 2 and Fig. 3, promoting the idea that *IPS* is a unifying concept, spread across different business. Fig. 4 and Fig. 5, in fact, show an example drawn from a *PSV* application, equipped with classified *DP* system.

Fig. 4 shows *IPS* high voltage part. It consists of same components of cruise application, even though arranged in a different fashion, in force of different rules to abide by. Power stations, interconnecting lines, main switchboard and transformers can be easily identified.

Fig. 5 shows a simpler *PSV IPS*, based upon low voltage supply and distribution. Still same layout and components can be identified: power stations, interconnecting lines, main switchboard and transformers.

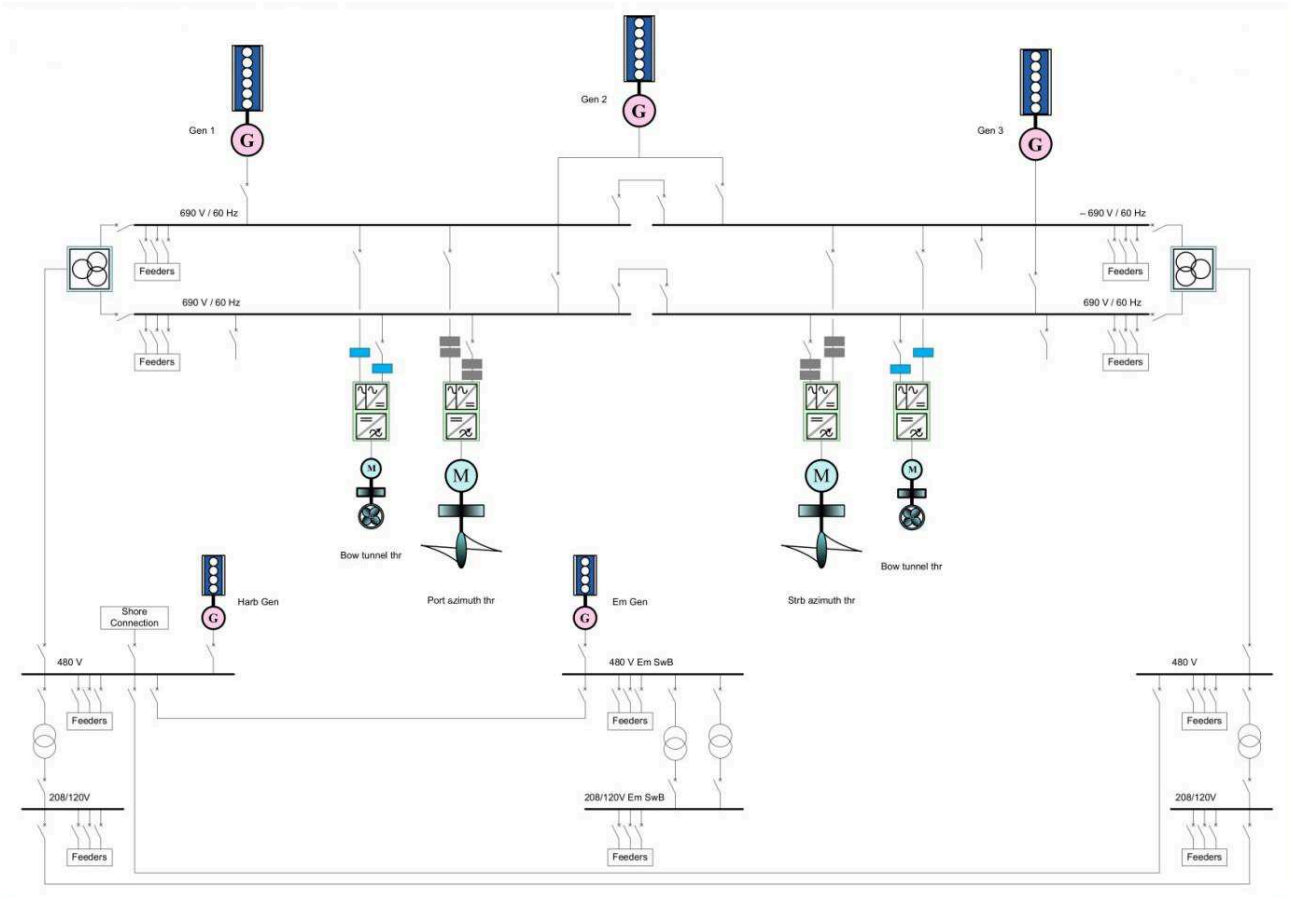

Fig. 5: ***IPS*** **Layout, Low Voltage Distribution. DP2 Vessel Application**

1.3.1.2 Emergency Electrical Power Supply System.

As anticipated, this system serves as dedicated reserve power supply for systems defined in Table 1, should a casualty generates an emergency leading to the failure of *Main Electrical Power Supply System*. In the context of marine rules, an emergency is intended as a fire or flood casualty the consequences of which may lead to a main electrical power supply failure with consequent loss of manoeuvrability and propulsion[13].

Emergency electrical power supply system is arranged as a power station, independent from main and transitional, located in an area deemed safe against fire, flood and damages caused by a collision. Emergency power station shall be, furthermore, **self-contained**: all auxiliary dedicated to its functioning shall be located in the same space[14], including fuel storage, prime mover and its starting arrangements (engine powered hand cranked air compressor with relevant piping and/or electric starter motor, with associated cables,

[13] Surprisingly enough, no formal definition of emergency can be found in the rules. Definition of emergency in the context of this work has been "reverse engineered" from the requirements, which basically call for fire and flood fighting.

[14] Emergency power station can be imagined as a containerised power supply that needs power connections to external loads only to operate.

power supply and its controlling equipment and source of power, etc.), cooling (heat exchangers, pumps, etc.), ventilation (fan motor, impeller, dampers, starting panel, power cables, etc.), etc.

Risk of fire within the emergency power supply space shall be minimised; every possible ignition source, such as batteries, unless not essential to the functioning of the emergency power supply (batteries to start emergency power source, if it is constituted by a diesel engine, for instance), is not allowed.

1.3.1.3 Transitional Electrical Power Supply System.

This system is as well arranged as a self-contained independent power station, and serves two main purposes:

- Maintain power supply to users listed in Table 2 in case emergency is not resolved and emergency source of power has exhausted, for half an hour. Those users are sensitive for abandoning the vessel and request help, as they mainly serve the purpose of identifying escape routes, providing evacuation indications, position fixing and communicating distress.
- Backing up power for essential safety systems (fire detection and hull water tightness integrity).

The transitional source of electrical power shall consist of an accumulator battery, located as described in *1.3.1.2*. The battery source shall be charged by *Emergency Electrical Power Supply System* and be able to operate, without recharging, while maintaining the voltage of the battery throughout the discharge period as listed in Table 2.

1.3.1.4 External (Shore) Electrical Power Supply System.

In the attempt of safeguarding environment reducing ships smoke emission when alongside (and following suit the consideration that land base power plants are more efficient in transforming fossil fuels into electrical energy) ships are requested to be equipped with the possibility of receiving electrical power from ashore, arresting onboard generators. Given the amount of power requested (even small vessels nowadays need megawatts of power to keep habitable conditions, cargo systems for loading and unloading, and sufficient auxiliary to maintain readiness to recover from a shore power system failure), use of medium voltage[15] is often envisaged. Ships with high voltage power stations are then to receive electrical power at a suitable voltage level in the range of 1 to 15kV (Table 3); ships with low voltage power stations may receive

[15] Here the word “medium” refers to definition given in IEC 60038, or a voltage between 1 and 35kV. Ship classification societies refer to low voltage as a voltage lower than 1kV, and high voltage to a voltage higher than 1kV. In the following, the word “medium” refers to a shore standard, as opposed to word “high”, which refers to a marine standard. It is worth noting classification societies do not allow system voltages in excess of 15kV, therefore there will be no ambiguity of meaning when discussing high voltage in shore installation, as such levels (from 35 up to 230kV) do not belong to marine environment.

electrical power directly at low voltage level[16] (see an example in Fig. 5) or be equipped with a dedicated step down transformer, either mounted onboard, as Fig. 6 shows, or ashore.

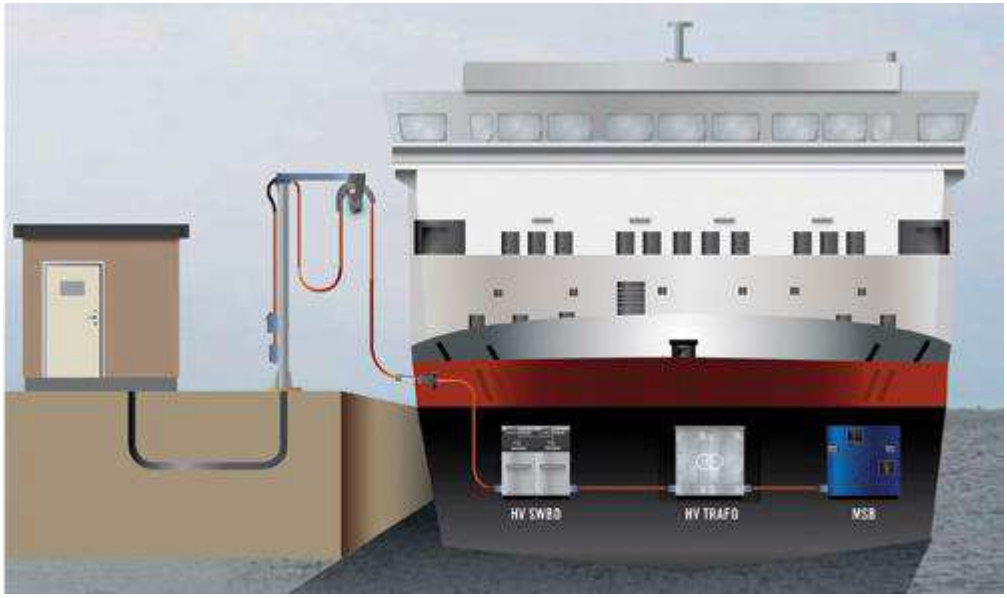

Fig. 6: High Voltage Shore Connection with Ship-borne Transformer

Transformer may be needed in case of low voltage shore connection too, as Fig. 3 illustrates; 690V is not common in the US where 450V is available instead. This fact forces the adoption of a further transforming step.

Compulsory requirements are set forth by classification societies to discipline this mode of operation ([**7**] and [**8**]) owing to the fact ships can be engaged in operations, such as loading or unloading, that may be sensitive to personnel, environment, cargo and vessel safety, so falling under their competence. Even in this circumstance ship owners may decide to complement class requirements with others, derived by their trading needs. Requirements are presented in the following, and some basic safety assumptions are made:

- Vessel is supposed to stay safe between a black-out, originated by shore supply failure, and its recovery by ship systems. This assumption is not unreasonable, as it applies every time a black out happens at sea, so it is already built in the ship design.
- Vessel electrical systems are supposed to stay safe even when powered from shore; shore supply is to be adapted to ship systems, which will be unchanged. Adaptation is to be made within the *HVSC* or *LVSC* system.

In essence, a *HVSC* or *LVSC* system must be designed to safely and effectively deliver a certain amount of electrical power, sufficient to support services needed for ship operation in port, at a suitable voltage and frequency level (Table 3). To this extent, following provisions are considered necessary:

- Shore transmission lines equipped with over current and under voltage release (Fig. 7, item 1). This transmission line departs from shore distribution system and powers the transformer and is controlled from ship by means of a “permit to operate” signal, generated when all safety conditions are met (see in the following). This signal is designed to be fail-safe, being the safe

[16] It is worth recalling the preparation effort in this case: a 120 mm^2 three cores marine cable can carry about 237A; at 690V transmitted power is about 283 kVA. This means that 4 cables are needed per each MVA of transmitted power, so 8 terminations and adequate supporting and management for the weight.

condition denial to operate. All control equipment is located within item 3, being the *HVSC* cubicle built according to form 4, mandatory for this kind of installation.

- An insulation transformer. This item can be installed in two different ways:
  - Ship-borne (see Fig. 6 for reference). In this case (see Fig. 7) item 2 becomes a straight connection and circuit breaker on item 1 is interlocked with earth section breaker on item 4. Item 10 is the ship borne transformer.
  - Shore based. In this case (Fig. 7 refers) item 10 is replaced by a straight connection.
- A flexible transmission line, equipped with an automatically operated earth switch enabling safe discharge of the cable and safe handling of the plug and socket (Fig. 7, item 6).
- a shore connection box containing:
  - plug receptacles to receive shore flexible connection (Fig. 7, item 9)
  - An earth switch, enabling safe discharge of the cable and safe handling of the plug and socket (Fig. 7, item 9).
  - Means of displaying phase rotation and system live condition (Fig. 7, item 8).
- Fixed ship cabling from shore connection box to power station switchboard (Fig. 7, item 11).

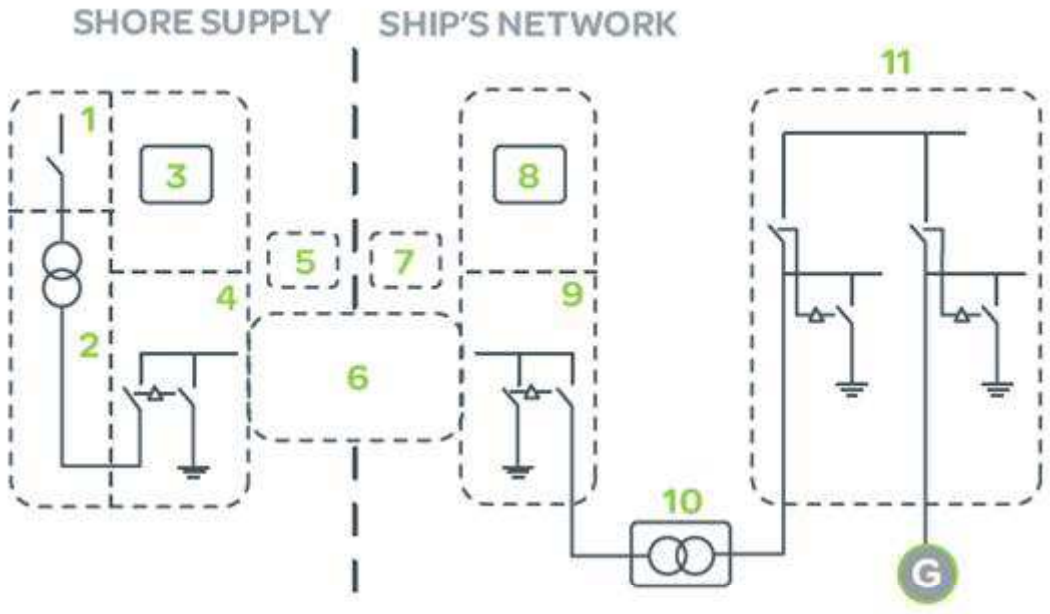

Fig. 7: Shore Connection System Component Overview.

Shore electrical power is delivered on board at power station input interconnecting line (Fig. 7, item 11). This line is to be equipped with over current and bi-directional short circuit protection, under-voltage trip and instrumentation for a short time parallel, long enough to permit smooth ship generators unload. This breaker is operated once voltage from shore is detected, by means of an appropriate voltage coil, installed on cable side.

System is to be remotely operated from engine control room, and short time parallel and consequent generators unloading, automatically managed.

Safety is ensured by designing the system so that:

- A separate conductor for protective earthing shall be connected between the hull of the vessel and the ground on the shore.
- The vessel's designed system earthing is to be maintained in electrical shore connection operation.

- There shall be installed equipment enabling efficient cable handling and connection. The equipment shall ensure mechanical tension control of the cable and provide alarm at high cable tension to a manned position. If tension exceeds its safety limit, the shore connection shall be automatically disconnected, and the earthing switches closed.
- There shall be a monitoring system ensuring proper connection between shore ground and hull. This is a safety requirement, it imposes potential be same all the times between ship and shore, so that personnel walking off the ship would not incur in a dangerous step voltage[17].

1.3.2 Electric Propulsion System.

Propulsion is, as anticipated, one of the vessel main functions ([**5**], Part 1, Chapter 1, Section 1, Paragraph A.220), therefore under class control. It shall, according to mandatory requirements:

- At least move the vessel through the water in a controlled manner, at a navigable speed[18], to the planned port, or to another safe stopping position. Maximum and service speed, together with vibration requirements are specified by owners subsequently.
- Bring the moving vessel to stand still, by use of a pre-defined procedure.
- Keep the vessel with bow against the wind in weather conditions as applied for design[19].
- Be designed as a duplicate system, so that a single failure does not lead to the unavailability or inability to start or stop the main function. This basically means that ships shall have duplicated **propulsors**. A propulsor is:
    - In case of a ship equipped with shaft lines, the set made of the following components (see Fig. 8 for reference, stern tube, line and thrust bearings are not shown):
        - A propeller and its associated pitch control hardware, if provided;
        - A shaft line and its associated bearings (stern tube, line and thrust);
        - A reduction gear and its associated pieces of auxiliary (clutch, lubrication, cooling, etc.), connecting shaft line to its torque generators;
        - One or more propulsion electrical motors, and their associated fans, heat exchangers, bearings and excitation system (if provided), converting electrical power into mechanical torque;
        - One or more propulsion frequency converters, and their associated cooling system, controlling electrical power to drive electrical motors;
        - One or more propulsion transformers (if provided), and its associated cooling system, adapting grid voltage level to that of converters Number of those transformers may vary according to *THD* and induced vibrations requirements.

[17] This requirement relies on the assumption that ship berth is included into shore power station earthing mat. Such assumption needs be carefully verified, as explained in [**27**].

[18] Navigable speed is 7kn in calm waters, as [**5**], Part 4, Chapter 1, Appendix A states.

[19] Wind Beaufort 8 and associated sea conditions.

- In case of a ship equipped with pod propulsion, the set made of the following components (see Fig. 9 for reference, transformers and converters are not shown, but are installed inboard, in a similar fashion as in Fig. 8. Cooling case and slip rings are not shown as well):
  - A propeller and its associated pitch control hardware, if provided,
  - A propulsion electrical motor, and its associated heat exchangers, bearings, bilge system, power transmission[20] and excitation system (if provided),
  - One or more propulsion frequency converters, and their associated cooling system,
  - One or more propulsion transformers (if provided), and their associated cooling system. Number of those transformers may vary according to *THD* and induced vibrations requirements.
- In case of a ship equipped with azimuthing thrusters, the set made of the following components (see Fig. 10, transformer and converters are not shown, but are installed inboard, in a similar fashion as Fig. 8):
  - A propeller and its associated pitch control hardware, if provided,
  - A propulsion electrical motor, and its associated heat exchangers, bearings and excitation system (if provided),
  - One or more propulsion frequency converters, and their associated cooling system,
- One or more propulsion transformers (if provided), and their associated cooling system. Number of those transformers may vary according to *THD* and induced vibrations requirements.

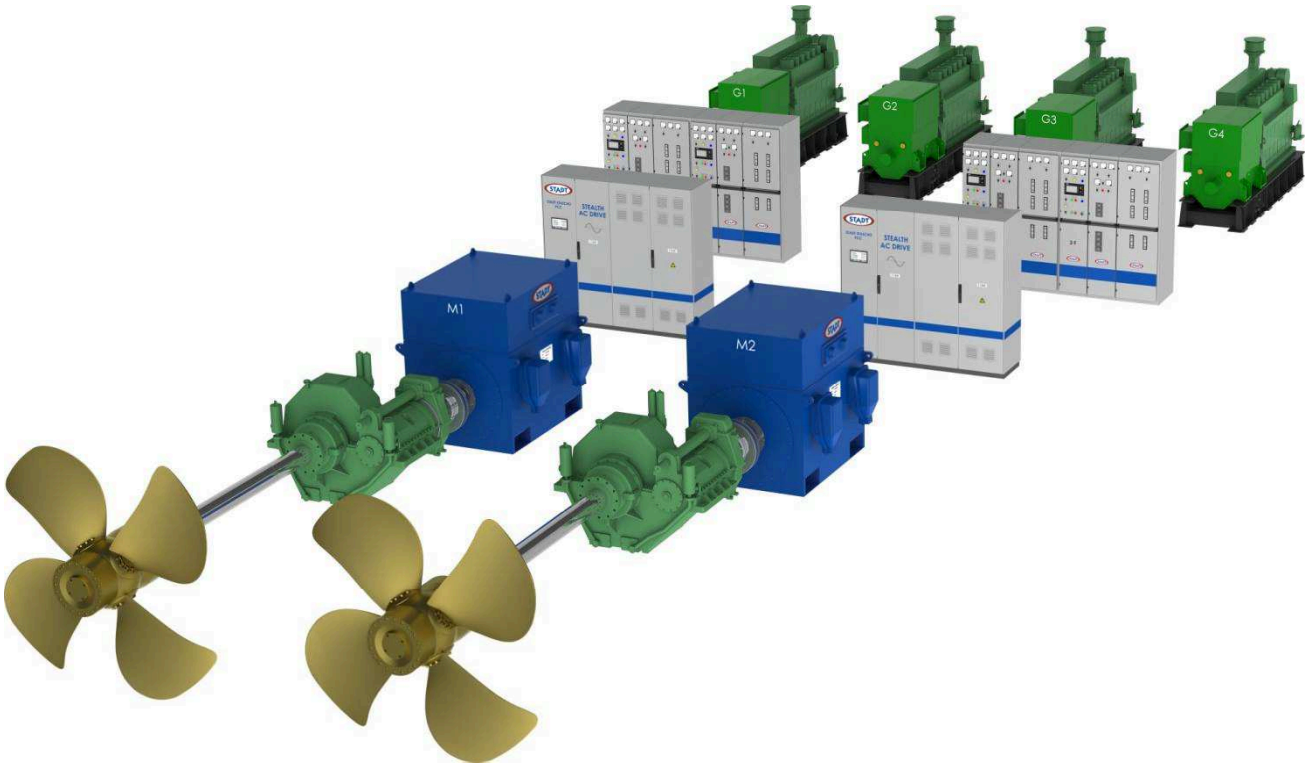

Fig. 8: Typical Shaft Line Arrangement with Electrical Propulsion. Thrust and Line Bearings Are Not Shown

[20] Power transmission is meant, in this circumstance, from the fixed inboard part to the movable (steerable part). It usually happens by means of brushes making contact on dedicated copper rings.

- Be designed with redundancy type R1 so that power for manoeuvrability is restored preferably within 30 seconds, but in any case not more than 45 seconds after loss of power.
- Be designed to ensure that no common mode failures endangering the manoeuvrability of the vessel, except for fire and flooding[21], which are accepted as common mode failures, are present.
- Be designed to ensure *THD* limits are not exceeded during its use. Harmonic filters may be considered.

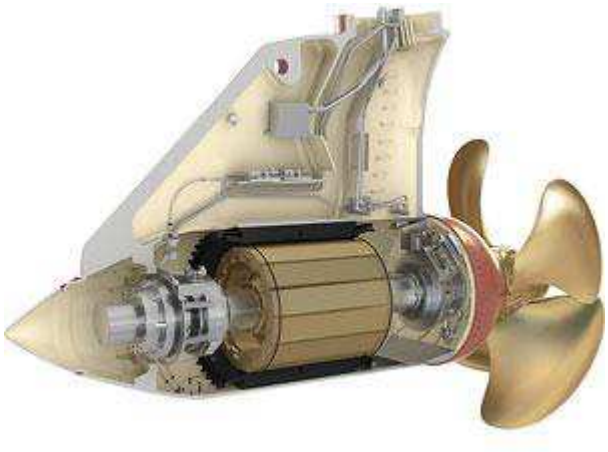

Fig. 9: Typical Pod Arrangement

Fig. 10: Typical Azimuth Thruster Arrangement

1.3.3 Steering System.

Steering system shall ([**5**], Part 4, Chapter 14):

- be capable of operating the rudder for the purpose of steering the ship at maximum ahead service speed which shall be demonstrated
- have capacity to turn the rudder from side to side according to requirements given below at maximum ahead service speed:
  - from 35° on one side to 35° on the other and vice versa
  - from 35° on either side to 30° on the other side respectively within 28 seconds
- turning rudder back to neutral position from any possible steering angle that intentionally or unintentionally may be initiated

As a main function, this system shall be engineered with duplication features: all actuating and controlling equipment shall be duplicated (rudder stock is exempted).

Power supply is arranged in a way to offer duplication to the highest extent: every steering gear unit shall have two power supplies, one from main and the other from emergency system. In case of multiple steering gear units, they must be installed in different watertight spaces, and their main power supply shall come, as far as possible, from different power stations. Power cables must be run so that they share minimum possible common path.

[21] Safe Return to Port casualties are in fact fire or flooding, as will be discussed afterwards, in 1.3.5.

Power supply shall be arranged for highest level of availability: no overload protection is to be installed.

Pod propulsion, in which steering and propulsion functions are combined into one or more individual units, termed **pod**, includes additional requirements that will be discussed later on in *1.3.4*

1.3.4 Controls.

Controls are necessary to main functions and services, and are to be considered as part of. They are responsible for the interaction among various services that promotes the concept of *IPS*.

Controls are located at different hierarchical levels:

- Direct control (digital, analogue[22] or operator actuated[23]). This control scheme foresees these characteristics:
  - Both controller (a device or a human) and actuator are located near to its controlled equipment, or are integrated in it.
  - One dedicated controller is installed for each **process segment**, or a collection of mechanical equipment with its related field instrumentation, e.g. machinery or piping system[24], serving one process operation ([**5**], Offshore Standard D202, Chapter 1, Section 1, Page 11, for instance). Segment controllers collect data from segment instrumentation and apply control action driving segment actuators; quite often this control is defined as **automatic**, as it is performed without the action of a human operator. Examples can be found in the following pictures: Fig. 11 shows a local direct manual control appliance, whilst Fig. 12 shows a local direct automatic control. In the case shown in Fig. 11 interaction takes place by means of pushbuttons, and situation awareness relies on local instrumentation completeness; instead, in the case described in Fig. 12, interaction takes place by means of a screen and keyboard, and it is limited to set point input, even though it is often possible driving actuator directly by means of dedicated keystrokes. Situation awareness still depends upon completeness of displayed information. Direct controls can only be local, given their typical implementation.
- ***SCADA***. Such a system consist of following hardware:
  - Remote terminal units (*RTU*[25]) in charge of collecting and digitalizing measures from field instrumentation and applying control action by means of dedicated outputs. Those pieces of hardware are distributed all around the vessel, near to monitoring instrumentation.
  - Programmable logic controllers (*PLC*) doing same service of *RTU* but with controlling abilities[26]. Those pieces of hardware are located all around the vessel, convenient to related

[22] Analogue control is nowadays old fashion, and can be found in particular instances only.

[23] Often direct control performed by a human operator is called **local** control, given the fact that control action is generated locally. Equally often this direct control performed by a human operator is termed **manual** control, owing to the fact that operator manually applies control action, via actuators.

[24] [**5**], Part 4, Chapter 9, Section 1, Paragraph B.107

[25] Those units are often termed *RIO*.

measuring points and/or controlled process segments. *PLC* may, as anticipated, execute direct control; therefore their location will be within the controlled process segment.

Fig. 11: Example of Local Control Panel

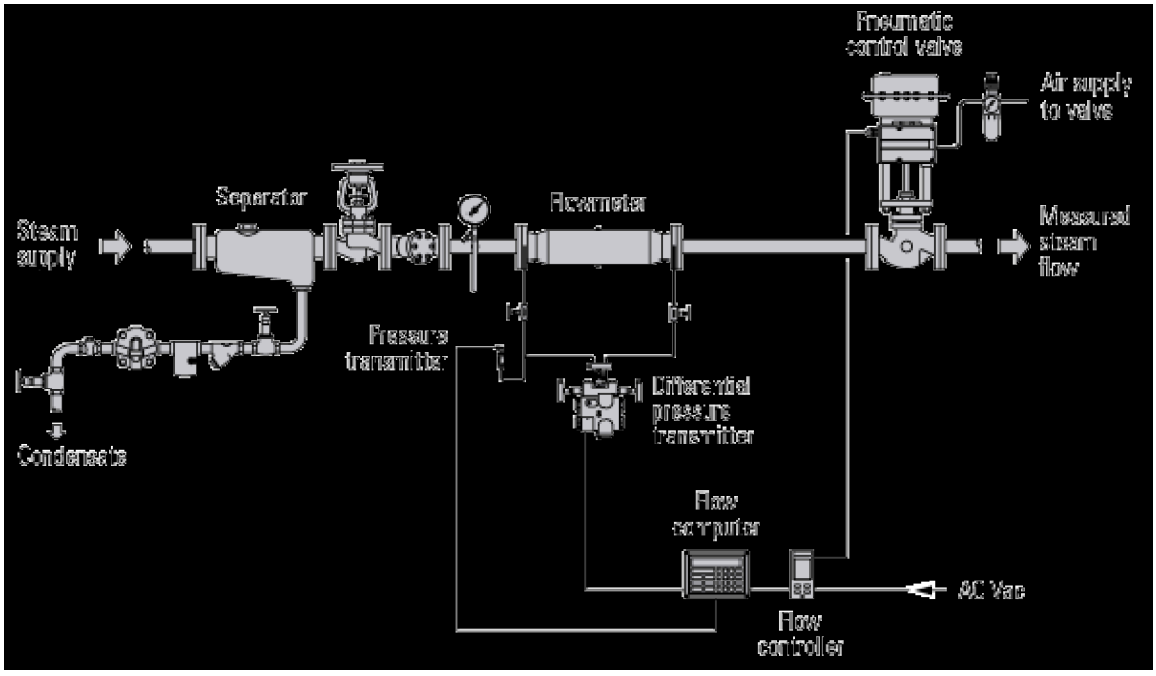

Fig. 12: Example of Direct Automatic Control.

[26] A *PLC* can do direct control, as opposed to a *RTU*, which is not supposed to. In case of *SCADA* control action is elaborated by supervisory computers, therefore there is no functional difference between a *PLC* and a *RTU*. Difference becomes sensible if a **distributed SCADA** is defined; such entity sees process computer be replaced by local *PLC*, and control application code be subdivided in functional part, executed locally.

- One or more computer data networks conveying measures from field to supervisory computers. Data network consist of all appliances and policies needed for data transmission, i.e. routers, switches, network adapters and so forth. Owing to their nature, data networks cover the entire vessel space.
- One or more supervisory computers, running a *HMI*, collecting historical values and interface with external computer systems (reporting application, remote maintenance, etc.) and interfacing with operators. This equipment is usually concentrated in the *ECR*.

One *SCADA* serves many (if not all) installed process segments: it collects data and relevant quality information (as per *OPC* standard) from *RTU* or *PLC*, conveys them via the computer data network to supervisory computers, which in turn elaborate the control action. Control action is transferred back to *RTU* via the computer data network, and actuated by them driving process segment actuators. As already mentioned, control action elaboration can be distributed; in this case only monitoring values and set points are transported by computer data network.

Operators may interact with control process, via *HMI*, in different ways:

- Changing the process segment set point or dynamic parameters (proportional, derivative or integral gain in case of *PID*).
- Inputting control action manually, generally operating increase/decrease soft push buttons.

SCADA is quite often referred as **remote** control, owing to the fact that control action is elaborated remotely; furthermore remote control may be termed **manual**, if a human operator is included in the control loop, or **automatic**, if no human is included in the control loop.

Fig. 13 shows an example of a marine *SCADA*.

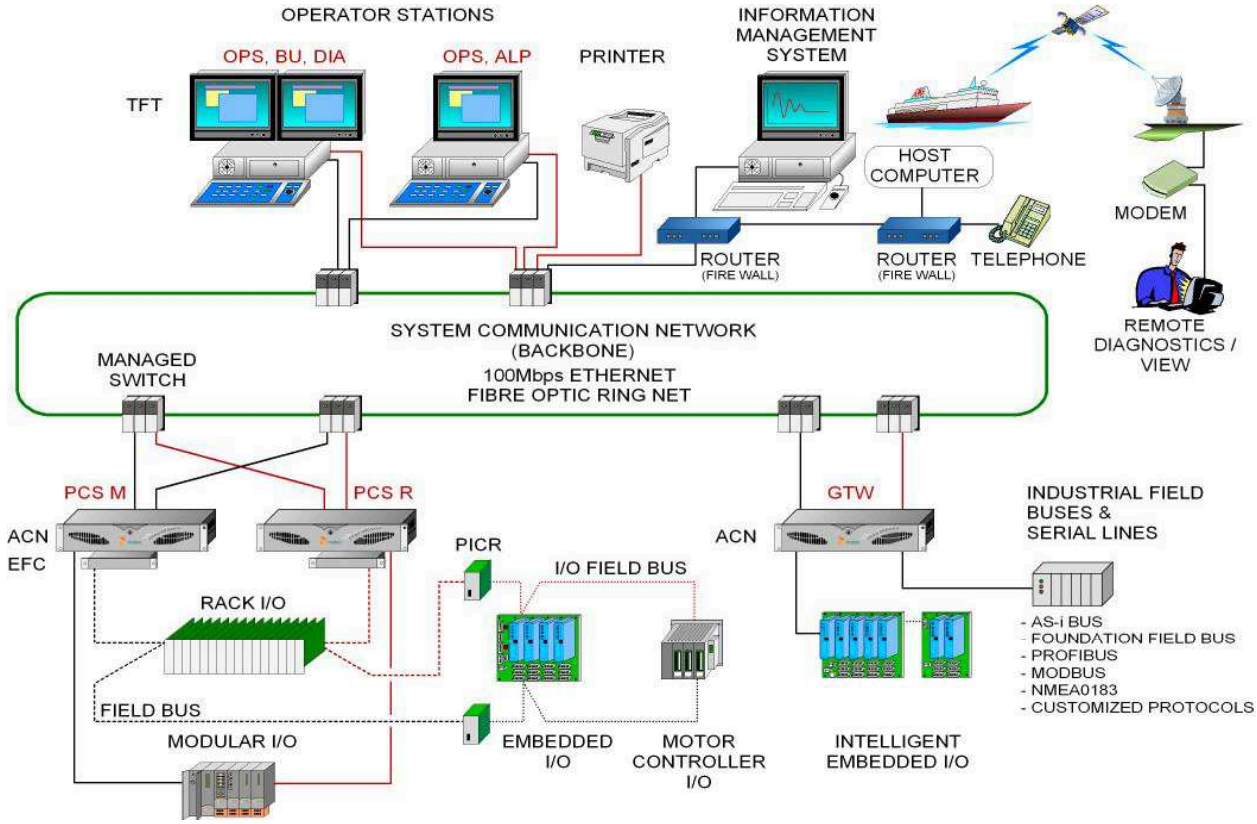

Fig. 13: *SCADA* Overview

Concepts may be summarised in the following table:

Hierarchical Level *(Highest to Lowest)*[27]	**Mode**	**Location**	**Notes**
Direct Control	Manual	Local	Operators control segment locally, visually or by means of local instrumentation
Direct Control	Automatic	Local	A *PLC* or a dedicated control system, installed as part of the process segment, is in control, without human operator supervision.
SCADA	Manual	Remote	Operators control segment remotely, via remote reading of instrumentation.
SCADA	Automatic	Remote	Supervisory computers control process segments, without participation of human operators, except for set point setting.

Table 4: Control Hierarchy, Modes and Location.

Rules specify control requirements basing on their way of classifying systems; same approach will be followed here. This specific approach will show how control systems belonging to different services are interconnected.

1.3.4.1 Main Electrical Power Supply System.

Requirements listed hereunder derive from [**5**], Part 4, Chapter 8. In this section, power distribution function is lumped together electrical power supply, respecting classification society use; in terms of functions and management, in practice, systems basically differ. Many authors treat the two systems as different entities ([**2**], for example), here there is no such need.

Normally Main Electric Power Supply System (and all associated process segments) is remotely and automatically operated, as per owners' technical specification, but it can be remotely or locally and manually controlled too, even though such controlling modes shall be intended as backup modes. Some processes, given their inherent small time constant, such as voltage, frequency, load control and consumer electrical protection, are controlled locally and automatically, by means of direct controllers, named *AVR* for voltage and reactive load, **speed governors** for frequency and active load and **protection relays** for consumer electrical protection; remaining will be managed by the *SCADA*, often termed *IAS*, or *IAMCS*. *SCADA* offers the possibility for the operator to enter commands overriding some automatic functions, in this sense electric power supply system is said to be remotely and manually controlled.

Controls shall accomplish following automatic functions:

- Maintain or immediately restore power for safety, propulsion and steering in case of loss of generators in service. This means that power system shall be equipped with:

[27] Highest priority controls can take over lower priority, whilst the opposite cannot happen.

  - Automatic load shedding or other automatic means to prevent sustained overload of any generator. Load shedding can be actuated tripping or reducing consumer load. If necessary, important consumers[28] may be tripped.
  - Automatic means for starting and synchronising stand by generators if remaining on line generators are not able to permit propulsion, steering and to ensure safety, or there is no remaining generator at all (black out). Fail safe[29] load sharing, within a tolerance of 10% of their actual proportionate value, between generators shall be ensured following suite synchronisation.
- Monitor electric power supply system insulation. In case insulation falls below a certain value, an alarm is sounded to promote maintenance at the earliest convenient occurrence, or the faulty section is isolated. High voltage systems, being exercised with neutral point earthed via a high value resistance, permit rapid and discriminative earth fault location and disconnection, if this is safe to do; low voltage systems instead, being designed as IT system, may tolerate an earth fault for how long as a second earth fault occurs enabling planning maintenance.
- Monitor component power supply, alerting operators in case a certain service is inoperative, or redundancy is lost due to power supply loss.
- Monitor system status, alerting operators if key parameters like power, voltage, frequency, isolation, components temperature, etc, fall outside design tolerances.
- Manage equipment redundancy by starting stand by equipment upon duty failure.
- Ensure discriminative electrical protection so that part of the plant affected by an electrical fault is minimised.
- Prevent wrong operations by means of interlocks. Such interlocks can be software or hardware based, according to level of control. Preventing local and manual dangerous or wrong operations requires hardware interlocks, whilst preventing remote dangerous or wrong operations a software interlock would suffice. Wrong operations may be, for instance, energising transformers from low voltage side, as stated in Section H.301.f, or connecting two systems at different frequencies, as detailed in section H.301.e.
- Optimise generated electrical power according to consumer or operator needs. This means:
  - Maintaining generator readiness conditions, or stand-by conditions (keeping bearings lubricated, monitoring heat exchanger leaking, for instance), and alerting operators in case readiness is lost.
  - Starting, stopping, synchronising and load sharing generators as dictated by actual load conditions (generator load exceeding or falling below predetermined values), alerting operators if actions are not completed successfully in a given amount of time or cannot be completed due to any circumstance.
  - Preventing heavy consumers to connect without having checked actual generating capability is sufficient to support the new load or to drive more load than available at any given time.

[28] Important (secondary essential) services are those services that need not necessarily be in continuous operation for maintaining vessel manoeuvrability, but which are necessary for maintaining the vessel functions. Important electrical consumers are electrical consumers serving important services.

[29] Load sharing failure shall not produce a black out; [**5**] Part 4, Chapter 8, Section 12, Paragraph A.602.

- Enabling operators to decide a minimum or a maximum number of generators to be operated, according to sea state or trading mission[30].

Controls shall be designed to ensure that:

- Failure of any remote or automatic control systems shall initiate an audible and visual alarm and shall not prevent normal manual control.
- Local manual operation is arranged for all essential and important consumers when remote control is arranged from an electronic/programmable system and for all essential consumers when remote control is arranged from outside of the engine room. A local/remote selector switch shall be implemented at the motor starter. Local manual control is available for all generator prime movers and generator circuit breakers.
- There is a unique control position active at any time. Local manual operation shall inhibit remote manual operation and vice versa (manual local operation has higher priority, as already stated, so can take over, but not be active at the same time), so shall local manual operation against local automatic, and so forth.
- Their power supply is common with controlled process segment, so that process segment and its control are available at the same time. Emergency stop, furthermore, if fitted is to act removing power supply; with control power so arranged risk of control action saturation (set to max hard driving actuator when power is reinstated) is excluded. Essential control and monitoring systems shall be provided with two independent power supplies. This applies to both single and redundant control and monitoring systems.
- Prevent wrong operations by means of interlocks. Such interlocks can be software or hardware based, according to level of control. Preventing local and manual dangerous or wrong operations requires hardware interlocks, whilst preventing remote dangerous or wrong operations a software interlock would suffice. Wrong operations may be energising transformers from low voltage side, as stated in Section H.301.f, or connecting two systems at different frequencies, as detailed in section H.301.e, for instance.
- Electronic governors shall have their power supply independent of other consumers and arranged with redundancy type *R0*, or service recovery time zero seconds (*UPS*/*BCP* back up, with storage batteries).

1.3.4.2 Electric Propulsion System.

Requirements in this section are taken from [**5**], Part 4, Chapter 8, Section 12.

Propulsion system includes several process segments, with different controllers, each one interacting with others and with power plant controls; determining whether propulsion system is remotely, locally, manually

[30] Dynamic positioning, for instance, may cause rapid power surges due to rising tide or different circumstances. Accurate position keeping requires fast power dynamics; therefore generator starting time (45 sec for a marine diesel engine) may not be short enough for the purpose. In this case a minimum number of generators are left active, despite their load not justifying it.

or automatically controlled is a matter of definitions. As anticipated in *1.3.2*, propulsion system accomplish the function of moving a vessel with a predetermined minimum speed, therefore controlling propulsion system means controlling its main function, or ship speed, via propeller rotational speed and direction. To accomplish this function several controllers are required, some of them are local, automatic or remote:

- Speed reference generation. This controlling action happens remotely and manually or automatically. Speed reference generators are, in a ship:
  - Operators, via devices called **speed levers** or **joysticks** (one for every propulsor). Speed levers can be automatically assisted to ensure all propulsors receive same speed reference, as opposed to joysticks, which normally are installed as single, combined reference generator[31].
  - Automatic systems:
    - Speed and course pilots. They keep ship speed, obtained by *DGPS*, to a certain reference value, set be operators (speed pilot) or dictated by course schedule (elaborated by a computer), adjusting propeller revolving speed. In this case speed reference (shaft revolving speed) is generated automatically.
- Speed reference selection. Shall control post or speed reference generator be changed; there is an automatic function, initiated by a manual operation that unambiguously transfers command to new control post, which transfers actual speed reference to avoid abrupt change in thrust.
- Speed reference transmission to drive control. This is a common computer data network that may be dedicated (most of occurrences) or shared with *SCADA*. This is not a control function, strictly speaking.
- Drive direct digital control, local and automatic in nature, which translates speed order into a firing sequence for solid state switching devices and suitable excitation current level (in case propulsion motor is synchronous). This controller, in generating firing sequence and excitation current level, ensure that motor nominal torque is not exceeded, and verifies power plant capability before accelerating further; should available power be not sufficient, then no further acceleration is to be produced or, eventually, a deceleration must be actuated. In case of pod propulsion, speed reference is compared against steering angle, producing a limitation should steering angle exceed a certain value. This controlling action happens locally and automatically, given process time constants and calculation burden.
- Auxiliary control, performed by *SCADA*. A certain number of ancillary systems need be activated before rotating shafts: thrust and shaft line bearings need be lubricated, propulsion transformers, excitation transformers, converters and propulsion motors need be connected and cooled, pod bilge needs be emptied, etc. This controlling action takes place remotely and automatically, upon initiation prompted by operator (propulsion start).

It is decided to derive propulsion system control location (local/remote) and mode (manual/automatic) from speed reference generation; propulsion system is, as a whole, remotely and manually or automatically controlled if speed reference generation is set to remote, manual or automatic. Principal control position is bridge.

[31] Joystick permits operators to generate a reference thrust vector by displacing its lever (thrust may be thought as the vector stemming from lever neutral position to lever present position). Joystick computer or software task, if run on a pre-existent computer with ability to generate speed, lateral thrust and heading reference, is to translate this vector into speed reference for propulsors and side thrusters, and heading reference for steering gear.

Controls shall be designed with following features:

- Each propulsor shall have a dedicated and independent speed reference actuation system.
- They shall be so arranged that a single failure in one system or one unit cannot spread to another unit.
- They shall be provided with two independent power supplies.
- A single failure in any control system shall not disable propulsion permanently.
- Only one control post shall be active at any given time.
- Local manual control shall be permitted and be kept independent from remote control system[32]. Failure of any remote or automatic control systems shall initiate an audible and visual alarm and shall not prevent normal manual control.
- Failure of the remote propulsion control system shall not cause appreciable change in thrust level or direction and shall not prohibit local control.
- Thrust shall not increase substantially in case of loss of an actual value signal from a discrete transmitter or loss of a reference value in the system.
- Shaft lines are independently controlled, with or without a common reference.
- Means for emergency stop of propulsion motors shall be arranged at all control locations. The emergency stops shall be independent of the normal stop, and separate for each propulsion line.
- In case remote control of a propulsion drive is arranged for selecting other than the normal speed control mode (e.g. torque or power) the propeller thrust shall not change significantly as a consequence of selecting an alternative operating mode.

Controls shall include the following functions:

- The normal propulsion remote control system shall include means for limiting the thrust levels when there is not adequate available power. This may be an automatic pitch or speed reduction.
- Safety functions installed in equipment and systems for electric propulsion shall not result in automatic shut down unless the situation implies that the equipment is not capable of further functioning, even for a limited time. Automatic reduction of propulsion power is accepted.
- Shutdowns caused by a safety function shall, as far as possible, be arranged with a pre-warning alarm. Automation shall be designed in a manner which ensures that threshold warning of impending or imminent slowdown or shutdown of the propulsion system is given to the officer on watch in time to assess navigational circumstances in an emergency. In particular, system shall control, monitor, report, alert and take safety action to slow down or stop propulsion while providing the officer of the watch an opportunity to manually intervene, except for those cases where manual intervention will result in total failure of the engine and/or propulsion equipment within a short time, for example in case of over-speed. ([**9**] Ch. II-1/31.2.10)
- Critical alarms for propulsion shall be relayed to the navigation bridge and displayed with separate warnings, separated from group alarms.

[32] Local manual control means auxiliary services and speed reference, together with its direction of rotation, can be controlled by an operator from a control post located near the propulsion equipment. Drive control (thyristor firing according to vector control or direct torque control) has still to be accomplished by a direct digital controller.

1.3.4.3 Steering Gear.

Requirements in this section are taken from [**5**], Part 4, Chapter 14.

Steering system is designed to be remotely controlled from the bridge, being local manual control present and with highest priority. As already discussed for propulsion system, control position and mode will be decided following steering angle reference generation, being this the service system is called to provide. Reference is generated remotely and independently per each steering gear, in different ways:

- Manually, by operators (called **helmsmen**), via different devices, such as:
  - Wheels (follow up[33] control);
  - Push buttons or levers (non follow up[34] control);

  Control can be separated (each steering gear being controlled as a separate entity) or combined (all steering gear share the same reference, generated by a common source).
- Automatically, by different systems, such as:
  - Heading pilots (or **gyro-pilots**). Similarly to speed pilots they control ship heading to maintain a given reference adjusting steering angles as necessary.
  - Course pilots (or **track pilots**). They control ship heading to follow a predetermined course, and adjust steering angle to follow generated heading reference.
  - Joysticks. Steering gear reference is a result of a calculation to execute action input by an operator.

  In this circumstance control is combined only.

Steering system process segments are quite similar in terms of function to propulsion system; they are:

- Steering angle reference generation, remote and manual or automatic;
- Steering angle reference selection and transmission; unambiguous selection procedure is initiated by operators and reference is transferred automatically before transferring actual control. In this case reference transfer is only important in case of follow up controls.
- Reference actuation.

Controls shall be designed with following features:

- Each rudder shall have a dedicated and independent steering angle actuation control system, together with relevant instrumentation.
- They shall be so arranged that a single failure in one system or one unit cannot spread to another unit.
- Systems shall be provided with two independent power supplies
- Failure of remote and/or automatic control systems shall initiate an audible and visual alarm and shall not prevent normal manual control.

[33] Follow up control is that control designed in such a way that rudder actual position is generated; this means if wheel is spring loaded and returns in zero position, then rudder stock returns to zero position (central) as well.

[34] Non follow up control is that control designed in such a way that rudder actual variation of position is generated; in this case no signal equals to rudder stock remaining in the position it was left before, no movement in either direction.

- Steering gear circuits shall only trip upon short circuit. However if additional over-current trip is used, the release current shall be at least 200% of rated, with a time delay of minimum 60 seconds. An overload alarm shall be activated when the current exceeds full load working current.
- Protective shutdown functions associated with the steering gear shall be limited to those necessary to prevent immediate machinery breakdown. Any protective shutdown shall initiate an alarm.
- All alarms associated with steering gear faults are to be indicated on the navigating bridge and in machinery space.
- Rudder angle indicating system is to be independent of any control system. Rudder angle indicating system shall be so arranged that a single failure in power supply or anywhere in the indicating system does not cause loss of rudder angle indication on the bridge.
- Power shall be taken from a dedicated separate circuit supplied from a steering gear power circuit from a point within the steering gear compartment, or directly from switchboard bus bars supplying that steering gear power circuit at a point on the switchboard adjacent to the supply to the steering gear power circuit.
- Every steering gear is controlled independently from others.

Controls shall include the following functions:

- Local disconnection of any remote control system.
- Control system shall be capable of being brought into operation from a position on the navigating bridge.
- Steering angle feedback failure is to cause no actuation. In other words, should the steering angle feedback be lost, controller shall act as non follow up.
- Steering angle limitation. This limitation shall cover both the maximum achievable angle, that cannot exceed rudder stock actuator limits, and the rate of turn that can take place as a consequence of the order; as the ship speed increases, the speed at which the rudder travels or the maximum travelled angle shall be consequentially reduced so that the resulting rate of turn remains within acceptable limits.

1.3.4.4 SCADA.

Requirements described in this section are taken from [**5**], Part 4, Chapter 9, Section 4, mainly. Local (direct) control systems have been described in their relevant sections; here subject of examination is the computer based system, *SCADA*, which, in addition to fulfil process segments control task itself, coordinates all local controls to obey to an agreed strategy or goal. In facts, its main function is providing system management, as direct control functions can be accomplished by a dedicated hardware, in case.

In previous paragraphs *SCADA* was mentioned relatively often, telling about its importance in supporting functions that are either requested as mandatory or considered important for ship mission.

Since early 2000 computer based systems[35] have been successfully used for safety purposes; to that extent an additional set of rules, not mentioned in the following, need be obeyed by; for the purpose of this work the computer system acting as *SCADA* does not implement safety related functions[36].

SCADA main functions are, as anticipated in*1.3.4*:

- Performing automatic control actions directly and/or relaying information to local direct controls so that they can perform control actions in accordance with a decided strategy. Control actions shall be such that equipment parameters are stably kept within design limits.
- Actuating control actions decided by operators in such a way that:
  - Operators are kept aware of the effect of their action,
  - Dangerous actions are blocked by suitable logic checks,
  - Conflicting actions are avoided by unambiguous definition of active control post. Control shall only be available on workstations from where control is intended and access shall be provided via a command transfer system.
- Verifying that planned control actions are timely executed.
- Attracting operators' attention in case of process parameter deviation from specified design values or failing to execute control actions in a timely manner. This function is often termed **alarm handling**, and must obey to international standards, such as *ISA* 18.2 or *EEMUA*.
- Giving operators awareness upon system actual status, via *HMI*s. This awareness is intended to enable anticipation, via historical data analysis, of impeding failures. In this respect, any modern monitoring system provides trending tools and stores data collected over a long period for offline analysis (preventive maintenance, [**6**]).

System shall be designed with following features:

- There shall be one named body responsible for the integration of the total system. This body shall have the necessary expertise and resources enabling a well managed integration process.
- Where a computer based system is part of an essential function, back-up or emergency means of operation shall be provided, which to the largest extent possible shall be independent of the normal control system, with its user interface.
- Minimum performances to be granted are shown in Table 5:

Data sampling for automatic control purposes (fast changing parameters)	0.1 s
Data sampling, indications for analogue remote controls (fast changing parameters)	0.1 s

[35] Purposely, no distinctions are made between computer based systems and *SCADA*. This is due most to the fact that the word "computer" appears vaguely defined. In most control applications a computer is a device consisting of a *CPU*, a non volatile memory hosting operating system and data, network and *I/O* devices; in this context a *PLC* can safely be considered as a computer, and therefore any control application relying on a *PLC* can be considered a computer based control system. Consequently, a *SCADA* can only be based on *PC*s or *PLC*s, therefore is a computer based system.

[36] Safety has a twofold meaning, most of times. In this framework both most common meanings, i.e. protecting machinery and personnel, are considered. *IPS SCADA* does not protect machinery and personnel integrity; machinery integrity relies upon their direct controls and electrical protection relays, personnel integrity relies upon dedicated, eventually computer based systems.

Other indications	1 s
Alarm presentations	2 s
Display of fully updated screen views	2 s
Display of fully updated screen views including start of new application	5 s

Table 5: *SCADA* Minimum Performance for Data Sampling and Presentation.

- Resilience to single fault. A single fault in any active component shall not impair system functionality. In this respect it is possible to affirm *SCADA* has *R0* redundancy. Fig. 13 gives a graphical overview of this.
- The integrity and autonomy of each network segment[37] within an integrated system shall be secured with appropriate network components, e.g. switches or routers. It shall be possible to protect each segment from unnecessary traffic on the remaining network, and each segment shall be able to work independent and with necessary operator interface.
- In a network integrating control and/or monitoring systems all network components controlling network traffic and nodes communicating over the network shall be designed with inherent properties to prevent network overload at any time. This implies that neither nodes nor network components shall be able to generate excessive network traffic or consume extra resources that may degrade network performance. The performance of the network shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.
- Cables and network components belonging to redundant networks shall be physically separated by separate cable routing and installation of network components belonging to the redundant network in separate cabinets, power supply to such units included.
- It shall be possible to maintain local control of machinery independent of network status. This may imply that essential nodes hosting such control functions shall be able to work autonomously, and with necessary operator interface independent of the network.
- Any powered network component controlling the network traffic shall automatically resume to normal operation upon restoration of power after a power failure.
- Field instrumentation belonging to separate essential[9] process segments shall be mutually independent. When local manual emergency operation of an essential process segment is required, separate and independent field instrumentation shall be provided for the purpose.
- Redundant units shall be provided with independent power supplies.
- Self check capability of detecting following failure types:
    - Loop failures, both command and feedback loops (normally short circuit and broken connections).
    - Earth faults.
    - Communication errors.
    - Computer hardware failures.
- Possibility of disengaging remote automatic control at any time.

[37] A segment is a specially-configured subset of a larger network. The boundaries of a network segment are established by devices capable of regulating the flow of packets into and out of the segment, including routers, switches, hubs, bridges, or multi-homed gateways (but not simple repeaters).

- Where indication of the automatically controlled parameter is required, the sensor for indication shall not be common with the sensor for feedback to the automatic control.

System shall include the following functions, in addition to what already mentioned in *1.3.4.1*, *1.3.4.2* and *1.3.4.3*:

- Significant alteration of process equipment parameters shall be avoided when transferring control from one location to another or from one means or mode of operation to another.
- Start-up and restart shall be possible without specialised system knowledge. On power up and restoration after loss of power, the system shall be restored and resume operation automatically.
- Unambiguous command transfer between stations, in some special cases of vessels.
- Password protected access to some important functions or set points.

1.3.5 Safe Return to Port.

This additional set of requirements is created with the intention of enriching anticipated fault scenarios ship borne essential systems are to stand, along with associated required performances. It is in fact a widening of the statutory dependability related requirements and, as such, to be complied with, together with all other requirements discussed earlier. Three new fault scenarios are added[38]:

- Flooding of one watertight compartment below bulkhead deck.
- Fire in a space protected with fixed fire extinguishing system. In this case, fire is assumed to have spread to the nearest A class boundaries[39], within the same space of origin.

[38] For the purpose of assessing the ship systems capabilities, fire and flooding casualty may be considered as not occurring in the same time.

[39] ''A'' class divisions are those divisions formed by bulkheads and decks which comply with the following criteria:

- they are constructed of steel or other equivalent material;
- they are suitably stiffened;
- they are insulated with approved non-combustible materials such that the average temperature of the unexposed side will not rise more than 140 deg. C above the original temperature, nor will the temperature, at any one point, including any joint, rise more than 180 deg. C above the original temperature, within the time listed below:
  - class ''A-60'' 60 min
  - class ''A-30'' 30 min
  - class ''A-15'' 15 min
  - class ''A-0'' 0 min
- They are so constructed as to be capable of preventing the passage of smoke and flame to the end of the one-hour standard fire test.

Decks are considered as class A boundaries. [**9**], Chapter 1, Regulation 2, Section 2 refers.

- Fire in a space not protected with fixed fire extinguishing system. In this case, fire is assumed to have spread to adjacent (sideways and one deck upwards) spaces up to the nearest A class boundaries, which are not part of the space of origin.

It can be seen now fire and flooding are not regarded as common fault generating causes any more, as far they are limited in extension; the single fault principle is now abandoned, in favour of a more realistic interpretation of the effects of listed casualties. Still it is assumed fire and flood are different causes, which cannot happen at the same time.

Fault scenarios and their impact on system subject of this work are better characterised through following statements, extracted from [**9**], Chapter II-2, 21, according to interpretation given in [**10**] and [**11**]:

- Electrical cables are considered to continue to work in a space affected by a flooding casualty provided the end of the cables are located outside the flooded compartment or any connections, joints and devices have a degree of protection IPX8 (head of water expected at their location for a period not inferior to that estimated for the safe return to port).
- Fire resistant cables complying with *IEC* 60331-21, *IEC* 60331-31 or EN 50200 passing through and not serving spaces are considered operational after a fire casualty, provided they have no connections, joints or equipment connected to them within the space affected by the casualty.
- Installation of these cables should be made to support their survival in a fire casualty and during its fire fighting.
- Trunks closed at all boundaries constructed to "A-60"[39] standard and containing ducts, cabling and/or piping are considered operational when passing through a space of origin of a fire or flood casualty.
- A steel shaft line passing through a space affected by a flooding or fire casualty, may be considered operational if it is enclosed in a protected tunnel or alternatively if:
  - in the flooding case it can be shown that it can operate under water, and
  - In the fire case it is protected by a dedicated water based fire extinguishing system. A shaft line passing through a Category "A"[40] machinery space is not to be considered operational.
- Manual control at local positions can be accepted, provided adequate communication is arranged and it is demonstrated that the loss of any control and monitoring system does not prevent or impair any such manual/local control of the propulsion and electrical power supply systems.
- Systems for internal fill, transfer and service of:
  - fuel;
  - other flammable hydrocarbons; or
  - any fluid that may be flammable or dangerous if heated to a very high temperature (both within the pipe and on going through pumps, orifices or other equipment), should not be considered operational within spaces affected by a fire casualty.

[40] Machinery spaces of category A are those spaces and trunks to such spaces which contain:

- internal-combustion machinery used for main propulsion;
- internal-combustion machinery used for purposes other than main propulsion where such machinery has in the aggregate a total power output of not less than 375 kW;
- any oil-fired boiler or oil fuel unit.

[**9**], Chapter 1, Regulation 3, Section 17 refers.

Essential systems are required to continue delivering a reduced service under those newly defined casualties. Reduced services are described hereafter.

Propulsion:

- For the fire casualty, the ship should be able to maintain a speed of min 6 knots while heading into Beaufort 8 weather and associated sea conditions. All auxiliaries in services are considered to have service factor equal to 1 and to function all at the same time (diversity factor 0). Ship shall be able to travel 2000 nautical miles, or 3704 km, under the casualty.

Electrical system:

- Electrical power and local control for steering gear operation at full capacity shall be granted.
- Electrical power for following navigation systems shall be granted (on the bridge or on another location, should the bridge be disabled by fire):
  - barograph, hand wind-speed meter, and suitable devices to receive weather forecast maps
  - compass (magnetic or gyro) and bearing repeater
  - nautical charts and publications or ECDIS
  - receiver for a global navigation satellite system (e.g. GPS)
  - rudder, propeller thrust and pitch indicators (or means of communication)
  - 9 GHz Radar
  - automatic identification system (AIS)
  - whistle
  - navigation lights
  - Daylight signal lamp.
- Electrical power for public address systems, arranged as general alarm systems, shall be ensured in the main vertical zones not affected by the casualty.
- Electrical power for charging communication or other portable devices relevant to the emergency in progress shall be available in more than one main vertical zone.
- Electrical power and local control for remaining fire pumps (one only is lost, according to casualty characterisation).
- Electrical power and local control for ballast pumping system and all associated equipment for its operation shall be ensured in spaces served by the system and not directly affected by the casualty.
- A minimum of one toilet per 50 persons or fraction shall remain operational[41]. Grey and black water is accepted to be disposed into the sea.
- A minimum of 3 litres per person per day drinking water shall be available[42]. Additional water for food preparation and hygiene may need to be provided.
- Electrical power for hospital and equivalent areas shall be granted.
- Electrical power for basic air conditioning (heating and/or cooling, depending on ship's trading route) in safe areas shall be granted.
- Electrical power for light and ventilation in safe areas shall be granted. Ventilation volume should be available as a minimum of 4.5 m^3/hour and person.

[41] In modern ships toilets are based on a vacuum pipe system; vacuum is generated by electrical blowers. Such sanitary system is then, electrically actuated and it is a user of the electrical system.

[42] Potable water circulating pumps are electrically actuated in modern ships. Those pumps are needed to transfer water from tanks to taps, via a manifold.

- Electrical power for internal fill, transfer and service of fuel oil to active propulsion and power generation equipment.

IAS:

- Flooding detection systems are accepted to be lost only in spaces directly affected by the fire casualty and in other spaces in the same compartment that are part of the same system section provided all other detectors remain operational in any other compartment served by that system section.

Dependability requirements, in terms of tolerance to described casualties, are consequently reformulated.

- Manual action to promote system recovery and use shall be thoroughly assessed (in light of a possible reduced access), even though is accepted. This requirement encourages use of essential systems capable of automatic recovery (remotely and without operators' assistance) after the casualty. Computer based integrated control and monitoring systems complying with these requisites shall therefore be designed for high redundancy, fault tolerance and, above all, remote control.
- Physical separation shall be enforced to the level of a watertight zone (flood casualty) or space (fire casualty[43]). Two duplicated components belonging to an essential system shall not be located in the same compartment (flood casualty) or space (fire casualty).
- Water tightness level shall be raised from 4 (rain resistant) to 8 (immersion resistant).
- Electrical power supply cables for essential systems crossing more than one compartment shall be fire resistant.
- There must be at least two control stations (for remote controlled systems) located in spaces so that a fire casualty cannot affect both at the same time. This requirement is specially stressed for bridge, as there shall be a "second bridge", with at least equipment listed earlier in this section, and with visibility of all objects of interest for navigation such as ships and lighthouses, in any direction
- Propulsion system shall be arranged in a way shaft lines are located in compartments or spaces not simultaneously affected by a fire or flood casualty; any shaft line shall have sufficient power to propel ship at the requested speed in assigned weather conditions.
- Power stations shall be arranged in spaces or compartment so located not to be simultaneously affected by a fire or a flood casualty, and have sufficient power to ensure essential services listed above.
- Communication with public and emergency management teams shall be granted by decentralised systems, without one single central point (telephone exchange, for instance). In general all systems subject to this rule shall be designed as a "network" of independent servers, able to communicate in any casualty situation described above.
- Etc.

[43] The largest space affected by a fire casualty in accommodation space is indeed an entire main vertical zone.

2. Dependability-Oriented Design: Promoting Factors, Definitions and Theory.

2.1 Promoting Factors to Obtain a Dependability-Oriented Design.

In this chapter the meaning of the word "dependability" is further characterised, in order to allow appreciating all aspects. Now suffice to say that a dependable system delivers the correct service customers expect with an acceptable trust, for an agreed period of time, under certain circumstances.

2.1.1 Shipyard Perception.

Shipyards, as contracted suppliers, have several obligations, stated in the ship building contract, regarding dependability:

- They must provide the service classification societies expect. Expectations are detailed in designated classification society rule book, widely discussed in preceding sections. Shipyards are to interact with class following a defined procedure, called **plan approval**; during this phase design is assessed against rule requirements to provide a first, but not final, compliance certificate.
- They must provide the service customers expect. Expectations are detailed in a document termed **technical specification**, which describes vessel systems way of functioning, quite often using "soft concepts", such as "*A centralized wheelhouse and engine room control system is to be provided for reliable operation of the main propulsion machinery and the ship from the wheelhouse with an unattended engine room*"[44]. Technical specification complements rule requirements, with a lower priority in case of conflict.
    - Technical specification needs be unambiguously understood. In the example mentioned, the meaning of "*reliable operation*" needs be clearly stated.
    - Details emerging from technical specification analysis shall be elaborated into several sub-specifications, or **system specifications**, to be released to sub-contractors. Shipyards are not capable of producing all needed systems in house; they act as **system integrators**, buying systems from sub-contractors and engineering them to deliver ship requested service. System specification shall, furthermore, include environmental circumstances and additional warranties, if any.
    - Designated sub-contractors shall share with shipyards their product behaviour and requirements, so that arrangements are made to seamlessly accommodate them to enable successful integration. More details about typical ship design flow can be found in [**12**].
- They must provide the expected service for an agreed period of time. This means that operating conditions for systems are to be granted (room temperature for electronic equipment, for instance, or correct operating points for pumps and fans, in terms of flow and head). Access for maintenance and appropriate personnel working conditions are to be listed here.
- They must provide the expected service under specified circumstances. Those circumstances might be thought of sea water temperature, upon which heat management depends upon; ice presence in case of arctic trading, failure scenarios such as casualties described in *1.3.5*; etc.

[44] This sentence is extracted from a cruise ship technical specification.

Shipyards are to prove fulfilment of these requirements by means of a series of tests and trails, during which agreed circumstances are reproduced. Failing to prove requirement fulfilling may cause heavy financial consequences, to a level that shipyard may go bankrupt and suspend operation. Shipbuilding payment structure is often such that shipyards are heavily exposed [**13**]; payment is made by a number of progress payments occurring when certain milestones have been passed. These milestones could include: laying of the keel; completion of the hull; installation of engines, tanks and generators; installation of the superstructure; completion of interior finishing; completion of sea trials; and expiry of a trouble-free period. It is easy to note shipyards bear purchasing cost until progressive payment is installed (and not necessarily instalment covers the full expenditure); this period may least months. Propulsion equipment, for instance, is delivered approximately when the first block is laid, and paid in fully once performances are proven, i.e. after sea trials; in between these two moments in time a year can pass.

Warranty period has an inherent cost as well. All failures discovered in this period must be rectified with vessel in operation, exploiting opportunity windows that may entail stressing working conditions, such as night shifts or at a short notice. In most cases external personnel, with all associated contracting costs, is required. Warranty may erode project margin if dependability is not achieved.

2.1.2 Sub-contractor Perception.

Sub-contractors obligations and liabilities insofar as dependability is concerned are:

- Providing components and/or systems fit for purpose (i.e. suitable for the intended environment, capable of performing assigned functions and of delivering expected performance) and complying with system specification, extended by shipyards.
- Replacing defective components during the warranty period. Warranty period on components begins when operation starts; repetitive failures make so that warranty obligations are renovated.
- Assisting shipyards in creating all requested enabling conditions for supplied system to operate, and offering information about supplied system behaviour.
- Assisting shipyards during warranty period.

The capability of proving, before shipyards (ultimately, shipyards are sub-contractors customers), owners and classification societies, that a design is compliant to specification and rules requests shelters from heavy reworks and/or legal claims after trial session, when faults and failures are discovered, but time to delivery is usually falling short. The liability deriving from a non-compliant supply is usually limited to the price paid for the system in subject; no consequential damages can be claimed for this occurrence.

Post-delivery issues need handling by both shipyards and contractors; relevant costs can erode revenue margin, exposing both institutions to financial risks. Financial risks nowadays need be properly insured, thus generating additional costs.

2.1.3 Classification Society Perception.

As anticipated classification societies carry liability, albeit limited, with respect to losses generated by negligent actions and/or omissions; [**5**], Part 1, Chapter 1, Section 5, Paragraphs from A.100 to A.400 refers. Inasmuch as design is discussed, apparently there are no liability provisions to cater for lack of completeness, or a casualty not mentioned in the rules that causes a failure that is explicitly stated as not tolerable by them; quite often classification societies recur to "soft statements", like the one discussed in *2.1.1*, in order to "manage the unexpected". To the extent of liability, this approach may be seen as a further limitation, leaving risks generated by any uncovered scenario to shipyards and owners.

Classification certificates are widely relied upon by all sectors of the maritime industry as an indication that a vessel is reasonably fit for its intended use. Flag States can, and very often do, authorize classification societies to inspect and carry out statutory certification duties of the ships on their register. Port States rely on classification societies to confirm that a vessel is in class before allowing it transit into their waters. Charterers, ship owners and *P&I Clubs* rely on them to confirm that a vessel complies with international conventions and safety standards. Since classification societies also perform surveying and damage investigation, they are also involved with insurers, owners and charterers in carrying out these functions. Cargo owners and potential purchasers may also rely on class certificates and surveys when deciding to use or buy a particular ship

It can be observed that main damage classification societies suffer from lack of dependability is related to their reputation, and capacity to administer responsibility extended by governments and institutions. Should a classified ship not being able to deliver the expected service, which is, in this framework, ensuring safety of personnel, environment, cargo and vessel itself; the classifying society would probably be considered as unreliable and all revenues coming from their services to entities listed above would cease.

2.1.4 Owner Perception.

Ship owners are in the end bearing most liability for damages caused by their ships to personnel, environment, cargo and other vessels or possessions. Different legal bodies impose different liabilities:

- International conventions define ship owners' obligations imposing strict liability to pay compensation to persons (crewmembers, dockworkers, passengers, others) suffering damage (personal effect, personal injury, illness) or loss (life, personal effects, property) involving their ships. This means that ship owners will be required to pay compensation for damage caused by their ships, without the need for the claimant to prove that the damage was caused by recklessness, negligence or acts committed by the ship owner with intention to cause damage. This development allows persons suffering loss to claim compensation without having to resort to lengthy litigation to prove fault or negligence on the part of the ship owner. These conventions also require ship owners to be insured to cover their liabilities and provide for "direct action" that is, allow claimants to claim damages directly from the ship owner's insurer.
- International conventions define ship owners' obligations imposing strict liability to pay compensation for damages to environment, such as pollution.

- Shipping contracts define ship owners' obligations imposing strict liability to pay compensation if cargo is lost, damaged or late delivered.
- Ship owners are to bear the consequential damages of an underperforming ship in excess of its price. Ship owners order ships with a consolidated work load, and such work load implies liabilities, stated in those contracts, in case it cannot be undertaken. To clarify the concept, suffice to say the price for a *PLSV* very seldom exceeds the price of its cargo (submarine pipe or cable and associated laying system), and the total project budget does exceed the cargo value by orders of magnitude; an incapacity in position keeping within certain accuracy, and therefore incapacity in trading, can cause losses by far superior than the vessel price.
- Ship owners are to bear the consequential damages of a late delivery of the ship. Liabilities reside in the fact that contracts cannot be undertaken at the expected time.

Ship owners are, in the end, the party having the most interest in achieving dependability. Dependability generates revenues by continuing trading, albeit in unfavourable circumstances arisen from a failure, and avoids costs derived from liabilities and relevant insurance.

2.2 Promoting Factors to Demonstrate Dependability.

Positive demonstration of dependability reduces liability derived from insurance, for instance, as dependability reduces the probability that certain service failures cause damages or losses. This reduction in liability generates in turn revenues.

At the moment, dependability is proven by means of tests and trials: fault scenario is reproduced and vessel systems reaction is recorded for comparison against expected outcomes. This is quite an expensive way to achieve dependability demonstration, as it entails:

- a remarkable proportion of engineering in identifying tests and trials to be performed, involved systems and components, together with relevant fault scenarios, expected outcomes and criteria to determine success;
- a remarkable proportion of management in organising and manning decided test and trials, and collecting results in an appropriate format.

Safety during testing need be ensured, as outcomes, even though anticipated, may not necessarily happen, and a recreated failure may develop into hazard for personnel, environment, cargo and ultimately for the vessel itself. Safety measures require additional management and planning.

Testing activity mainly rely upon engineering experience, rules requirements (with due consideration to "managing the unexpected") and system knowledge; there is no systematic approach capable of granting completeness (all possible failures have been considered) and accuracy (all outcomes derived from a failure have been considered). This is a direct consequence of the fact that testing is a resource-intensive activity, in terms of number of employed persons, and their skill set, so not all failures are recreated, due to budget and time limits.

The possibility of generating a positive, accurate and complete dependability assessment must be sought in simulation, rather than physical testing; the reward in this effort is a consistent reduction in physical tests

and the anticipation of outcomes that permits early elimination of unwanted behaviours and safety awareness during mandatory physical tests. Simulation requires an appropriate system model and computational time that is less expensive and generally more available than qualified manpower. Accuracy and completeness relies upon system model, therefore modelling shall absorb the qualified human resources. System model is central in this work, and is treated in depth under *2.4.1*.

2.3 Definitions and Taxonomy.

Dependability theory has only recently been systematically developed as regards to terminology and contents. Here such terminology and contents are reported, because they are quintessential to theory application; words are only of interest because they unequivocally label concepts and enable ideas and view-points to be shared.

2.3.1 Basic Definitions.

A **system** is a set of components grouped together into a single entity with the purpose of delivering a service [**12**]. A system can also be seen as an entity interacting with other entities, i.e. other systems, including hardware, software, humans, and the physical world with its natural phenomena. These other systems are the **environment** of the given system. The system **boundary** is the common frontier between the system and its environment [**6**]. An *IPS* is a system that delivers a service, electrical power and propulsion, and interacts with other systems (thermal management, for instance), humans (often called operators, personnel, crew, etc.), and the physical world with its natural phenomena (weather and sea conditions, sea water temperature, etc.). *IPS* boundary is defined as the set of:

- User terminal boards, where control and power cables are connected;
- Electrical sockets;
- Stern-tube, through which shaft passes;
- Prime mover flanges, to which alternators are connected;
- Heat exchanger flanges, to which thermal management system pipes are connected;
- Local pushbuttons, speed levers, gauges, metres, HMI screens, etc., through which operators interact with the *IPS*;
- Hull, supporting all devices;
- Instrumentation wells and pockets;
- Etc.

System service is the set of operations performed by a system in favour of its user(s). System service is further specified by assigning it a **function**, described in technical specification, which is what the system is to objectively do in favour of its users, and a **behaviour**, or the set of operations users perceive as being

done by the system [**6**]. The two definitions can be merged saying that system behaviour corresponds to system function as perceived by users.

The service is correct if behaviour meets user specifications; otherwise, the service is not correct due to a fail in executing one (or more) operation [**12**].

System structure is what enables the system generating its behaviour [**6**]. Structurally, a system is composed of a set of constituents interconnected with the purpose of interacting to deliver a service; each constituent may be in turn a system itself, etc. The structure is considered fully defined when all constituents are considered **atomic**: any further internal structure cannot be discerned, or is not of interest and can be ignored. An atomic constituent is termed **component**. **System total state** is then defined as the set of its components state [**6**]; it is possible to further define system **external state** as the set of states perceivable by users at the **service interface**, and system **internal state** as the set of states not perceivable by users.

An example illustrating these concepts may be found in the synchronising function (more details are discussed in *3.1.3.3*):

System State	Internal	External
Bus bar voltage	Yes	Yes
Incoming generator running at rated speed	Yes	No *HMI* reports frequency only, not that rated speed has been achieved.
Incoming generator at rated voltage	No	No.*HMI* reports generator voltage only, not the fact that rated voltage is reached.
Speed control in droop mode	Yes	No. Droop state is masked during synchronisation.
Synchroniser is ready	No. This state is not monitored	No. Not being an internal state, it cannot be shown on the interface.
Synchroniser active	Yes. *IAS* activates it by means of a dedicated signal	Yes. A text, “Synchronising”, is displayed on *HMI* screen.
Synchroniser speed pulses	Yes. Directed to speed governor	No
Synchronisation reached	Yes. It enables closing signal to reach closing coil.	No
Closing signal active	Yes, *IAS* keeps it active during synchronisation process.	No
Breaker closed state	Yes	Yes
Synchroniser is deactivated	Yes	Yes. “Synchronising” text is removed
Speed governor set to isochronous	Yes. Circuit breaker closed state is relayed to speed governor.	No

Table 6: Example of Function and Behaviour.

Function objectively does sequentially all steps listed in Table 6; users perceive only a part of them, via the *HMI*. More in detail, users perceive that synchronisation is in progress and that synchronisation is

successfully completed, observing circuit breaker status. Following definition created earlier, *IPS* has delivered one expected service, synchronising, if a running and excited generator is closed on an active bus.

Steps mentioned in Table 6 are indeed system states, as they represent component characteristic (of being active, standby, at rated speed, etc.) that may change due to operation. Some states are internal, used by components but not shown at system interface, some are external, shown at system interface to promote user awareness, and some are undetected.

Different structures can support the same behaviour. If we consider *IPS* function is to generate electricity, this can be obtained with two different structures, as shown in Fig. 2 and Fig. 4. Number of external states may vary according to level of monitoring, and so forth.

2.3.2 Threats.

Threats are those events causing system stopping delivery its intended service, or the system function and its associated system behaviour. Threats are classified into three main categories:

- **Failures**. A failure is a deviation from correct service, described by function and behaviour. A service fails either because it does not comply with the functional specification, or because this specification did not adequately describe the system function. A service failure may as well be seen as a transition from correct service to incorrect service. The period of delivery of incorrect service is a service **outage**, and the transition from incorrect service to correct service is a service **restoration** [**6**].
- **Errors**. An error is a deviation of a state from its intended and correct value, which is the value assumed when system delivers the correct service. Since a service is a sequence of system external states, a service failure means that at least one (or more) external state of the system deviates from the correct state value; that deviation is an error ([**6**] and [**12**]). Not all errors cause failures, only those affecting external states.
- **Faults**. A fault is the adjudged or hypothesized cause that produces an error or a failure. A fault is **active** when it causes an error, otherwise it is **dormant** [**6**].

There is an apparent causal link between those categories: faults cause errors (an error implies a fault, but vice versa may not be true) and errors failures (a failure implies an error, but vice versa may not be true). Furthermore, the causal link may be seen as a recursion: a failure may generate a fault (in a different system), which in turn generates an error (in the same new system where the fault is localised), which generates a subsequent failure. Examples are several; in case under discussion a fire or flood casualty is a classical example, but thermal management is not to be forgotten: a failure of the air conditioning system may cause an *IAS* hardware fault, for instance, which may lead to a computational error or a wrong output activation, which may lead to a system failure in return.

The definition of fault and failure marks an important point: in classification society's point of view faults and failures are synonyms, in the dependability theory they have different meanings, concerning different entities (faults are related to components, as opposed to failures, related to systems), connected by a causal link.

When systems perform a set of several functions, failure of one or more functions may leave the system in a **degraded** mode. System, albeit affected by a failure, may still deliver a subset of functions to the user. In different words, system is said to have suffered a partial failure, but it continues delivering a partial service. Some of such modes, for an *IPS*, have been already introduced:

- **Emergency mode**. This mode is entered when main electrical power supply is out of order.
- **Abandon ship**. When either the main and emergency electrical power supplies are not available, or ship has suffered a casualty exceeding limits set forth by [**9**], Chapter II-2/21

2.3.2.1 Taxonomy

In this paragraph concepts of failure, error and fault exposed before, are further subdivided in classes, for ease of finding an accurate and comprehensive definition. Definitions reported in the following are not yet an international recognised standard, but are widely agreed within the community studying dependability; definition set is regularly maintained and promoted by an international board, even though not fully consolidated yet. They are for this reason considered in this work as a de facto standard, being the closest document to it.

System life cycle can be subdivided in three main periods or phases [**6**]:

- **Development**. During this phase system is conceived, designed and tested.
- **Use**. During this phase system delivers its intended service to users.
- **End of life**. During this phase system is decommissioned and disposed of.

Those phases offer a first classification criterion: time. These time subdivisions are marked with formal acts:

- Vessel delivery (from development to use). Delivery implies a fundamental shift in responsibilities: owners, accepting delivery, state shipyard have fulfilled their contractual obligations (but not warranty obligations) and release a corresponding expenditure in favour of shipyard. Owners have, after delivery, all responsibilities described in paragraph *2.1.4* (and more); shipyard had same responsibilities before that moment. The importance of that moment in time is easily appreciable and will be retained here.
- Vessel cancellation from international registers (*IMO*) (from use to end of life). From that moment on ship is removed from classification registers and therefore not allowed to trade any more. Insurance is suspended.

A further classifying criterion used in the text is viability. A failure will be defined as **partial** if it does not prejudice project completion, **fatal** if it does.

Failures may occur during any phase, and according to the phase they occur they can be conveniently be classified in development failures and use failures.

Development failures can be further classified in two main categories:

- **Budget failures**. A budget fatal failure happens when financing is no longer available to complete the project [**6**]. This is quite typical in shipbuilding given its financial exposition, as explained in *2.1.4*. Budget failures can be partial, thus leading to a budget **overrun**, causing revenue erosion (in

this case shipyard caused the failure by, for example, incorrectly estimating costs), or **specification downgrading** (in this case owners are responsible for the failure, specifying a product out of their financial capabilities).

- **Schedule failures**. A schedule failure happens when delivery schedule slips to a point in the future where the system would be technologically obsolete or functionally inadequate for user's needs [**6**].

Causes of development failures can be multiple:

- Incomplete or defective specification,
- Insufficient design management, producing poor design if compared to specification requests, too many design changes initiated by poor conceptual engineering, etc.
- Insufficient project management and consequent poor design or specification change management,
- Etc.

Use failures can be further classified in four main categories or viewpoints [**6**]:

- **Failure domain**. This class can be further subdivided in two main sub-classes:
  - **Content failure**. This kind of failures is related to information content; a content failure happens when information delivered at the service interface deviates from implementing system function. Classification requirements and technical specifications report several examples of requirements intended to avoid or discover content failures: [**5**], Part 4, Chapter 9, Section 4, Paragraph B, for instance, requires instrumentation loops be monitored in essential control systems; [**5**] Part 4, Chapter 1, Section 4, Paragraph A details which information is required, as a minimum, for controlling remotely propulsion system; etc.
  - **Timing failure**. This kind of failures is related to the time the information is made available at system interface, and the duration of it; a timing failure happens when information comes late or early and, as a consequence of this untimely delivery, system suffers a failures. Classification requirements and technical specifications report several examples of requirements intended to avoid or discover timing failures: [**5**], Part 4, Chapter 9, Section 4, Paragraph A.500, for instance, specifies required maximum information collection and display time, *HMI* refresh time (information duration), and so forth.
- **Failure detectability**. This class of failures is related to signalisation to user; a detectability failure happens when a system failure requiring user attention and/or action remains undetected. Classification rules and technical specification describe extensively which failures should be detected: [**5**], Part 4, Chapter 9, Section 2, Paragraph B.102, for instance, states minimum failure detection requirements for computer based systems; [**5**], Part 4, Chapter 9, Section 4, Paragraph A.600 states computer *CPU* temperature shall be monitored, and therefore cooling system failure detected; [**5**], Part 4, Chapter 9, Section 4, Paragraph C.104 states the performance of the network shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity are detected; etc.
- **Failure consistency**. This class of failures is related to user perception of a situation, that may in fact represent a failure or not. Failures are said to be **consistent** if the service is perceived as incorrect by all users, **inconsistent** if the perception of incorrectness is not unanimous. A consistency failure happens when users have different opinions with respect to the service system shall deliver, or if its specification is unclear, and it is interpreted in different ways.

- **Failure consequences**. This class of failures is related to the consequences failures generated. A scale of severity shall be defined to provide an adequate range of properly described sub-classes; here suffices introducing two main consequence sub-classes, named **minor failures**, or occurrences for which harmful consequences are of similar cost to benefits provided by correct service, and **catastrophic failures**, or occurrences for which harmful consequences are of orders of magnitude, if not incommensurably, more costly than benefit provided by correct service. Classification rules and technical specification do not classify failure according to their severity, but rather classify systems according to their importance; a failure of an essential system is regarded as catastrophic, as opposed to a failure in a non important system, which is seen as minor. The difference in approach is only verbal. It is understood classification societies requirements for essential systems are structured to minimise the likelihood of a failure to happen, and its consequences should it happen. As it will be shown further on in this taxonomy, this corresponds to avoid failures and tolerate unavoidable failures.

Faults are classified according to following viewpoints [**6**]:

- **Phase of occurrence**. As seen before there are two main phases: development and use. This leads to define
  - **Development faults** those happening during development phase, and
  - **Use faults** those happening during use phase.
- **System boundaries**. This criterion defines faults as:
  - **External**, if they are located beyond system boundaries; and
  - **Internal**, if they are located within system boundaries.
- **Phenomenological cause**. This criterion defines faults as:
  - **Natural** if their cause is not related to human activity or participation, and
  - **Human made** if their cause is related with human activity or participation.
- **Dimension**. This criterion defines faults as:
  - **Hardware** if they are originated or affecting hardware, and
  - **Software** if they are originated of affecting software.
- **Objective**. This criterion defines faults as:
  - **Malicious** if they are caused by humans with the intent of causing harm to the system, and
  - **Non malicious** if they are caused by humans without intent of causing harm to the system.
- **Intent**. This criterion defines faults as:
  - **Deliberate**, if they are caused by a harmful decision, made in awareness[45], and
  - **Non deliberate**, if they are caused by a harmful decision made without awareness
- **Capability**. This criterion defines faults as:
  - **Accidental**, if they are caused inadvertently, and
  - **Incompetence**, if they are caused by incompetence of operators or developers
- **Persistence**. This criterion defines faults as:
  - **Permanent**, if they are present till maintenance, and
  - **Transient**, if they appear and disappear in a time pattern not related to maintenance actions.

[45] Difference between a malicious and a deliberate fault is subtle: it might be said first case contemplates the awareness of harmful effect of the action, as opposed to the second, in which there is no awareness of harmful effect, and this causes the harmful decision to be made. In both cases users is aware of making a decision, in the second the user is not aware of the consequences, as opposed to first.

Viewpoints can be combined to create new sub-classes, reported in the following picture.

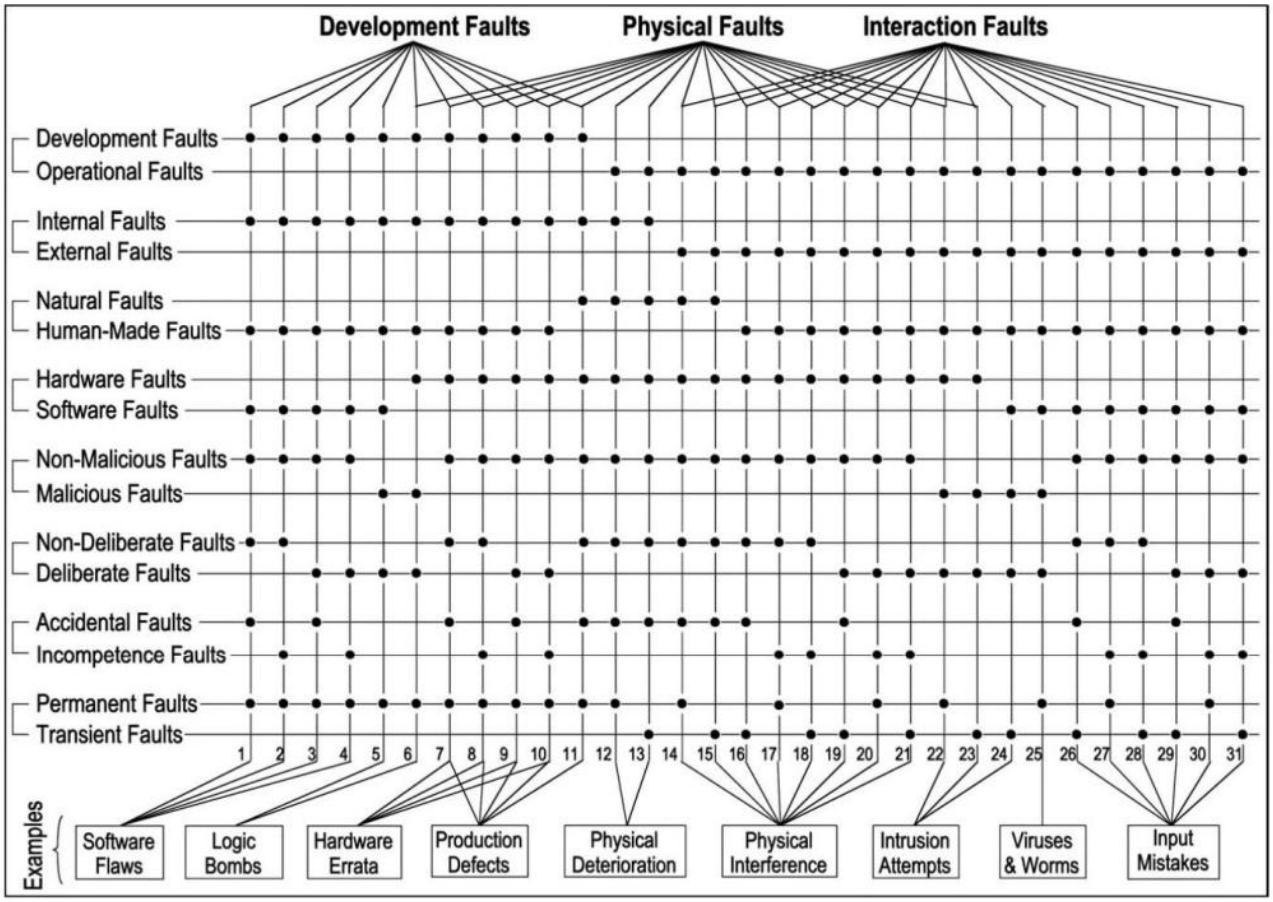

Fig. 14: Fault Sub-classes Definition [6].

2.3.3 Attributes and Indexes.

Dependability is a general concept that qualifies the ability a system has to deliver the expected service with an acceptable trust, or the ability to avoid service failures that are more frequent or severe than acceptable ([**6**] and [**12**]). This definition has been expanded and inspected in multiple directions, focusing on different point of views; this developing work has lead to the definition of some main qualifying attributes, together with quantifying and measuring indexes, widely used in the community. They are:

- **Reliability**. It is the probability that a system carries out the correct service at the time t>0 for a given set of operating conditions, provided that at time t_0 =0 the service was correct [**12**]. *MTTF* may be intended as a measure of reliability.
- **Maintainability**. It is the probability that a system delivers the correct service at time t>0, provided that at time t_0 =0 the service was not correct and a repair process is in progress [**12**]. This aspect is not part of this work scope, so definition only will be extended, for completeness. *MTTR* may be regarded as a measure of maintainability.

- **Availability**. It is 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. Availability is expressed, as a function of *MTTF*[46] and *MTTR*[47], as follows:

$$A = \frac{MTTF}{MTTF + MTTR}$$

  [**12**]. Intuitively, availability can be seen as a measure of system readiness to deliver the expected service [**6**].

- **Safety**. It captures the probability of absence of catastrophic consequences on the user(s) and the environment [**6**]. This aspect is not part of this work scope, so definition only will be extended, for completeness.
- **Security**. This concept, related in a way to the dependability defining quality of trust, covers different service disruption causes, generated by malicious intentions and/or unauthorised users. Unauthorised users may have malicious intentions or, simply, may not possess required skills needed for operating the system; in both cases they may induce service disruption. Security is seen as a composition of attributes, each one arising from a different approach to a common issue; these main attributes are:
  - **Integrity**. It captures the probability of absence of improper system alterations [**6**]. This aspect is not part of this work scope, so definition only will be extended, for completeness.
  - **Confidentiality**. It captures the probability of absence of unauthorized disclosure of information [**6**]. This aspect is not part of this work scope, so definition only will be extended, for completeness.

Following pictures summarise definitions treated so far.

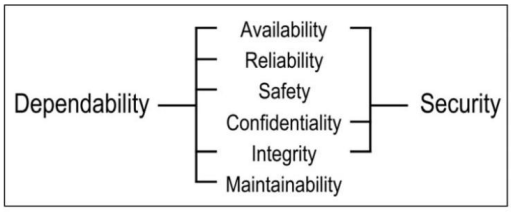

Fig. 15: Dependability Main Attributes.

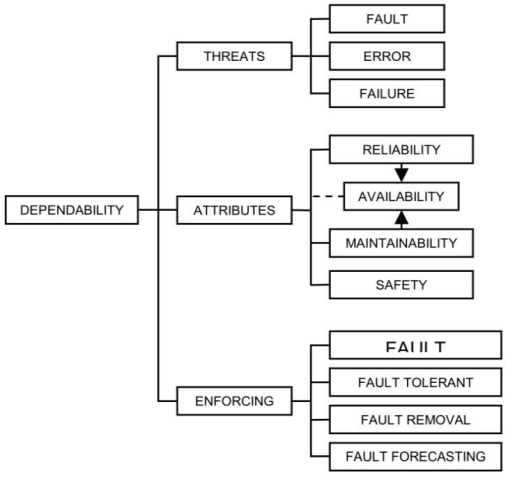

Fig. 16: Dependability Concept Overview.

[46] *MTTF* is a statistical index that captures the mean time expected to first system failure. [**28**], for instance; resource range is anyhow quite wide for this subject.

[47] MTTR is a statistical index capturing the mean time it takes to restore system service after a failure, as the name implies. [**28**].

2.4 Techniques.

A multiple of techniques are employed in dependability. Field of application are:

- Fault management. Those techniques are commonly named **enforcing techniques**.
- System analysis
- System modelling
- System dependability evaluation (or metrics). Those techniques produce indexes structured with the aim of comparing systems according to a dependability viewpoint.

In this section those techniques will be explained.

2.4.1 Dependability Enforcing Techniques

Techniques to obtain dependability are classified into four major categories, described in following chapters.

2.4.1.1 Fault Prevention.

This technique aims at avoiding the occurrence of a fault. It is applied mainly during system design, development and test stages [**12**]. In this work this technique has prominent importance, owing to the fact it is used during development phase. Classification rules and technical specifications show many fault prevention requirements; they can basically summarised in main categories:

- Prevention of physical faults, as defined in Fig. 14. Components are tested against anticipated climatic conditions ([**5**], Part 4, Chapter 8, Section 3, for example); located in such a way to reduce risk of fire, explosion (self or other equipment nearby. Separation is a word that recurs often in rules), collision, severe climatic conditions (air conditioned rooms for electronic equipment, if standard climatic conditions cannot be met. [**5**], Part 4, Chapter 9, Section 4, Paragraph A.600) or flood damage ([**5**], Part 4, Chapter 8, Section 2, Paragraph C.100, for instance). Systems are equipped with protective functions preventing operation beyond design limits, that can cause anticipated ageing ([**5**], Part 4, Chapter 8, Section 2, Paragraph B.213, for instance).[48]
- Prevention of software (code) faults, recurring to:
  - Modularisation, or the attempt of using well tested code modules to build core code (reference to [**5**], Part 4, Chapter 9, Section 1, Paragraph D.200),

[48] No mention is made in the rules about preventive maintenance as a mean to avoid physical faults. The main reason behind this choice is that preventive maintenance does not belong to development phase, but use phase, so out of classification societies scope of service. Still, owners appreciate the advantages offered by this technique and quite often implement it routinely.

  - Usage of strongly-typed programming languages,
  - Code simulation on a mock up reference scaled system,
  - Adoption of a software quality plan ([**5**], Part 4, Chapter 9, Section 1, Paragraph C.108).
- Prevention of development faults, as defined in Fig. 14. Classification societies strongly advise accurate design procedures and rigorous quality controls for design are put in place, according to EN-*ISO* 29000, for instance; and very often owners require such certification be held when admitting shipyards for bidding. Actions usually carried out to promote development fault prevention are [**12**]:
  - Review and discussion of technical specification and rules requirements, with emphasis on analysis of system goals, system requirements and engineering practices. This review is often called **kick off meeting** (**or project initiation** [**14**]).
  - Review and discussion of conceptual engineering, with particular emphasis on reaching:
    - A clear description of system architecture and its effective partitioning into subsystems and relevant interfaces,
    - A correct formulation and allocation of tasks to be performed by the system and its subsystems,
    - A clear and unambiguous system partitioning into homogenous technological areas to be assigned to design team members according to their expertise.
  - Review and discussion of detailed engineering, with particular emphasis on:
    - A correct implementation of system functions by selecting suitable technologies and solutions (hardware and software) to make the system dependable,
    - A careful analysis of the arrangement of the components and subsystems into the whole system for avoiding fault occurrence (for example, by selecting a suitable shielding).

    This phase is named **project definition** [**14**]

Worth noting, approach to fault prevention is multilateral and team intensive: classification societies positively addresses physical fault prevention, hardware errata[49] and production defects[50], whist setting forth a multiple of “soft requirements” when comes to other development faults, like software flaws and logic bombs (Fig. 14). Remaining fault classes are simply not addressed, or vaguely mentioned. Shipyards and ship owners must then closely cooperate to address remaining aspects, such as technology choice, appropriate specification for intended use and environment, etc.

[49] A”hardware erratum” is a development, internal, human-made, hardware, non-malicious permanent fault. A cable insufficient dimensioning compared to current it is designed to carry is such a fault if referred to a *IPS*, as it has happened during development phase, it falls within system boundaries, it is caused by a human designer or human made computer code, and the designer who has caused it did not have malicious intents (hopefully). He or she may have caused the fault deliberately (wrong decision caused, for instance, by wrong information on the user to be supplied), accidentally (input mistake to calculation routine), or because of incompetence (hand calculation ignoring electro-technical laws).

[50] Production defects differ from hardware errata because they can be natural as well. An EMC-induced fault is natural, in the sense that a natural effect of human action has caused the fault. An EMC-induced fault should happen only during development, and be rectified before use, affects hardware, and it is non-malicious in its nature; in summary it is a production defect. All hardware errata are production defects, but not all production defects are hardware errata, owing to the fact that natural faults are not included in hardware errata definition.

2.4.1.2 Fault Tolerance.

It is understood not all faults can be prevented; especially those originated by natural causes, like ageing, for instance. If system service is of outmost importance, unavoidable faults that may affect it must be tolerated, i.e. service shall not be affected by such faults. Fault tolerance capabilities are provided by employing dedicated techniques, to levels and systems that must be agreed upon during kick-off meeting.

Fault-tolerance has three levels of requirements, commonly classified as **fail-operational**, **fail-safe** and **fail-silent** (the generic term "fail" here refers both to faults and errors) [**12**].

By the fail-operational level, the system continues to deliver the correct service in spite of a fail, thus enhancing both reliability and safety. The fail-operational level is needed when an uninterrupted service is demanded. A particular case of fail-operational level is the fail-degraded level, or degraded operation, when the system delivers only a portion of the expected and correct service [**12**].

By the fail-safe level, the system responds to a fault reaching a safe behaviour. A fail-safe level is needed when an incorrect service is acceptable provided that it is safe [**12**].

By the fail-silent level, the system goes off after a fault. This level is applied when faulty system delivers a non-critical service or the user prefers to have no service rather than an incorrect [**12**].

There are two main basic strategies of tolerating a fault, namely: **system reconfiguration** and **fault masking**.

Techniques based on system reconfiguration work in three steps: in the first, named **fault detection**, the presence of a fault is revealed; in the second, named **fault location**, the source of the fault is located and in the third, named **system recovery**, the detected fault is eradicated and the service is restored through a system reconfiguration.

Techniques based on fault masking foresee ride through a fault by using a replication/multiplication scheme, skipping remaining phases, location and recovery [**12**]. Fault-masking techniques exploit the redundancy principle, i.e. the multiplication (replication, in case of identical parts) of components or sub-systems so that a faulty component or sub-system can be deactivated and one of its multiple (or replicas) is used to continue delivering a correct service[51]. Replicas and multiples are "extra", in the sense that replicas and/or multiples are not needed to deliver service in normal condition (in this sense replicas are redundant. For this reason adoption of replicas is often called **redundancy**. Multiples, as opposed, are often termed **backups**). In the following the difference between replication and multiplication is no longer remarked, as the service is considered as subject, and service is usually replicated, being kept identical or identically satisfactory [**12**].

When using replicas, two basic schemes can be arranged: **passive** and **active** replication [**12**]. When passive replication is adopted, the replica starts working to replace the faulty system or component only when a fault occurs (this configuration is often termed **cold standby**); when active replication is adopted, replicas run together with the system on duty and replace it in case of fault. In this case there are two possible configurations: replicas share load with duty system (**load sharing**), or replicas are active, delivering no

[51] Exact copies are said to be replicas; components or systems providing same services but adopting different physical principles are said to be multiple.

service, ready to take duty system over (**hot standby**). It is understood that, in case of load sharing, individual percentage shall be so that loss of one unit results in an acceptable load for the remaining.

These concepts are widely used in classification rules, in conjunction with essential and important systems; examples can be found in:

- [**5**], Part 4, Chapter 8, Section 2, in which it is stated that emergency system is, indeed, a degraded mode of *IPS* normal mode, and transition system acts as degraded mode for emergency system;
- [**5**], Part 4, Chapter 8, Section 2, Paragraph B.100, in which is stated that: "there shall be component redundancy for main sources of power, transformers and power converters in the main power supply system so that with any source, transformer or power converter out of operation, the power supply system shall be capable of supplying power to the following services:
  - Those services necessary to provide normal operational conditions for propulsion and safety;
  - Starting the largest essential or important electric motor on board, except auxiliary thrusters, without the transient voltage and frequency variations exceeding the limits specified;
  - Ensuring minimum comfortable conditions of habitability which shall include at least adequate services for cooking, heating, domestic refrigeration (except refrigerators for air conditioning), mechanical ventilation, sanitary and fresh water."
- [**5**], Part 4, Chapter 8, Section 2, Paragraph B.200, stating that there shall be at least two stand by generators, one per each power station, ready to start in case of black out
- Etc.

Redundancy (backup) is the only fault tolerance technique treated in classification rules as of now; no mention is made to **design** diversity, or the adoption of different designs to generate the same service. Redundancy is generally easy to test and verify, even though the underlying assumption that replicas are independent is not always so certain. Redundancy has cost implications rendering owners and shipyards not prone to extend it in a generalised way; in this sense classification requirements are to be considered as minimum requirements. Inasmuch as revenue-making systems are concerned, owners provide redundancy, without forgetting all financial implications; usually statistical consideration upon fault severity and associated frequency is conducted, without overlooking *MTTR* and store keeping costs, both onboard and ashore. An informed decision is then drawn.

2.4.1.3 Fault Removal.

These techniques are employed during both system development and system use phase. In the former case these techniques become part of system design procedures, whilst in the latter case they belong to the evaluation procedures.

Fault removal during development phase consists of three distinct steps: **verification**, **diagnosis** and **correction**.

Verification consists in deciding if system satisfies technical specification and adheres by relevant rules requirements in force. Verification can be conducted statically on the system itself (**static verification** [**6**]) analysing engineering drawings and documentation (classification societies name this activity **plan approval**), visually inspecting assembly, components and layouts (classification societies name this activity

inspection), or on a system model (**simulation** or **model checking** [**6**]); verification can be conducted dynamically (**dynamic verification** [**6**]) analysing system behaviour[52] against a range of pre-determined stimuli. Classification societies and technical specifications foresee three basic steps in dynamic verification, classified according to project timescale: factory acceptance trials, harbour acceptance trials and sea acceptance trials. List of test to be conducted is called **test memoranda**.

FAT are conducted at sub-contractors' premises, and are aimed at proving components and sub-systems fulfil design specification and rules in force, which are, in the case of an *IPS*: *IEC*, classification and technical specification. Examples of *FAT* can be found in [**5**], Part 4, Chapter 8, Section 4, Paragraph D, for instance.

HAT are conducted at shipyard, with the vessel alongside. They are aimed at proving system integration at a higher level compared to *FAT*, including shipyard engineering and installation. Examples of *HAT* can be found in [**5**], Part 4, Chapter 9, Section 2 Paragraph B, for instance.

SAT are conducted at sea, with the aim of proving vessel reaction as a whole to a pre-determined set of stimuli (test memoranda), in conditions as close as possible, to contract and classification. Examples of *SAT* can be found in [**5**], Part 4, Chapter 8, Section 12, Paragraph B for instance.

Dynamic verification includes several testing techniques, such as **fault injection**, **input simulation**, etc.

Owners have special interest in this phase, as it is prerequisite to successful and continued operation. Owners usually install systems not subjected to classification survey, and to that extent they prepare test memoranda and acceptance criteria.

Fault removal during system use is usually classified as **corrective maintenance**.

Shipyards do not pose much effort in developing and using those techniques, as they have an impact on production schedule. It depends though upon shipyard level of involvement in vessel engineering, and its associated responsibilities. The higher the involvement, the heaviest the focus should be, as accurate fault removal reduces warranty costs and therefore generates revenue, as anticipated in *2.1.1*.

2.4.1.4 Fault Forecasting.

These techniques focus on the evaluation of system dependability characteristics. Dependability is determined by means of either qualitative or quantitative methods.

Qualitative methods aim at identifying, locating and classifying faults causing a failure and at analyzing the associated failure modes.

Quantitative methods aim at assessing, in terms of probabilities, dependability quantitative attributes.

Evaluation methods of dependability characteristics are based on graphical models of the system. Some well-known methods are: Failure Mode and Effect Analysis (*FMEA*) for qualitative determination; stochastic Petri nets or Markov chains for quantitative measurement; *FTA* for both qualitative and quantitative

[52] System is, in this case, operating. It cannot be said system is in use as, in 2.3.2.1 use phase is initiated when system has been thoroughly tested and accepted for use. Development phase anyhow foresees a testing session, during which system is proven in an environment as closed as possible to its use; in this phase fault removal techniques are applied.

methods. *FMEA* and *FTA* are among the most popular methods. *FMEA* identifies the failure modes by a bottom-up approach (inductive analysis) that goes up from the faults to the failures. *FTA*, instead, studies the causes of the failures by a top-down approach (deductive analysis) that goes down from failures to faults.

More details on these techniques are offered under *2.4.3*.

Classification societies often refer to *FMEA* as their technique of choice to receive evidence of a fault forecasting activity being undertaken, and to ensure engineering process has been carefully controlled. In this respect *FMEA* may be regarded as a fault removal technique; this is not unexpected as, by means of it, faults may be forecasted and thus handled during development.

2.4.2 System Analysis Techniques.

It is understood system analysis shall be performed at an early stage of project, owing both to classification societies requirement, and to protect shipyards and owners from consequences of a severe development fault discovered late, when most expenditures have been committed.

It is as well understood it is preferable discovering possible faults and failures before they happen during the use phase (and that may have been left undiscovered during testing), in which consequences can be financially far worse. Effective action plans (prevent or tolerate) can be devised, without contingency pressure, and procedures put in place to execute them, since development.

From those basic assumptions, the necessity for a system model that can be analysed in depth, before the construction of actual system, descends. Dependability technique classes considered so far rely upon a system representation permitting systematic observation of effects caused by threats applied on components or sub-systems, to the atomic level (*2.3.1*) as defined under *2.3.2*. Objective of this section is describing a decomposition to generate a system model starting from its atomic components. This system decomposition shall be as far as possible unambiguous (each system shall be represented by a unique model), complete, accurate and of easy implementation and integration into most common shipyard engineering applications. An application of this procedure is offered in *3.4*.

Decomposition is developed as a top-down procedure, beginning with the system and its service in its widest definition, narrowing down as the process continues, to an atomic level. System definition is drawn from technical specification, whilst sub-systems and components become apparent as the engineering process continues. As a general rule, all entities that may be affected by selected threats shall be included in the model.

Shipyard engineering drawings show atomic components, as intended by them. System decomposition is then to be stopped at that level. It is shipyard practice to name every component (or atom) with an identifying code, called **piece mark**. Piece mark identifies every entity that is handled (procured, installed on board, connected to or forming part of systems such as cooling, aeraulic[53], electrical power, automation,

[53] Aeraulic is a short for compressed air and hydraulic systems

instrumentation, etc.) by shipyard. A piece mark may identify a sub-system, such as a **package** handled as a single entity, such as a fuel purifying module, or a component, such as a lamp or a cable.

Atomic components are interconnected by means of other atomic components, such as cables or pipes, transiting in different spaces.

In some instance, engineering drawings do not offer a level of accuracy suitable for an effective dependability analysis; such instances are to be addressed on a case by case basis, and description conveniently expanded to reach requested accuracy. This procedure, though, can be sub-contracted as well, given the fact that requires specific engineering knowledge, possessed by the designated sub-contractor.

2.4.3 System Modelling Techniques.

Now that model components are defined, the architecture can be conveniently represented. Architecture, or the structure of connections among components, is necessary to unveil the outcome of a certain threat or set of threats.

System modelling techniques can be subdivided into two main classes: **static** and **dynamic**.

Static techniques consider relations among components as time invariant; they make use of basic logic operators (AND, OR, K out of N, NOT, etc.) to model such relations. Result of interactions depends upon input value at that precise moment in time, and varies as inputs vary.

Dynamic techniques, instead, consider relations among components as time variant; they make use, in addition to basic logic operators, of enhanced operators like: PAND, FDEP, SEQ and SPARE [**15**]. Such operators are briefly explained hereunder:

- Priority-AND, or **PAND**. This block changes its status, from normal to fail, if all inputs change their status from normal to fail) in a predetermined sequence[54].
- Functional dependency or **FDEP**. Functional dependence occurs when the failure of one component (referred to as the trigger component) causes other components (referred to as dependent components) within the same system to become inaccessible or unusable. A FDEP block then propagates the trigger event as a fault state to all dependent components.
- **SPARE**. SPARE gates model one or more principal components that can be substituted by one or more backups (spares), with the same functionality. The SPARE gate fails when the number of operational powered spares and/or principal components is less than the minimum required. Spares can fail even while they are dormant, but the failure rate of an unpowered spare is lower than the failure rate of the corresponding powered one. SPARE gates can be subdivided into main categories, reflecting substitution practices:
    - Cold spare or **CSP**: replacement is activated upon primary failure.
    - Hot spare or **HSP**: replacement is active, but producing no output.

[54] PAND changes its output only when inputs happen to reach active state in a predetermined sequence, as opposed to AND, which changes its output when inputs happen to reach active state, no matter in which order. Time dependency is apparent.

    - Load sharing or **LS**: primary and replacement are active, taking each part of workload. Upon primary failure, replacement is to take full workload.
- Sequential Enforcing or **SEQ**. A SEQ gate changes its output from normal to fail if and only if its inputs fail in a particular order that cannot change. While the SEQ gate allows the events to occur only in a pre-assigned order and states that a different failure sequence can never take place, the PAND gate does not force such a strong assumption: it simply detects the failure order and fails just in one case.

It can be easily notices those advanced operators not only account for input present state, but past states. Drawback of dynamic techniques, if compared to static, is difficulty: static techniques may offer results without great computational effort, as opposed do dynamic, which cannot avoid automated means of numeric computations.

Following paragraphs describe most common modelling techniques.

2.4.3.1 FTA *and* DFTA.

FTA is a top-down deductive process based on a graph, a fault tree, which begins with a specified failure event, called **top event**, and an analysis scope, or the listing of affecting factors (internal rather than external, malicious or not malicious, etc.). Generally, the top event coincides with system failure, or with any undesired state. Interaction continues researching all immediately preceding possible causes, within analysis scope, leading to the top event. These causes are related to each other by means of basic logical relations, such as AND (all immediately preceding causes shall be active to cause top event), OR (at least one of the immediately preceding causes is active to provoke top event), voting OR (at least k out of n immediately preceding causes shall be active to provoke top event), or a composition of them. Once all immediately preceding causes have been found; each of them is treated as a top event, so all immediately preceding causes are sought. Iteration is arrested when all causes are resolved in terms of basic events or immediate causes. Basic events are events related to atomic components, and are generated by immediate causes. Resulting dependencies are represented as a tree, called **fault tree**. Fig. 17 shows an example of a fault tree derived for a system made of a DC electric motor, a single pole, single thread switch and a power supply (battery). The top event is the fact that motor does not start, the reason why is researched within the system (external causes like thunders, or excessive braking load, for instance, are excluded).

A fault tree is a different way of explicating a Boolean expression, thus it permits calculations relating top event to basic events or immediate causes. Usually, such calculation is made considering basic event probability; given those probability values and law relating them to the top event, the probability that top event happens as function of probability of basic events to happen is deducted.

There are some underlying assumptions in this technique:

- Fault rates are constant, so *MTTF* is.
- Graph, and the function it represents, is not time-dependant. Future states available to the system depend upon only its present state.
- Each system element has two, mutually exclusive, states.
- System elements are not repairable.

- Basic events are statistically independent.

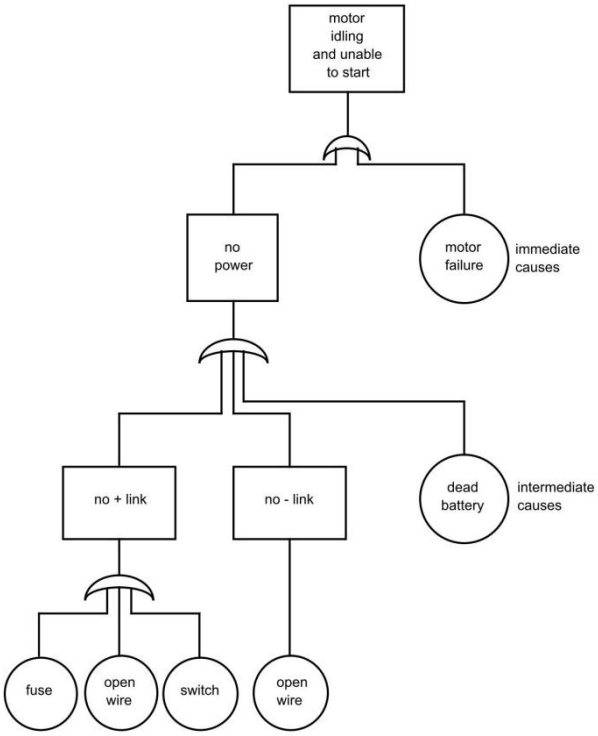

Fig. 17: Example of a Fault Tree Graph

FTA may be considered a fault forecasting as well as a fault prevention technique; it makes use of fault injection, even though "virtually", defining basic events.

FTA is disciplined in *IEC*-61025 (2006), *ANSI*/*IEEE*-Std-352 (1987) and SAE-ARP-4761 (1996)

FTA has recently been expanded to compensate for the inability to model dynamical interactions among components or subsystems, or to represent system configuration changes: **Dynamic Fault Tree Analysis**, or *DFTA*, has been defined.

DFTA does not have international rule support, as opposed to *FTA*.

2.4.3.2 RBD *and* DRBD.

A Reliability Block Diagram (*RBD*) is a diagram containing a series of blocks, representing each one a component or a sub-system belonging to system under consideration, connected in such a way that existing fault relation of dependency is expressed: a fault in a component implies all components located downstream in the same line are equally faulted or not available or reachable. Blocks are allowed to have two states only: operating or faulty. If a path may be found through the network of blocks from beginning to end, the system is said **operational**; if no such path can be found, then the system is said to be **failed**.

A *RBD* may be drawn using switches in place of blocks: a closed switch represents a working component; an open switch represents a failed component.

A *RBD* may be converted to a success tree by replacing series paths with AND gates and parallel paths with OR gates. A success tree may then be converted to a fault tree. All representations contain same information.

A *RBD* shall be drawn for every particular component configuration, or system function; it represents pictorially a Boolean expression, which is the fault relation of dependency discussed above. Main difference from a fault tree is that *RBD* is success-oriented, e.g. shows how system works, as opposed to fault tree, which shows how system fails. *RBD* offers more comprehension of redundancy and ease of computation.

An example of *RBD* can be found in Fig. 18.

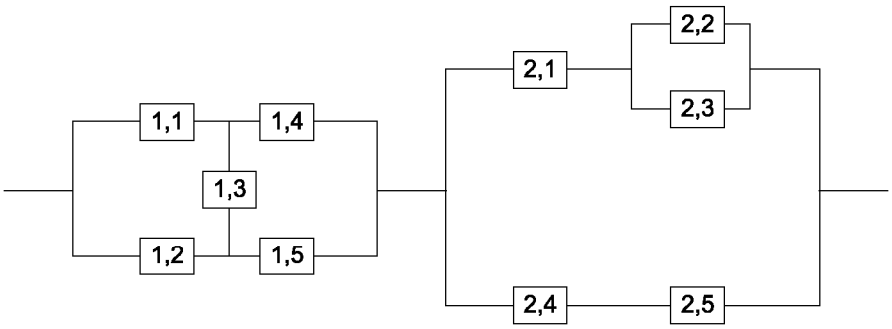

Fig. 18: Example of *RBD*

A *RBD* is constructed following steps listed below:

- Defining functions system is to perform, and the operating states (stand by, full power, etc).
- Deciding which functions, or combination of functions, constitute minimum requirement for successful operation. In the example of Fig. 18 two main functions can be seen: the first constituted by blocks named 1.x, and the second constituted by blocks named 2.x. Both are needed for system successful operation because, if those functions are imagined as switches, both need be closed to find a path from beginning to end.
- Associating each functions with its needed components, connected in a way to show fault relation. Referring to function 1 in the example of Fig. 18, it is appreciated function is performed by 5 components, connected as shown. Structure shows no single fault in function 1 components causes function failure; double fault (component 1.1 and 1.2, component 1.4 and 1.5) causes function failure.

A *RBD* is quantified as follows:

- Reliability $R_{i,T}(t)$ of each component is known. Defining T as the lifetime of a component, any observed time to fail is then a value of the random variable T. The probability distribution of T ∈ [0, +∞) is its unreliability

$$F_{i,T} = P(T \leq t), \qquad 0 < t$$

  Reliability is then defined as:

$$R_{i,T}(t) = P(T > t) = 1 - F_{i,T}(t)$$

  Meaning that reliability is the probability of no fault or failures in the interval [0,t], or, similarly, the probability of a fault or failure after time t.

- System reliability $R_{Sys,T}(t)$is calculated using rules of statistics.
- Indexes are calculated from $R_{Sys,T}(t)$. Assuming $R_{Sys,T}(t) = e^{-\lambda_{Sys}(t)}$, then

$$MTTF = \int_0^\infty R_{Sys,T}(t)dt = \frac{1}{\lambda_{Sys}}$$

There are some underlying assumptions in the technique:

- Every component must have a fault mode only. This is due to the fact *RBD* only deals with two states: normal and faulty. Each different fault mode may require a dedicated *RBD*.
- Structure is not time-dependant. System may have different configurations according to multiple purposes; a fault or failure may affect parts not in use.
- System components are independent from each other; they are only related in the fashion shown in the *RBD*. This means there is no correlation among unreliability functions. If a dependency between two or more components exists (for example if it is always true that component A fault implies component B fault), then it must be made apparent by drawing those components as series connected in any instance of their use.

RBD is a standard technique disciplined by *IEC* 61078 and *ANSI*/*IEEE* Std. 352, used by major institutions, such as NASA and Royal Navy.

RBD suffers from same limitation *FTA* does (as both representations do contain the same information), therefore a similar update has recently happened, leading to the definition of Dynamical Reliability Block Diagram, or ***DRBD*** [**16**]. A *DRBD* features two main improvements, in addition to what mentioned under *2.4.3*, compared to a *RBD*:

- Components now can have multiple states. States are represented in Fig. 19 and can be described as follows:
  - Active. Component or sub-system is delivering the intended service.
  - Failed. Component or sub-system is not delivering the intended service due to a fault or failure.
  - Standby. Component or sub-system is not delivering the intended service but it is ready for. Component or sub-system is reliable, but not available.

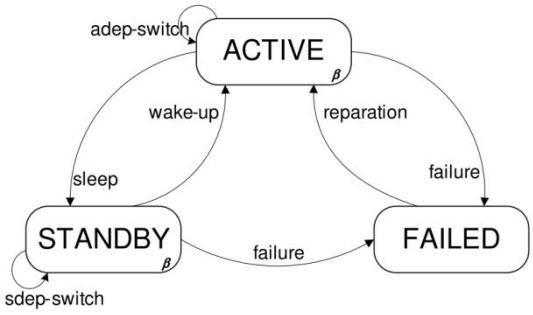

Fig. 19: Component States in a *DRBD*.

- States are entered as a consequence of an **event**, which initiates a **transition**. Events are external to components and generated by other components. Activation rules are specified when declaring the **dependency** between two components, or a specific transition involving them. An example is given in Fig. 20.

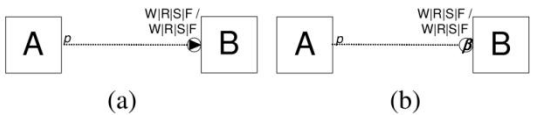

Fig. 20: Example of Dependency in a ***DRBD***

Dependencies are oriented, therefore their direction matters. In the example system or component A acts on system or component B; A is the **driver**, whilst B is the **target**. Possible state transitions are basically three:

- Wake-up. Component or sub-system starts delivering its intended service. It leaves the standby state and enters the active state. The opposite transition is named sleep.
- Fault or failure. Component or sub-system ceases delivering its intended service due to a fault or failure. The opposite transition is named reparation.
- Fault or failure can affect standby components as well; therefore there might be a transition from standby to fault. In this case there is no opposite transition, as reparation need be proven by activating the system or component.

Possible dependencies can be many, and they represent the actual state of components involved. Should the driver component enter in a state not foreseen in the dependency, the target becomes fully active. Some examples can be given, referring to Fig. 20:

- WRS|S dependency. Component A activation (wake-up) causes component B to sleep; component A repair (and subsequent activation) causes component B to sleep; component A standby causes component B to sleep. Component A failure causes component B to wake up. This behaviour may be seen in a standby scheme with a leading and a following component, in which leading component is kept preferably running and following preferably standby.
- W|S dependency. Component B is waken up as component A fails. Component B is to be deactivated by another dependency, as there is no such event in the relation with component A.

DRBD do not contain the same information of their respective DFTA, and an exhaustive comparison is discussed in [**15**].

DRBD cannot be solved directly, but need be transformed in a different symbolism to be properly quantified. There are two main classes of techniques to achieve this extent: analytical and simulation techniques. Analytical techniques make use of Markov chains, Bayesian or Petri networks; simulation techniques make use of Monte Carlo simulations. Analytical techniques and their use are disciplined by:

- *IEC* 60300 (selection, definition),
- *IEC*-61165 (2006) and *ANSI*/*IEEE*-Std-352 (1987) (Markov chains),
- *ISO*/*IEC*-15909-1 (2004) (Petri nets).

Simulation techniques are not included in the international rule corpus; their implementation is left to the analysis team.

2.4.3.3 FMEA *and* FMECA.

FMEA is a multicultural teamwork-based inductive analysis predicated upon a system description by means of its atomic components and physical relations. Its objective is demonstrating system failure behaviour [**17**]. *FMEA* should give a description of the different failure modes for all the items of equipment in respect of their functional objectives. In this way, all catastrophic or critical failure possibilities can be identified, and either eliminated or minimised at an early stage in the project through design correction or the introduction of clear operational procedures [**17**]. An *FMEA* can be approached both bottom-up and top-down, the latter being favoured owing to its inherent saving of resources; worth remembering, the former offers unparalleled completeness.

FMECA is an extension of *FMEA* that includes a preliminary risk analysis.

An *FMEA* is developed in subsequent steps:

- Identification of the system being analysed and all relevant main components falling within the scope of analysis and determination of their functions and existing interfaces and relations among them. Components and interfaces are to be numbered for ease of reference. Bills of materials and single line diagram are useful to this extent.
- Consideration and documentation of all failure modes each component has. A capacitor, for instance, has two fault modes: fail short and fail open.
- Preparation of a list of potential effects of each failure mode. All failure modes, relevant to every component in the system, shall be listed.
- Assignation of a severity rank to all fault modes (*FMECA*). The highest severity rank corresponds to a fault leading to a hazard without warning, the lowest to a fault carrying no consequences. An exemplificative severity scale is reported in [**17**], paragraph 5.6.3.
- Assignation of an occurrence rank to all fault modes (*FMECA*). The highest occurrence rank corresponds to a fault mode that has high probability to happen, the lowest to a fault mode that has a low probability to happen.
- Assignation of a detection rank to all fault modes (*FMECA*). The highest detection rank corresponds to a fault mode that is unlikely to be detected, whereas the lowest rank corresponds to a fault mode that is certainly detected.[55]
- Calculation of *RPN* (**Risk Priority Number**) for all fault modes (*FMECA*). *RPN* is calculated multiplying the three ranks defined earlier. *RPN* is the basis for decision making, as:
  - An acceptable value shall be stated before the analysis
  - Actions are to be promoted if minimum *RPN* is not attained
  - *RPN* is to be recalculated after actions have been put in place
- Definition of tests and trials to confirm assumptions on failure effects and rank attribution, or to identify failure modes that could not be completely devised during design, as necessary.

Results are summarised in a table like Fig. 21.

FMEA is disciplined by means of several international rules, such as:

- US Department of Defence MIL-STD-1629A,
- *IEC* 60812 – Analysis techniques for system reliability - Procedure for failure modes and effects analysis (*FMEA*)

[55] The reason of this reversed notation is to be found in the fact that consistency is sought: high ranks correspond to high risks, and an undetected occurrence may pose a high risk.

- *BS* 5760-5:1991 - Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis).
- *IMO MSC* Resolution 36(63) Annex 4 – Procedures for Failure Mode and Effects Analysis.

Product/Process	Quad Detachable Lift	Date	1/31/2008
Prepared By	John Chair Operator		
Notes	Initial Draft		

Function / Requirement	Potential failure mode	Potential effect of failure	SEV	Class	Current process controls					
					Potential cause	Occur	Prevention	Detection	Det	R.P.N.
Chair/Basket	Chair Falls	Injury or Death	10	SRL	Cable failure	1	10 X Design Margin	None		0
					Cable Coupling Breaks	1	10 X Design Margin	None		0
					Detachable Grip Failure	1	10 X Design Margin	None		0
					Detachable Grip Corrosion	2	Inspection	During Inspection	1	20
	Restraining Bar will not lower	Legal Exposure	9	SRL	Obstructing object	4	Operator	Operator	3	108
					Frozen Bearing	1	Low temp bearing	Operator	3	27
Chair Loading/ Unloading	Skier Falls Loading	Injury	9	SRL	Dragged or Pushed Skier	8	Detached Chair	Operator	2	144
	Skier Falls Unloading	Injury	9	SRL	Dragged or Pushed Skier	8	Detached Chair	Operator	2	144
	Skier Abort (changes mind)	Paniced Skier, Injury	9	SRL	Humans	3	Warning	Operator	3	81
Bullwheel	Long Term Lift Stoppage	Paniced Skier, Injury	9	SRL	Cat. Prime and Aux Mover Failure	1	Preventative MX	Operator	1	9
					Catasrophic Mechanical Failure	1	Preventative MX	Operator	1	9
	Tensioning System Failure	Excessive slack in cable	8		Systemic Failure	1	Preventative MX	Control System	1	8
	Braking System Failure	Inop Overspeed Protection	6		Mechanical Failure	2	Inspection	Inspector	2	24

Fig. 21: Example of a Design ***FMEA*** Sheet

As opposed to other methods, *FMEA* is not easy to be quantified, and therefore offers poor comparison capabilities. Strict and repeatable definition for soft concepts as severity and occurrence may be not easy or unambiguous; therefore quantification in terms of *RPN* may be subjective.

2.4.4 System Dependability Evaluating Techniques, Metrics.

Metrics are needed to both measure system dependability as an absolute value, and compare designs to decide which is the more dependable. At present a certain number of metrics have been proposed, but no general consensus has been reached on their application. Measure of dependability shall enable producing a dependability specification, in which targets are set via indexes, calculated according to agreed metrics; repeatable and unambiguous indexes shall permit in turn fair comparisons between different implementations.

2.4.4.1 QoS.

This metric is explained in [**18**]. *QoS* is basically an index representing how reliably an electrical power system distributes its commodity, or electrical power, to the standard required by users. It is calculated as an *MTBF*, where a failure is defined as an event in which service is disrupted for a time duration sensible to loads, or commodity possesses quality parameters not suitable to be used by loads (too low or high voltage,

or too low or high frequency, for instance). In this perspective, a power outage affecting a device possessing some sort of stored energy (a fridge, a battery bank, a heater, etc.) is not perceived as a disruption if the time it lasts is such that it does not affect load operation (in the case of a fridge, temperature shall not exceed a certain threshold and goods are still correctly preserved; the stored energy is given by goods mass and temperature kept till service disruption, colder than the threshold). *QoS* does take into account equipment failures and normal system operation transients.

Inasmuch as dependability is concerned, *QoS* may offer a comparable quantity in benchmarking *AES IPS*; in terms of absolute values authors consider a value of 30.000 running hours as appropriate. Shall a dependability specification being drawn upon *QoS*, then the basic requirement is that *QoS* be larger than 30.000 running hours.

2.4.4.2 Operability

This metric is fully defined in [**19**]. Operability is a measure of how well a system continues to provide service to its users following to an event. In the case of an *IPS* of an *AES*, the users are the loads to which the system provides electric power.

The operation status of the i[th] user at time t is denoted as $o_i(t)$. Typically, this is a binary function such that

$$o_i(t) = \begin{cases} 1, & user\ i\ is\ receiving\ adequate\ services \\ 0, & user\ i\ is\ not\ receiving\ adequate\ services \end{cases}$$

Each user i is assigned a possibly time-varying weight $\omega_i(t) \geq 0$ indicating the importance of that user. The operability metric O:$E \times P^* \rightarrow [0,1]$, in which E is the set of possible events, expressed in terms of information useful to predicting system reaction (component states, relations) and P^* is the set of possible systems, quantifies the (weighted) degree to which services are provided to users following an event. Operability is defined as follows:

$$O(\theta, \Omega) = \frac{\int_{t_0}^{t_f} \sum_{i=1}^{I} \omega_i(t)\, o_i^*(t) o_i(t) dt}{\int_{t_0}^{t_f} \sum_{i=1}^{I} \omega_i(t) o_i^*(t) dt}$$

In which:

- Ω is the system in consideration, so that $\Omega \in P^*$
- $o_i^*(t) = \begin{cases} 1, & user\ is\ commanded\ to\ be\ on\ (operable) \\ 0, & user\ is\ commanded\ to\ be\ off \end{cases}$
- θ is a specified event so that $\theta \in E$
- I is the number of different users.

Operability has similarities with *QoS* as both indexes are load-biased; they are different in respect to the fact operability differentiates between on and off users and ranks them according to an importance function.

Operability introduces the concept of **average system dependability** as the expected value of operability over the distribution of events with which the system could be faced. In this context, the event can be considered a random variable Θ. Be $f_\Theta: E \times P^* \rightarrow [0, \infty)$ the parameterised probability function associated to Θ so that:

$$\int_E f_\Theta(\theta;\Omega)d\theta = 1 \quad \forall\Omega \in P^*$$

Then average system dependability is defined as:

$$\overline{D}_S(\Omega) = \int_E O(\theta,\Omega) f_\Theta(\theta;\Omega)\, d\theta$$

Of course, minimum dependability, if found more interesting than average dependability, is defined as:

$$D_{s.min} = min_{\theta\in E} O(\theta,\Omega)$$

2.4.4.3 Vectorised Dependability Metric

This metric, described and explained in [**20**], focuses on systems having defined degraded services. Albeit defined for computer systems, this metric has an interest in the application subject of this work; due to the fact *IPS* has degraded services, as already stated in *2.3.2*.

In the following, a brief synopsis is included, for ease of reference.

The metric is based on a concept called service level. A service level is defined as a group of system states, each with a user-specified degree of performance or functional accomplishment. Service levels are dependent on the design and layout of the system as well as on the application of the system, i.e. how the system is used. Therefore, the service levels are said to be **application-related**. The highest service level is denoted service level 0 (**SL0**) or **full service** level. This level must include the system state that describes the complete fulfilment of all the requirements in the specification, the fully operational state.

In the simplest case there is only one more service level, the **failed service** level, corresponding to the system failed state, when no service is delivered or the service delivered is of no use to the user. In this case the system has only one operational state with a specified degree of performance and the sole alternative is the failed state. The expected time the system is in the operational state before making a transition into the failed state is a measure of system reliability.

Intermediate service levels must be defined in a way that reflects users' opinion or perception of the degradation, in terms of missing service. A specification review identifying those functions or sub-services that belong to each level is necessary. The need to include more than one failed service level should be considered.

Be:

- E the set of system states,
- $SL_0, \dots, SL_l$ the set of service levels (operating or failed). By definition: $E = \bigcup_{n=0}^{l} SL_n$,
- $O = \bigcup_{n=0}^{k} SL_n, \quad k < l$ the set of operational states, in which the system provide service, either full or degraded,
- $F = \bigcup_{n=k+1}^{l} SL_n$ the set of failed states, in which the system does not provide any useful service to users. By definition $E = \bigcup(O, F)$.
- λ_{ij} the intensity for transition $i \to j, (i.j \in E, i \neq j)$

- π_i the initial probability of the state i
- By definition a transition $i \to j$ in which $i, j \in O$ is a **degradation**; if $j \in F$ it is a **failure**. No transitions are possible from a failure status (system without maintenance), so $\lambda_{ij} = 0, i \in E, j \in F$,
- u_i is the expected time in state i, or *MTTD*,
- p_i is the probability system enters the state i,
- v_i is the conditional expected time the system is functioning before being absorbed in i (the *MTTF* given the system eventually fails in state i)

Then the dependability vector becomes:

$$\boldsymbol{v} = ((u_i)_{i \in O}, (p_i)_{i \in O \cup F}, (v_i)_{i \in F})$$

Given the dependability vector, its norm may be regarded as the dependability index being sought.

3. Application to a Notional *IPS* of an *AES*.

3.1 System Description.

The system being investigated is mainly the *Main Electrical Power Supply System*, together with its controls, of an existing *AES*. Initial description covers the entire *IPS*; but main focus with be kept on *Main Electrical Power Supply System*; *Electric Propulsion System* and *Steering Gear* are regarded as users (in the taxonomical sense). The system is installed on a 128500 *GRT* cruise vessel, as part of its *IPS*, trading both in the Caribbean and in the Mediterranean, engaged in 14 days trips, typically. Vessel is about 306 metres long, can proceed at a maximum speed of 22.5 knots (service speed about 21 knots), and can carry 5021 persons (1369 crew members and 3652 passengers). Total installed power equals to 84 MVA.

IPS has the main functions listed in the following (refer to [**21**]):

- *Electrical Power Supply System*, compliant with *1.3.1*. Electrical power supply system physically converts chemical energy in the fuel to electrical energy, with specified quality, delivered to users via the Grid/Distribution function.
- Grid/Distribution, in charge of delivering electrical power to users.
- *Controls*, as illustrated in *1.3.4*. This function provides monitoring and control to all other functions, as dictated by classification rules and technical specification.

Main functions are fulfilled via systems and components, listed in the following. List derives from actual installation and is prepared in a recursive way, moving in a top-down direction, as discussed in *2.4.2* and *2.4.3*. The list is, in its essence, a decomposition of the system, and it is prepared bearing in mind its objective: generate a system model. List, furthermore, helps defining system boundaries. Modelling technique is chosen later on, but it can be easily anticipated to be a top-down technique. Top-down techniques have the advantage of being recursive, and this permits monitoring the effort and level of accuracy every step takes before entering it; their shortfall is that completeness cannot be evaluated without information in hand that would permit a bottom-up approach. Top-down techniques are suitable for the purpose of the work, and for this reason are used in the following.

System model is restricted to suit the case study, better defined in *3.3*, and to enable conclusions. Providing a complete and exhaustive model is beyond the scope of this work, which focuses, instead, on the procedure to prepare it.

Piece numbers are used to the purpose of compiling a model; they are required when using *FMEA*, and highly recommended when using different techniques. Such numbers offer several advantages, namely:

- Unambiguous component/sub-system identification. This provides in turn:
  - Unambiguous reference to engineering drawings (single line diagrams, general arrangement, etc.), highlighting functional and spatial relations, needed to build dependability studies and *SRtP* casualty evaluation (see *1.3.5*).
  - Completeness assessment, cross-checking with bills of material. Every piece number corresponds to a piece.
- Tight integration with engineering applications, so that information for dependability analysis can be found without dedicated operations.
- Tight integration with project management applications, so that project phases are controlled (see *2.4.1*).

In this work effective labels do not possess a particular importance; the fact that a naming convention exists does instead possess a particular importance, as it is explained hereafter. Using a naming system rather than another does not invalidate conclusions; naming is used for ease of reference and conveniently expanded to suit purpose of work.

System decomposition is, in addition, a well established management practice known under the name of **WBS**, or **Work Breakdown Structure**. *WBS* is widely used as a coordination tool, defining design subdivision and cost allocation. Every company may have a different way of breaking down their products, and label elements arising from it; the important fact is that the present structure can be used, perhaps with small adjustments, to evaluate dependability too. As an example, main function definition used in this paragraph, and derived from [**21**], is reflected in a shipbuilding major group *WBS*. Power supply is labelled L (propulsion system, so competence of the electrical design/engineering office) 01; Grid/Distribution is labelled F (electrical plant, so competence of the electrical design/engineering office) 02 (high voltage), 03 (low voltage), etc.; engine room automation is labelled F05, and so forth.

Present decomposition, although not fitting WBS to the word, adopts the same principle. In present work *Electrical Power Supply System* is not included in to *Electric Propulsion System*, this latter being regarded as a user. Impact of this different stand point is negligible. Classification societies treat propulsion system as an individual, admitting though it is heavily connected with *Electrical Power Supply System*; many requirements detail this integration. Present work integrates *Electric Propulsion System* into *IPS* concept at a control level, reflecting practical implementation. The always claimed need of a system integrator is then built in the definition of *IPS*, rather than being a simple request.

3.1.1 Electrical Power Supply System.

It consists of, according to the purpose of this work[56], of three distinct entities, as per rules requirements: a main, emergency and transitional electrical power supply system.

Information is derived from shipyard single line diagrams and bills of materials.

3.1.1.1 Main Electrical Power Supply System.

A first coarse decomposition leads to defining following components:

- Two power stations, identified with their respective piece number XA/872A_1 (port) and XA/872A_2 (starboard).
- One interconnecting line, named after the cable it contains, H/0000019AAA. An interconnecting line is defined as the set including one cable and two breakers, installed each one at a cable end.

[56] Prime movers and their auxiliary will not be covered; system boundary is set at alternator coupling flange, in this instance.

A second recursion, more refined, leads to defining following components.

- Interconnecting line:
  - Two identical circuit breakers, together with their relevant relay, cable and circuit breaker compartment, where instrumentation is installed. Names are:

Circuit Breaker	Protection Relay & Instrumentation	Power Cable[57]	Power Source[57]
XA/872A_1_119	XA/872A_1_119_prt	P/3900010AAA	FZ/239QB
		F/4000011AAA	FZ/240QB
XA/872A_2_220	XA/872A_2_220_prt	P/3900011AAA	FZ/239QB
		F/4000010AAA	FZ/240QB

Table 7: Interconnecting Line, Tentative Component List

- Power Stations:
  - Six identical diesel engine driven, high voltage (11kV), salient pole, brushless excited, synchronous alternators. Names are:
    - Alternator[58] 1: XA/274A (XA/872A_1);
    - Alternator 2: XA/274B (XA/872A_1);
    - Alternator 3: XA/274C (XA/872A_2);
    - Alternator 4: XA/274D (XA/872A_2);
    - Alternator 5: XA/274E (XA/872A_1);
    - Alternator 6: XA/274F (XA/872A_2).

    Alternators are connected in groups of three (triplets) to each power station.
  - Six transmission lines, connecting each alternator to its respective switchboard. A transmission line is defined as the set of a cable, its respective circuit breaker, eventually equipped with integrated protecting functions and its relevant cable and circuit breaker compartment in the high voltage switchboard[59], where instrumentation is installed. Names are:

[57] This item does not belong to interconnecting line, but to critical electrical power supply system, defined later on. It is a useful accessory indication.

[58] Originally piece number referred to the generator set, or the assembly of the alternator and its relevant prime mover. In this work pieces numbers have been further specified and adapted to a different system subdivision. This further refinement has lead to associating this number to alternator only, as its reference. As discussed early, this naming is just a reference convention. From a logistic standpoint, usually small generator sets (<4MWe) are delivered as a unique set, whereas large units (>4MWe) are delivered loose, i.e. engine and alternator come not coupled on a common skid. Reason for that practice lays on transportation capabilities: small generators may be moved via land on a lorry, as opposed to large unit, despatched via barge. Again, considering generators as a subset or a group of loose components is just a question of opportunity; the model will not be affected.

[59] These borders are easy to locate when high voltage switchboards are specified to be form 4; metallic partitions delimit those spaces.

Alternator	Power Cable	Circuit Breaker	Protective Relay & Instrumentation	P. Relay Power Supply Cable[57]	P. Relay Power Source[57]
XA/274A	H/0000001AAA	XA/872A_1_101	XA/872A_1_101_prt	P/3900020AAA	FZ/239QB
				F/4000020AAA	FZ/240QB
XA/274B	H/0000005AAA	XA/872A_1_105	XA/872A_1_105_prt	P/3900018AAA	FZ/239QB
				F/4000018AAA	FZ/240QB
XA/274C	H/0000002AAA	XA/872A_2_202	XA/872A_2_202_prt	P/3900025AAA	FZ/239QB
				F/4000025AAA	FZ/240QB
XA/274D	H/0000003AAA	XA/872A_1_103	XA/872A_1_103_prt	P/3900019AAA	FZ/239QB
				F/4000019AAA	FZ/240QB
XA/274E	H/0000006AAA	XA/872A_2_206	XA/872A_2_206_prt	P/3900027AAA	FZ/239QB
				F/4000027AAA	FZ/240QB
XA/274F	H/0000004AAA	XA/872A_2_204	XA/872A_2_204_prt	P/3900026AAA	FZ/239QF
				F/4000026AAA	FZ/240QB

Table 8: Transmission Lines, Tentative Component List

- Six identical *AVR*s, each one directly controlling its alternator and drawing power from it, by means of permanent magnet generators, installed on alternator shafts, solidly flanged. They are installed in triples into two different cubicles, XM/274EA port and XM/274EB starboard, installed in each switchboard room, together with relevant high voltage switchboard. Names are:

Generator	*AVR*	excitation power source	power supply cable	excitation current	stator current analogue feedback	phase voltage analogue feedback
XA/274A	XM/274EA_1	XM/274EA_1_pmg	H/0000001AEA	H/0000001AFA	H/0000019AGA	H/0000019AJA
XA/274B	XM/274EA_3	XM/274EA_3_pmg	H/0000003AHA	H/0000003AIA	H/0000003AJA	H/0000019ANA
XA/274C	XM/274EB_1	XM/274EB_1_pmg	H/0000002AHA	H/0000002AIA	H/0000002AJA	H/0000019BQA
XA/274D	XM/274EA_2	XM/274EA_2_pmg	H/0000001AMA	H/0000001ANA	H/0000001AOA	H/0000019ARA
XA/274E	XM/274EB_3	XM/274EB_3_pmg	H/0000006AHA	H/0000006AIA	H/0000006AJA	H/0000019BRA
XA/274F	XM/274EB_2	XM/274EB_2_pmg	H/0000004AHA	H/0000004AIA	H/0000004AJA	H/0000019BSA

Table 9: ***AVR***, Tentative Component List

- Two identical PLCs, named XM/274EA_m and XM/274EB_m, acting as power station voltage controllers[60], installed each one in *AVR*s cubicle. They interface with their own power station

[60] They compensate AVR droop in such a way that bus bar voltage always equals the nominal, no matter the load. Reactive power sharing is more a consequence of droop control, rather than their action.

*AVR*s when interconnecting line is open; they switch to hot standby configuration when interconnecting line is closed. In fact they are inessential to voltage control, as it is controlled by *AVR* droop; they provide better voltage quality by eliminating voltage drop generated by inductive loading. This action is carried out, as it is discussed later, biasing generators *AVR*s.

- Six identical speed governors, each one directly controlling its respective diesel engine. Speed governor controllers may be installed on the engine or remotely, enclosed in cabinets, located away from engine rooms, usually in ECR or switchboard rooms. Names are:

Generator	Speed Governor	Power Supply Cable	Battery Charger	BC Power Supply Cable[61]	BC Power Source[61]
XA/274A	XM/274AD	U/B5H0010AAA	FZ/UB5QB	U/B500017AAA	*3.1.2.1 Main Distribution System.*
XA/274B	XM/274BD	U/B5H0011AAA	FZ/UB5QB	U/B500017AAA	*3.1.2.1 Main Distribution System.*
XA/274C	XM/274CD	E/D600010AAA	FZ/9D6QB	E/00000D6AAA	*3.1.2.2 Emergency Distribution System.*
XA/274D	XM/274DD	U/B5H0012AAA	FZ/UB5QB	U/B500017AAA	*3.1.2.1 Main Distribution System.*
XA/274E	XM/274ED	E/D600011AAA	FZ/9D6QB	E/00000D6AAA	*3.1.2.2 Emergency Distribution System.*
XA/274F	XM/274FD	E/D600012AAA	FZ/9D6QB	E/00000D6AAA	*3.1.2.2 Emergency Distribution System.*

Table 10: Speed Governors, Tentative Component List

- Six cubicles containing resistors, grouped into two groups, one per each power station, configured as displayed in Fig. 22. Names are:

Generator	Neutral Point Resistor Cubicle (Resistor & Switch)	Power Cable to Own Neutral Point Resistor	Power Cable to Common Neutral Point Resistor
XA/274A	XM/274A	H/0000001APA	H/0000001AQA
XA/274B	XM/274B	H/0000005APA	H/0000003AVA
XA/274C	XM/274C	H/0000002APA	H/0000002AQA
XA/274D	XM/274D	H/0000003AUA	
XA/274E	XM/274E	H/0000006APA	H/0000004AQA
XA/274F	XM/274F	H/0000004APA	

Table 11: Neutral Point Resistor System: Tentative Component List

[61] This item in fact belongs to Grid/Distribution, but it represents useful information here.

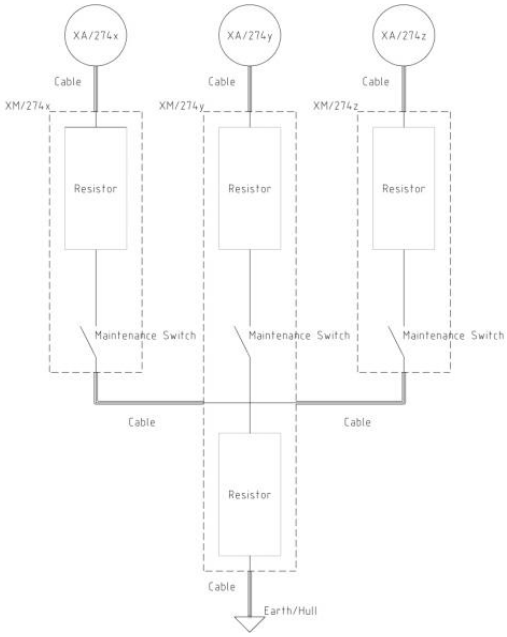

Fig. 22: Exemplificative Earthing Arrangement for One Power Station.

Two identical battery charger panels (batteries are installed within the same cubicle of power conversion), connected in hot standby configuration (auctioning diodes), powered from both main and emergency power supply systems, configured as Fig. 23 illustrates. This system serves both power stations, as figure shows; owing to this peculiarity it will be treated from now on as an independent system, termed **critical electrical power supply system**. Names are:

Battery Charger & Distribution Panel	**B.C Power Supply Cable**	**B.C. Power Source**
FZ/239QB	P/0000039AAA	*3.1.2 Grid/Distribution*
FZ/240QB	F/0000040AAA	*3.1.2 Grid/Distribution*

Table 12: Critical Electrical Power Supply System, Tentative Component List

3.1.1.2 External Electrical Power Supply System

A first coarse decomposition leads to defining following components:

- Two identical shore connections, each one consisting of a cubicle and a transmission line. Names are:

Cubicle	**Cable**	**Connected to:**
XA/877A (Port)	P/0000001ADA	FZ/001TFA
XA/877B (Starboard)	F/0000002ADA	FZ/001TFB

Table 13: Shore Connections, Tentative Component List

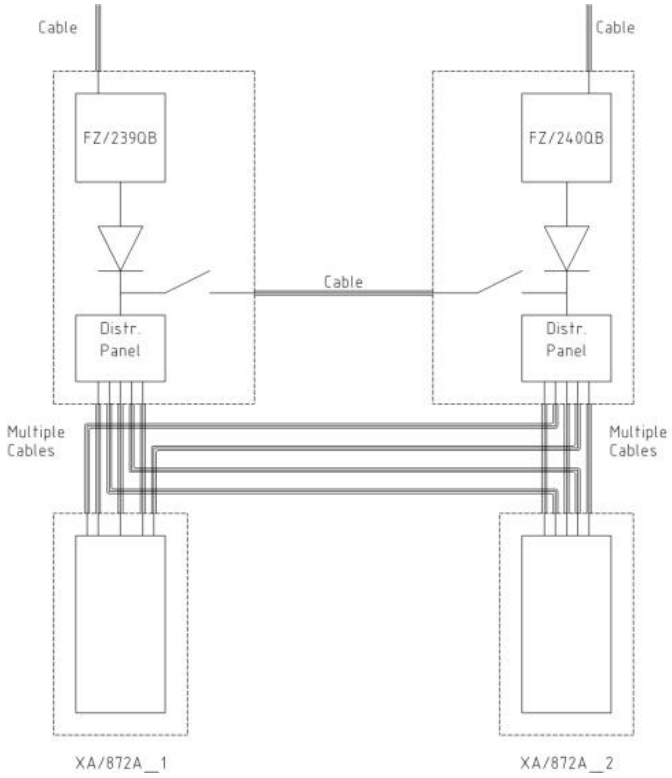

Fig. 23: Main Electrical Power Supply System Critical Power Distribution Arrangement

3.1.1.3 *Emergency Electrical Power Supply System.*

It consists, under a first and coarse decomposition, of:

- A power station, named XA/873A
- Two interconnecting lines, each one coming from a different main low voltage switchboard, in turn consisting of:
  - Port low voltage switchboard XA/872B_1
    - A cable, P/0000003AAA;
    - Two circuit breakers, XA/872B_1_303 and XA/872A_902.
  - Starboard low voltage switchboard XA/872B_2
    - A cable, F/0000004AAA;
    - Two circuit breakers, XA/872B_2_404 and XA/872A_905.

Refining further, power station consists of:

- A diesel driven salient pole synchronous alternator identified as XM/277;
- A transmission line connecting generator to power station, identified as:
  - Circuit breaker XA/872A_901 (protection relay is integrated in the circuit breaker),
  - Cable E/0000001AAA
  - Cable and circuit breaker compartment.
- An *AVR*, usually integrated into alternator casing, named XM/277EA;

- A mechanical speed governor, named XM/277D. This element, given its nature, is regarded as part of the mechanical system, therefore not covered in this work.

It may seem very objectionable here considering interconnecting lines as part of the system; they do not have same relevance interconnecting line has for *Main Electrical Power Supply System* (no associated bidirectional power flow, etc.). Such choice has been made to preserve consistency, but a different one could have done, i.e. including transmission lines within *Grid/Distribution* defined in the following.

3.1.1.4 Transitional Electrical Power Supply System.

It consists, under a first and coarse decomposition, of a power station, named FZ/909QB connected to the Emergency Electrical Power Supply system by means of a transmission line, named after the cable, E/0000009AAA. This power station is not involved in the scope of this study, and is therefore not decomposed further.

3.1.2 Grid/Distribution.

This system fulfils the task of distributing electrical power to users, linking therefore electrical power supply system to users/loads. Following on the definition, components belong to the system are:

- High Voltage Switchboard bus bar compartments;
- Transformer feeders together with their relevant direct controls (protection relays and relevant instrumentation), cable and circuit breaker compartments;
- Low voltage transformer incomers, with their associated direct controls;
- Low voltage bus bars;
- Interconnecting lines (reference is made to *1.3.1.1*, where this element is defined) between the above mentioned components.
- All associated direct controls.

3.1.2.1 Main Distribution System.

With reference to the notional *IPS* and to Fig. 2 and Fig. 3, a first and coarse decomposition may hypothesize four components:

- An 11kV system.

- A 690V system. This system is further broadly functionally subdivided into engine room and accommodation sub-systems. 690V engine room offers a partial backup to 690V accommodation (FZ/001TFC power)
- A 450V system. This system covers special users, such as galley and laundry.
- A 230/120V system.

These components are interconnected by means of transformers and/or transmission and/or interconnecting lines[62].

Developing decomposition one further level, systems mentioned before may be seen as consisting of:

- 11kV system:
  - 11kV_1 (port) and 11kV_2 (starboard) sub-systems (bus bar compartments).
- Five transformer-interconnecting lines[62] (from 11kV to 690V engine room), namely: FZ/001TFA to FZ/001TFC, FZ/002TFA to FZ/002TFB. Three[63] of them are connected to port 11kV system, and remaining three to starboard. FZ/001TFC is a spare line backing up 690V engine room in case of failure of any of the 11kV systems.
- Eight transformer-interconnecting lines (from 11kV to 690V accommodation), namely: FZ/006TFA to FZ/006TFG and FZ/003TF. Four of them are connected to port 11kV system, whereas remaining four are connected to starboard.
- One transformer interconnecting line (from 11kV to 450V), namely: FZ/003TF.
- Eight transformer-interconnecting lines (from 11kV to 230V), namely FZ/006TFA to FZ/006TFG and FZ/003TF. Those lines have same names of 690V because transformer is of three windings type.
- 690V system:
  - 7 bus bar sub-systems: XA/872B_1 to XA/872B_5, FZ/319QF, FZ/418QF, located in the engine room. This is in fact the previously defined engine room sub-system.
  - 7 bus bar sub-systems: FZ/001QP1A to FZ/001QP7A, located in the accommodation area. This is in fact the previously defined accommodation sub-system.
  - Interconnecting lines as per Fig. 3.
- Three transformer-interconnecting lines (from 690V to 450V), namely: FZ/009TFA, FZ/009TFB and FZ/012TF. All these three lines are connected to 690V engine room sub-system.
- Seven 690/230V transformer-interconnecting lines (from 690V accommodation to 230V), namely FZ/007TFA to FZ/007TFG.
- One 690/208V transformer interconnecting line (from 690V engine room to 208V), namely FZ/428QF. This line serves special loads (entertainment).
- Eight 690/120V transformer-interconnecting lines (from 690V accommodation to 120V), namely: FZ/008TFA to FZ/008TFG and FZ/428TF.
- 450V system
  - Two main bus bar systems: FZ/470QFA and FZ/002QP1A.
- 230V system:

[62] It is worth at this point defining a new entity: the **transformer-interconnecting line**. This entity is the set of a primary transmission line (breaker & cable), a transformer and a secondary transmission line (cable & breaker). This entity is named after transformer piece number. There might be particular cases in which secondary transmission line degenerates into a cable only; those cases are dealt with when they occur.

[63] FZ/001TFC is counted twice, as it is connected to both 11kV systems.

  - Nine bus bar systems: FZ/001QP1B to FZ/001QP7B, FZ/002QP1B and FZ/470QFB.
- 208V system:
  - One bus bar system: FZ/428QF.
- 120V system:
  - Nine bus bar systems: FZ/001QP1C to FZ/001QP7C, FZ/002QP1C and FZ/493QFB

3.1.2.2 Emergency Distribution System.

With reference to the notional *IPS* and to Fig. 2 and Fig. 3, a first and coarse decomposition may hypothesize three components:

- A 690V sub-system,
- A 230V sub-system.

These components are connected by means of transformers and/or transmission and/or interconnecting lines.

Developing decomposition one further level, systems mentioned before may be seen as consisting of:

- 690V sub-system:
  - One bus bar system: XA/873A,
- Two transformer-interconnecting lines (from 690V to 230V): FZ/011TFA and FZ/011TFB.
- 230V sub-system:
  - One bus bar system: XA/873B.
- One interconnecting line (from 230V to 230V AC/DC): XA/873B_9C3.

3.1.2.3 Transitional Distribution System.

With reference to the notional *IPS* and to Fig. 2 and Fig. 3, this system consists of only one bus bar system: XA/873B_ACDC.

3.1.3 Integrated Automation System.

System is divided into two main parts, as explained in *1.3.4*: direct control, as detailed in *1.3.4.1*, *1.3.4.2* and *1.3.4.3*; and *SCADA*, as defined in *1.3.4.4*.

Functions of interest pertaining to direct control and *SCADA* are listed and detailed, in their actual implementation (coherently with scope of this work), in following paragraphs.

3.1.3.1 Direct Controls.

Generator Voltage Control.

This function, accomplished by AVRs, which component list is developed in *3.1.1.1*, has four main purposes:

- Keeping generator voltage within tolerance at load variations,
- Share reactive load with other generators in a proportionate manner,
- Protect alternator rotor from sustained over-current,
- Support short circuit current to promote discrimination.

Actual implementation slightly differs from system to system: main and emergency power supply sub-systems, being based on rotating alternators, make use of digital *AVR*, in turns using dedicated voltage (three phase) and current (one phase) transducers[64]; transitional power supply sub-system, as opposed, using battery bank, resources to *UPS* electronic circuitry, which uses embedded voltage and current transducers, placed both at load and source end.

More in detail, main power supply sub-system *AVR*s, consisting of a source of electrical power, a permanent magnet generator, a digital controller with embedded power output stage, perform a dual loop PID control ([**22**], [**23**]): the inner loop, or machine voltage control, is performed by alternator AVRs detecting actual machine voltage, comparing it with a hard coded reference and computing output; the outer loop, or reactive power control, is performed by master AVRs, reading each active generator reactive power via dedicated reactive power converters, installed in high voltage switchboards, computing proportional reactive load and using it as reference to bias alternator AVRs voltage reference (summing to hardcoded value) to obtain desired output value. Outer loop is activated upon circuit breaker closed signal; network extension is defined by interconnecting line status signal (open means sharing network coincides with a power station, closed means sharing network coincides with two power stations). Both control loops are equipped with reference limit software blocks and associated dynamic, so that machine voltage and reactive power may not exceed continuatively hard coded limits, even though a transient is permitted.

Emergency power supply sub-system is configured so that its alternator is not to run in parallel with any other alternator: in this case reactive load sharing circuitry is of no purpose and it is not installed. AVR power source in this implementation comes directly from alternator itself via shunt-excitation.

Transient power supply sub-system is configured so that its source of power is not to run in parallel with any other source of power, therefore there is no need of load sharing circuitry. Power from control circuitry is drawn directly from battery bank.

Instrumentation is installed within generator casing and switchboard cable compartment, or in the converter cabinet (transient power supply sub-system). *Main Electrical Power Supply System AVR*s are installed in dedicated cabinets located in electrical rooms containing main switchboards; *Emergency Electrical Power*

[64] A transducer differs from a sensor because calculations are made. A power transducer measures voltages and currents and calculates power; such power then is relayed as a different signal in its physical essence, say 4 – 20mA. A voltage sensor, as opposed, senses an AC voltage and return an AC voltage, for instance, differently scaled.

Supply System AVR is installed within emergency switchboard, typically. Cables connect all components together. There is no direct fault detection for instrumentation built in this system, but only indirect: a fault in voltage feedback signal causes severe over-excitation or PWM control malfunction; a fault in interconnecting line status signal may cause incorrect reactive power sharing. An in deep analysis of *AVR* system failure modes are beyond the scope of this work, which anyway is to account for faults depending on chosen architecture; for example a redundant instrumentation scheme (based upon design diversity: detecting excitation current at no load may permit line voltage backwards calculation, using no load characteristic) is an architectural choice and its consequences may be analysed in this context.

Generator Frequency Control.

This function, accomplished by speed governors, has three main purposes:

- Maintain alternator frequency within tolerance as load varies,
- Share active load proportionally.
- Assist engine starting and stopping, providing appropriate fuelling.

Actual implementation slightly differs from system to system: *Main Electrical Power Supply System* and *Emergency Electrical Power Supply System*, being based on rotating alternators, make use of digital or mechanical speed governors, in turns using dedicated speed sensors (inductive pickups placed on flywheel) and active load (kW) transducers; transitional electrical power supply sub-system, as opposed, using battery bank, resources to *UPS* electronic circuitry, which uses embedded voltage and current sensors, placed both at load and source end.

More in detail, *Main Electrical Power Supply System* speed governors, consisting each of a digital controller with embedded power output stage, powered from a dedicated battery charger, suitable for driving a fuel rack actuator (usually a step or DC motor), perform a dual loop PID control: the inner loop, or machine speed control, is performed by alternator speed governors detecting actual alternator frequency, comparing it with a hard coded reference and computing output; the outer loop, or active power control, is performed by all participating speed governors, reading each other active generator active power and interconnecting line status via dedicated ring net field-bus, computing proportional active load and using it as reference to bias its own speed reference (summing to hardcoded value) to obtain desired output value. Outer loop is activated upon circuit breaker closed signal; network extension is defined by interconnecting line status signal (open means sharing network coincides with a power station, closed means sharing network coincides with two power stations). Both control loops are equipped with reference limit software blocks and associated dynamic, so that alternator speed and active power may not exceed continuatively hard coded limits, even though a transient is permitted.

Speed governor is usually installed in the same hardware prime mover control system is, so it is considered as integral part of it.

Emergency power supply sub-system is configured so that its alternator is not to run in parallel with any other alternator: active load sharing circuitry is of no purpose and it is not installed. Speed governor, in this installation, is of hydraulic type, and draws mechanical power from prime mover.

Transient power supply sub-system is configured so that its source of power is not to run in parallel with any other source of power, therefore there is no need of load sharing circuitry. Power from control circuitry is drawn directly from battery bank.

Instrumentation is installed within generator casing, when present; or in the converter cabinet (transient power supply sub-system).

Power transducers for *Main Electrical Power Supply System* are installed within *IAS*.

Main Electrical Power Supply System speed governors are installed in dedicated cabinets located in electrical rooms containing main switchboards; *Emergency Electrical Power Supply System* speed governor is installed directly on prime mover.

This system provides partial instrumentation fault detection: speed signal is to be received within a certain time delay after prime mover cranking, should it not be received, starting procedure is aborted; this fault is indirectly detected by observing the consequences. Fault in active power signal implies switching to droop control. Inconsistent power signal, due to wrong calculation or a fault at sensor input (power signal is in fact the output of a sensor) is not detected at all. Field-bus fault causes isochronous control to be aborted, in favour of a droop control; this fault is then directly detected. Power failure causes fuel rack to return to zero, and consequently prime mover stops; this failure is directly detected by means of an appropriate power relay.

Cables connect all components together.

Generator Connection Control.

This function, accomplished by six synchronisers supplied from critical power source, is relevant to *Main Electrical Power Supply System* only, and has three purposes:

- Allowing generator connection when its frequency and voltage shift angle are both within tolerance limits, hard coded in the relays. This purpose is further defined in [**24**], code 25.
- Generating speed increase or decrease pulses to bias generator speed governors to obtain desired frequency and shift angle. This purpose is further defined in [**24**], code 15.
- Manage synchronisation between power stations (closing of the interconnecting line).

Synchronising relay detects bus bar and generator actual voltage, computes frequency difference and angle shift and generate a pulse train that incoming alternator speed governor executes. Once those parameters fall within pre-determined hard coded limits, synchroniser generates a closing pulse, which drives breaker circuitry to close. Synchronising relay is activated by *IAS* when incoming alternator has reached rated speed (detected by speed governor system) and deactivated at the end of synchronisation, detected by breaker closed feedback.

Instrumentation, consisting of potential transformers, is installed within cable compartment (generators) and bus bar compartment (interconnecting line). Synchronising relays are installed in generator control cubicles. This implementation does not offer direct instrumentation fault detection, but partial and indirect: no signal from potential transformers causes synchronisation not to happen successfully; this occurrence is

detected via a timer measuring delay from synchronisation beginning: if breaker close feedback is not received within an agreed timeframe, synchronisation is aborted and operators' attention reclaimed. Untimely synchronism detection (releasing permit to close) can cause severe damages to equipment and a specific safety hazard. Missed breaker closed feedback, or interconnecting line status may cause active power control to perform incorrectly.

Power station synchronisation, in this particular project, is only possible when a power station is supplied with one generator only, so to make use of its synchronising relay. As regards to failure modes, it can be retained that generator synchronisation failure modes may be applied to interconnecting line.

Power source is drawn from power station critical electrical power supply; power failure would cause no synchronisation to take place.

Generator Protection.

This function, accomplished by protection relays and relevant instrumentation, one per each generator, has the purpose of preserving generator from protracted abnormal operation. As generator operation is defined by values of stator voltage and current, excitation current, insulation and frequency, abnormal operation is defined as any operation during which design values of above mentioned main parameters are exceeded.

Protection relays detect stator currents (three phases), zero sequence current and star voltages (three phases), compute actual active and reactive load, frequency and insulation, and directly trip circuit breaker in case values exceed design limit for an unacceptable amount of time. Installed protective functions are, according to [**24**], code 27, 32, 40, 46, 50, 51, 59, 67N, 81, 87G and *AFD*. Their specific actions aim at preserving service continuity, via a discriminative logic. Over-current protections 50 and 51, for instance, are set to pick overloads (50) and short circuits (51); 51 causes interconnection line to trip first, to isolate faulty station, and after that the affected element is disconnected[65]. 50 causes only the affected breaker to trip.

Protection relays are power from power station critical power supply, and are designed to stay put in case of power failure, e.g. breaker position is not affected by protection relay loss of power. Protection relays health is monitored by *IAS*.

Instrumentation is installed within alternator incoming cubicle cable compartments. This system offers no direct instrumentation fault detection, but partial, indirect detection: current or voltage transformer fault (open circuit), for example, coincides with a deactivated alternator, the two conditions being impossible to be discriminated (at least at this system level and within an appropriate timeframe); *AFD* is directly light actuated, therefore, besides a power fault relay, there are no means of ascertain light detectors are operating. More in general, direct instrumentation fault detection consists entirely in power loss detection, where applicable, as indicated in the rules; sensor fault detection is seldom considered. In this specific system problem of defective detection is considered, albeit not in full, and dealt with using design diversity. Solution to a possible inaccurate detection is found in adopting a backup scheme, even though that scheme does not offer a full functional backup. There are in fact three stator earth protections, 67N (installed in any

[65] Absence of voltage prevents a directional detection, as reactive power flows cannot be measured.

alternator incoming cubicle), 64S and 51N (installed in interconnecting line compartments) based on three different pieces of instrumentation, with three different levels of accuracy and information. 67N detects alternator zero sequence current and, together with zero sequence voltage, reconstructs fault impedance and therefore its direction (if upstream the current transformer, so towards circuit breaker and grid/distribution, or downstream, so towards the cables and alternator); 64S is based on a current transformer installed on neutral point common resistor, that simply detects an earth fault, not discriminating direction, and finally 51N detects the star voltages vector sum, if different from zero then an earth fault is active. Sensor fault detection happens, anyway, during fault conditions, and can be considered as a by product of backup protection. Same considerations may include *AFD*, which detects the results of a specifically located earth fault.

Interconnecting Line Protection.

This function, accomplished by protection relays and relevant instrumentation, installed in both high voltage switchboard cubicles, has the purpose of preserving power supply from main internal and external failures. Preservation happens via separation: should any failure having a substantial impact, such to be able of causing complete power outage, then power stations are separated to preserve at least the one failure is not insisting upon, so that it can continue its service. Internal failures under consideration are:

- Short circuits and earth failures in the interconnecting line.
- Phase to phase short circuits (symmetrical failures).
- Control failures inducing excessively high or low system frequency or voltage.

External failures are:

- Short circuits and earth failures within *Grid/Distribution*.

This function is interconnected via contacts with *Generator Protection*, and so programmed to better achieve the purpose, as explained in *3.1.3.4*.

Protection relays monitor system voltages and current flowing across interconnection lines, generating a trip should any of mentioned parameters exceed design value. *AFD* monitors cable compartments for light development as a consequence of an arc, by means of photometric sensors. Both protection relays and *AFD* are supplied from critical power supply system, and their health is monitored by *IAS*. As anticipated, protection relays are not to trip breakers in case of fault.

Only one interconnecting line breaker is directly operated; the other is simply commanded as a slave to follow its position.

Grid/Distribution Protection.

This function, accomplished by means of protection relays, *AFD* and hardwired logic circuitry, has two main purposes:

- Reducing service disruption to the minimum number of users (failure discrimination),
- Blocking unsafe operations.

Fault discrimination mainly concerns earth failures and short circuits, and develops in three different stages:

- Location detection. A first discriminative step entails locating the failure, qualifying it as external or internal with respect to the system. Earth failure is located by means of directional relays, short circuit by means of differential current relays. Those relays make use of current and voltage transformers installed within switchboards (Grid/Distribution zone) and on board alternators, on neutral point connection. External faults are cleared isolating affected users or alternators.
- Component isolation. All transmission and interconnection lines to faulty component are locked open via a hard wired logic detecting contacts on protection breakers. Interconnection lines are closed to components not interlocked with zero voltage detection active.

As an explanatory example an insulation failure is considered within transformer FZ/001TFA high voltage side (reference to Fig. 2 and Fig. 3): such failure causes a discharge to earth. Fault current flows from alternators, via interconnecting line, through transformer circuit breaker and, via the fault, through the steel and back to alternators via neutral point grounding system. Following signals activate:

- *Electrical Power Supply System*:
  - 64S. Current transformers detect fault current and protection relays activate trip sequence.
  - 67N. Protection relays detect fault as external to electrical power supply system, so possibly located within distribution or users.
- *Grid/Distribution*:
  - 51N activates on transformer-interconnection line only. This signal blocks power station splitting sending an inhibit contact to interconnecting line protection relay (only one circuit breaker is equipped with all protection, other follows its position by means of contacts interchange).
  - Transformer-interconnecting line is open at its high voltage side, fault is cleared and 64S resets[66].
  - Transformer-interconnecting line is open at its low voltage side because of zero voltage detected at its breaker terminals (under-voltage coil installed upstream).
  - XA/872B_1 detects under-voltage without fault (information relayed by FZ/001TFA transformer-interconnecting line).
  - Under-voltage without fault does not interlock interconnecting line from XA/872B_5, which closes, restoring power to XA/872B_1.

As far as blocking unsafe operations, following are advised:

- Avoiding paralleling power stations, possibly not synchronised, on low voltage sub-system, due to high synchronising currents that can arise,

[66] 64S shall be sufficiently delayed to safely allow all discriminative operations.

- Avoiding paralleling with low voltage shore supply,
- Permitting a short load transfer between *Main* and *Emergency Power Supply System*.
- Avoiding transformer energisation via low voltage windings.

Blocking logic is implemented recurring to status contacts and local hardwired logic; for instance high voltage sub-system interconnecting line status is relayed to low voltage sub-system to block all dangerous configurations. Similarly, shore connection contact status interlocks all generators in open positions, as well as interconnecting lines to emergency system.

Short load transfer hardware logic relies on an automatic synchroniser installed in the *Emergency Power Supply System*, activated by voltage presence on interconnecting lines, and a timer that controls emergency generator circuit breaker to unload and open as one of the interconnecting lines is closed[67].

Grid/Distribution Control.

This function controls Grid/Distribution circuit breakers, allowing grid reconfiguration in case of fault. It interfaces with *Grid/Distribution Protection* when comes to manage interlocking conditions. Breaker control happens by means of dry contacts, as power is taken from network or critical power, depending upon service and location. *Grid/Distribution Protection* dry contacts are in series with Grid/Distribution control so that both systems are requested to be operational to perform the service. Plant complexity does not require special strategies; therefore reconfiguration logic reduces to a pool of one stand by unit, T5 in our case study.

Special mention deserves hardware logic managing spare transformer FZ/001TFC. In normal conditions it is supplied by both power stations (interconnecting line closed).

Should interconnecting line open, then both feeders open in turn to avoid paralleling through that line, not suitable for this purpose.

Should one transformer fail, then the feeder belonging to opposite power station (respect to failed transformer) opens, so that load on each power station is maintained constant. Further to that appropriate interconnecting line closes to restore power.

3.1.3.2 SCADA.

SCADA is configured in compliance with *1.3.4.4*; structure of the notional case can be found in Fig. 13. Information is collected by means of local input devices (*I/O*), powered by dedicated central *UPS*s, and relayed to process units for elaboration, via a ring network. Process units calculate control outputs, which

[67] Both interconnecting lines to emergency power generation system cannot be closed at the same times, as they belong to two different low voltage sub-systems, and can possibly carry synchronising current.

are dispatched via the same ring network, back to local devices for execution. Execution is verified by means of feedback signals, which are to come within a pre-determined time lapse. Should execution check fails, the concerned component is declared faulty and unavailable.

System has following duplicated, hot standby components: processing units, network hardware and management, power supply (battery backed up), operator stations together with their relevant input devices. One part, called main, is active whilst the other, called reserve, elaborates inputs but provides no outputs. Reserve becomes active whenever main fails. Main fails when any of duplicated components fails, except operator stations.

In this architecture operator stations have two main functions, in addition to providing awareness to operators: allowing set point change and permit manual control. They are unnecessary to computing control actions.

System functions are listed in *1.3.4* forasmuch this work is aimed at. *IAS* considers a component available when it is set to remote control, and no active faults are detected; *IAS* operates all available components according to programmed functions. More in detail, power management automatic routines are discussed in the following:

- Generator standby. This routine controls standstill available (selected for automatic control) generators. Auxiliary are monitored for readiness and thermodynamic conditions maintained to grant fastest load taking. Forasmuch as this work is concerned, generator standby is active when *Generator Voltage Control*, *Generator Frequency Control* and *Generator Protection* relies contacts indicating their readiness to perform their service[68]. Generator neutral point earthing shall signal resistors are engaged to proceed with excitation so, in the end, this system participates to form the set of conditions for readiness.
- Generator start/stop. This routine controls active and standby generators, in sequence, generating start/stop signals. Generators are started and stopped one by one, following a predetermined, adjustable sequence so that no more than one generator starts connecting to a power station at any time, and no more than one generator starts disconnecting. Start signal is relayed to prime mover control system and to *Generator Frequency Control*. Prime mover control system performs all necessary actions (open starting air valve and fuel rack to start position in case of a diesel engine prime mover, start crank motor and open fuel valve in case of a gas turbine, etc) to bring prime mover to self-sustained speed; *Generator Frequency Control* admits fuel for ignition. A generator is considered started when its speed, measured by its governor or by its prime mover control system, exceed the self sustaining level; from that moment on energy generated by combustion suffices keeping rotation. This condition is notified to *IAS* by means of a contact closing. When the generator is started, prime mover control system deactivates starting components (closes starting air or stops crank motor), while frequency control gradually increases fuel admission to achieve constant acceleration till rated speed. Stopping routine consists basically in reversing all operations described so far: stop signal is relayed to both prime mover control system and *Generator Frequency Control*; the latter reduces fuel admission so that constant deceleration is achieved till the self sustaining level is crossed (this condition being detected by the contact mentioned earlier); from that moment onwards it stops fuel admission. As zero speed is of inaccurate detection, a time

[68] No such feature is available for generator synchronisation system in this project. Its readiness status is assumed, but not detected.

lapse is set within prime mover control system to declare generator stand-still; that time lapse begins when self sustaining level is crossed and, when is elapsed, the generator is considered stand-still. Prime mover control system releases a contact informing *IAS* generator is again ready for start.

- Generator connecting/disconnecting. This routine controls active generators. Once a generator is declared started, and after it has reached its rated speed, indicated by a contact generated either by its *Generator Frequency Control*, or by its prime mover control system[69], *IAS* activates a signal (contact) to *Generator Connection Control*; once conditions are met, closing coil is energised, and a feedback contact (breaker closed) is released. Routine receives feedback contact and deactivates *Generator Connection Control* accordingly.
- Generator replacing. This routine controls active and standby generators, detecting when operating parameters are nearing critical values, generating start/stop signals. Operating parameters in question have slow dynamic, like alternator magnetic core or winding temperature, therefore immediate shut down can be procrastinated for at least the time it takes to bring a stand by generator on line. Course of action can be seen as a composition of routines described above: stand by generator is started upon warning, connected and loaded; faulty generator is then unloaded, disconnected and stopped. Needles to say, faulty stopped generator will not be considered part of stand by pool, as its operational parameters do not fall within stand by range for a reason that requires investigation.
- Generator load dependant start/stop. This routine controls active and stand by generators, generating start/stop signal based upon active load. Starting or stopping signals are computed basing upon actual power and status signals coming from active generators: if any of automatically controlled generators indicates its output power has exceeded a predetermined, adjustable (via HMI) threshold for a predetermined amount of time[70], then an additional stand by generator is started; if all of automatically controlled generators indicate their output has fallen below a predetermined, adjustable threshold for a predetermined amount of time, then an active generator is stopped.
- Power request. This routine controls users having power comparable with that of a generator (often called **heavy consumers**). A user designated as heavy consumer can only connect if available power is sufficient to supply it; to that extent, before starting, that user sends a contact requesting power. *IAS* keeps user power requests recorded in a database and checks if active generators can cover actual request; if they can a contact is returned to user allowing connection, otherwise a new generator is started, and then, once connection has taken place, request is granted. *IAS* controls interconnecting line status too, so that power request can be addressed to correct power station, and appropriate start actions can be taken.
- Active power limitation. This routine controls certain users in such a way to maintain power supply system within design values limiting their consumed power. Power limitation routine is power station sensitive, and addresses power reduction to users connected to the power station suffering output limitation. Absorbed power is controlled in two different manners:

[69] Rated voltage condition is not checked explicitly. Generator connection control verifies incoming generator voltage matches with network voltage, without informing operators on reasons why matching is not achieved.

[70] Sometimes a power/time inverse characteristic is used: the severest the overload, the fastest the reaction.

  - By sending a power available signal to every user that has the possibility of controlling its power consumption. Such users are: propulsion system, that controls absorbed power by controlling shaft rotational speed; chilled water generation system, that controls absorbed power by controlling cryogenic gas pressure at the end of expansion, and ventilation system, that controls its power in the very same manner propulsion system does. Power available signal is a scaled signal that determines percentage of rated power a user can draw in any specific moment: it may become low due to a fault affecting one generator, and it may return high after standby has been brought on line. Power available per single generator is calculated deducting actual generated power from actual rated active power[71]; power station power available is the sum of relevant generator power available and finally supply system power available is the sum of power station available powers.
  - By sending a trip signal to unessential and unimportant users. In this way their absorbed power is zero. Trip signal is conveyed by *IAS* remote *I/O* unit and executed by hardware logic in the affected user (supply breaker). Trip signals need generally operator reset, so once this action is executed, there is no automatic restoration. This sub-routine is often called **Preferential Trip**.
- Interconnecting line management. This routine controls interconnecting line and, eventually, active generators to join power stations. System detects configuration and, if it allows synchronisation (there should be a power station with one generator only connected), activates concerned sub-systems: *Generator Connection Control* and interconnecting line circuit breaker control. The latter consists only in sequencing order so that master is operated before slave.
- Black out recovery. This routine controls standby generators, *Grid/Distribution Protection* and *Grid/Distribution Control*. In case a blackout happens, routine starts all stand-by generators. First generator to start is in fact the first generator that connects. Once high voltage sub-system, that can be split or joint, is alive again (condition detected by protection relays and derived by status contacts), transformer-interconnecting lines are closed by *Grid/Distribution Control*. Once the entire *Grid/Distribution* is alive again, then users are connected to restore configuration recorded before black out

3.2 Modes of Functioning.

Notional *IPS* has three main functioning modes, with their relevant sub-modes. Such modes are originated in the technical specification, and correspond to configurations most used for trading of the vessel. Expected load in any of those modes influences prime mover sizing and *IPS* architecture. More in detail harbour operation determines prime mover rating, as it is considered best efficiency is achieved with only one prime mover active, at its best loading point; whilst open sea, and its relevant service speed, determines the number [**12**].

[71] Actual rated power may differ from rated power due to ageing, running in or fouling effects. Such effects may be accounted for giving operators chance to set a de-rating factor. Furthermore, operators may want that a constant amount of power is reserved (not used) to avoid stressing prime movers.

3.2.1 Harbour.

This mode is entered when vessel is moored alongside and performs loading/unloading operations of passengers and goods.

This mode has generally two different sub-modes, namely: vessel generator or shore connection. Inasmuch as systems are concerned, table shows their expected status according to chosen sub-mode.

System	Sub-System	Main Power Supply Used	External Power Supply Used
Electrical Power Supply System.	*Main Electrical Power Supply System.*	Active	Stand-by
	External Electrical Power Supply System	Inactive	Active
	Emergency Electrical Power Supply System	Ready for service	Ready for service
	Transitional Electrical Power Supply System.	Ready for service	Ready for service
Grid/Distribution.	*Main Distribution System.*	Active	Active
	Emergency Distribution System.	Active (supplied by main power supply)	Active (supplied by external power supply)
	Transitional Distribution System.	Active (supplied by main power supply)	Active (supplied by main power supply)
Integrated Automation System.	*Generator Voltage Control.*	Ready for service	Ready for service
	Generator Frequency Control.	Ready for service	Ready for service
	Generator Connection Control.	Ready for service	Ready for service
	Generator Protection.	Active	Ready for service
	Interconnecting Line Protection.	Active	Active
	Grid/Distribution Protection.	Active	Active
	Grid/Distribution Control.	Active	Active
	SCADA.- Generator Stand by	Active	Active
	SCADA.- Generator Start/Stop	Active	Inactive
	SCADA.- Generator Connect/Disconnect	Active	Inactive
	SCADA.- Generator Replacing	Active	Inactive
	SCADA.- Generator Load Dependant Start/Stop	Active	Inactive

System	Sub-System	Main Power Supply Used	External Power Supply Used
	SCADA.- Power Request	Active	Inactive
	SCADA.- Power limitation.	Active	Inactive
	SCADA.- Interconnecting line management	Active	Active
	SCADA.- Black out recovery	Active	Active
Users	Propulsion	Inactive	Inactive
	Steering Gear	Inactive	Inactive
	Services to Passengers and Crew	Active	Active

Table 14: Harbour Mode, List of Systems and Relevant Statuses

3.2.2 Manoeuvring.

This mode is entered when vessel is still moored alongside and prepares for departure, or when initiates entrance to a port of call (pilot on board).

This mode has a sub-mode, called dynamic positioning. In this notional application, dynamic positioning is a non-classified mode, therefore not subject to all relevant and extensive corpus of requirements; the existence of it is reported owing to its prominent importance in different field of ship operations, like Oil and Gas, just to mention one. Furthermore, more and more cruise vessels are equipped with it, owing to more stringent environmental requirements aimed at preserving coral reefs from detrimental actions coming from anchors. Such areas are valuable for the cruising industry, and the industry invests in compliance with laws and rules.

This mode possesses an inherent sensitivity deriving from the fact that it is activated in congested areas and shallow waters; any loss of manoeuvring capability is likely to produce a collision. Other vessels or land structure may be involved, with significant losses. This sensitivity privileges conservative choices; many operators, in fact, manoeuvre with split power supply and distribution system.

Inasmuch as systems are concerned, following are expected to be operational:

System	Sub-System	Manoeuvring	Dynamic Positioning
Electrical Power Supply System.	*Main Electrical Power Supply System.*	Active	Stand-by
	External Power Supply System	Inactive	Inactive
	Emergency Electrical Power Supply System.	Ready for service	Ready for service

	Transitional Electrical Power Supply System.	Ready for service	Ready for service
Grid/Distribution.	*Main Distribution System.*	Active	Active
	Emergency Distribution System.	Active (supplied by main power supply)	Active (supplied by main power supply)
	Transitional Distribution System.	Active (supplied by main power supply)	Active (supplied by main power supply)
Integrated Automation System.	*Generator Voltage Control.*	Active	Active
	Generator Frequency Control.	Active	Active
	Generator Connection Control.	Active	Active
	Generator Protection.	Active	Active
	Interconnecting Line Protection.	Active/Indifferent if mode has split power stations	Active/Indifferent if mode has split power stations
	Grid/Distribution Protection.	Active	Active
	Grid/Distribution Control.	Active	Active
	SCADA.- Generator Stand by	Active	Active
	SCADA.- Generator Start/Stop	Active/start only	Active/start only
	SCADA.- Generator Connect/Disconnect	Active/Generator start only	Active/Generator start only
	SCADA.- Generator Replacing	Active	Active
	SCADA.- Generator Load Dependant Start/Stop	Active/Load Dependant Start only	Active/Load Dependant Start only
	SCADA.- Power Request	Active	Active
	SCADA.- Power limitation.	Active	Active
	SCADA.- Interconnecting line management	Active/Indifferent if mode has split power stations	Active/Indifferent if mode has split power stations
	SCADA.- Black out recovery	Active	Active
Users	Propulsion	Active	Active
	Steering Gear	Active	Active
	Services to Passengers and Crew	Active	Active

Table 15: Manoeuvring Mode, List of Systems and Relevant Statuses

3.2.3 Open Sea.

This mode is entered when pilot left the vessel, and it is maintained till the next port of call. Ship proceeds at service (trading) speed, for which it is designed. Power stations are kept joined to exploit maximum fuel economy. This notional *IPS* is designed to trade with five active generators, while the sixth is kept as stand by unit.

Inasmuch as systems are concerned, following are expected to be operational:

System	**Sub-System**	**Open Sea**
Power Supply System.	*Main Electrical Power Supply System.*	Active
	External Power Supply System	Inactive
	Emergency Electrical Power Supply System.	Ready for service
	Transitional Electrical Power Supply System.	Ready for service
Grid/Distribution.	*Main Distribution System.*	Active
	Emergency Distribution System.	Active (supplied by main power supply)
	Transitional Distribution System.	Active (supplied by main power supply)
Integrated Automation System.	*Generator Voltage Control.*	Active
	Generator Frequency Control.	Active
	Generator Connection Control.	Active
	Generator Protection.	Active
	Interconnecting Line Protection.	Active
	Grid/Distribution Protection.	Active
	Grid/Distribution Control.	Active
	SCADA.- Generator Stand by	Active
	SCADA.- Generator Start/Stop	Active
	SCADA.- Generator Connect/Disconnect	Active
	SCADA.- Generator Replacing	Active

System	Sub-System	Open Sea
	SCADA.- Generator Load Dependant Start/Stop	Active
	SCADA.- Power Request	Active
	SCADA.- Power limitation.	Active
	SCADA.- Interconnecting line management	Active
	SCADA.- Black out recovery	Active
Users	Propulsion	Active
	Steering Gear	Active
	Services to Passengers and Crew	Active

Table 16: Open Sea Mode, List of Systems and Relevant Statuses

3.3 Definition of Case Scenario.

Dependability techniques are applied to a specific group of systems in a specific configuration. These pieces of information define the case scenario.

Notional *IPS* is analysed in its *Open Sea* configuration, and relevant systems and sub-systems involved are defined in Table 16. Focus is placed on *Main Electrical Power Supply System*, and its relevant controls. Furthermore vessel is trading at service speed, with its payload on board[72]. Weather conditions are per design: sea state calm, normal air and sea water temperature. Systems onboard are supposed to operate normally.

3.3.1 Hypoteses.

As per electrical load balance and contractual stipulations configuration stated in *Forewords* is further defined:

- *Power Supply System*:
  - 5 generators active

[72] Sometimes cruise ship move a trading speed without passengers; these occurrences may happen when port of call is changed because of the season (relocation cruise) or resuming service after a dry dock, or a main maintenance event requiring trading suspension.

    - Interconnecting line closed. This condition is imposed by propulsion system: in light of crossing connections shown in Fig. 2; appropriate pulse reaction (24 pulses) can only be achieved if power stations are synchronised. Should they be not, full power is not available.
- *Grid/Distribution*:
    - Bus bars split, each one supplied by its own transformer. In other words, it can be said that transformer-interconnecting lines are closed.
    - Spare transformer supplied by both power stations.
    - Interconnecting lines open
- *Integrated Automation System*:
    - Direct controls operational,
    - *SCADA* operational.
    - *IAS* remotely and automatically controls *Power Supply System* and *Grid/Distribution*.

3.3.2 Symplifying Assumptions.

Followings simplifying assumptions are made:

- Faults are assumed as such, they are not classified in this context.
- Safe return to port casualties (see *1.3.5*) are too severe to be applied to the case in subject, therefore are not considered.
- Components are assumed to be enclosed and separated in a way that blocks fault propagation. A fault in a sub-system affects all sub-systems functionally dependent upon it, and no others.
- Manual control, both remote and local, is not considered. In this context focus is directed towards automated operation.
- *SCADA* is not requested to initiate load dependant action, as load is supposed to be stable enough not to cause a variation in generating unit number.
- *SCADA* is identified with the computer(s) executing its code. Code development faults are not considered in this work.
- *Emergency Power Supply System*, *Transitional Power Supply System*, *Emergency Distribution System* and *Transitional Distribution System* are not included in the model.
- Machinery dimensioning is considered suitable for the expected load.

3.3.3 Threats.

Threats are sought within applicable classification society rules, international rules and ship owner technical specification. Following occurrences are found [**25**]:

- [**5**], Pt.4 Ch.8 Sec.2 specifies that any single failure shall not render duplicated consumers serving essential or important services inoperable. The threat can then be identified as a fault in any

component belonging to a generator set (under the assumption generator sets are replicated system); the expected system reaction is that no elements belonging to other generators are affected.

- Technical specification. Power supply system shall be joined to develop maximal propulsion power, needed in the configuration under investigation. In terms of components this requirement may be translated in the necessity of a path connecting power station 1 with power station 2.
- Technical specification. Power to users shall be granted to maintain comfort. This threat can be expressed as the need that *SCADA* routine "Power Limitation" is active in case of fault affecting power supply system.

More in general threats considered by rules and pertinent to this work (development phase) can be identified in (reference to *2.3.2*):

- Software flaws
- Logic bombs
- Production defects
- Hardware errata
- Physical Deterioration
- Physical interference
- Input mistakes

3.4 Generation of a System Model from the Case Scenario.

A top down approach is adopted, compliant with guidelines explicated in [**21**]. *Fault Tree Analysis* and *Reliability Block Diagram* techniques, described under *2.4.3.2*, are adopted and compared. *FTA* is, towards the case under investigation, less flexible than *RBD*, therefore the latter is preferred when comes to deepen the analysis.

3.4.1 *IPS*, Level Zero.

At a first approximation, in a *RBD* framework, *IPS* has the structure shown in Fig. 24. Number in the box indicates system of belonging.

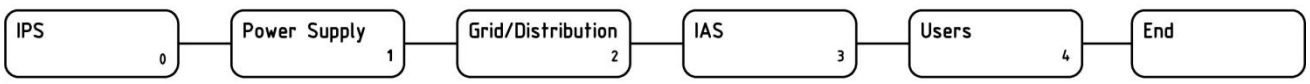

Fig. 24: ***IPS*** Structure, Level Zero Decomposition, ***RBD***

Its relevant fault tree is illustrated in Fig. 25.

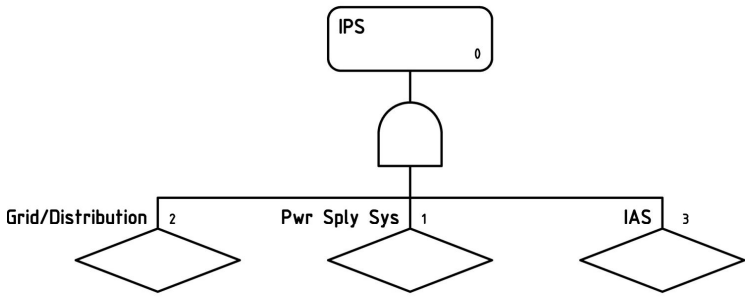

Fig. 25: ***IPS*, Level Zero Decomposition, *FTA***

As stated in *1.2*, worded in accordance with the taxonomy set forth in *2.3.1*, *IPS* service is providing electrical power possessing agreed quality to users[73]. In this respect it can be affirmed *IPS* delivers the expected correct service if *Power Supply System*, *Grid/Distribution* and *Integrated Automation System* (*IAS*)[74] are delivering their respective correct service. In terms of *RBD*, if all blocks are representing sub-systems delivering their expected service, they may be replaced with a link; in this case direct observation shows there is a path linking beginning to end, so system is delivering its expected service. On the contrary, if any single fault disables a sub-system, then the link is broken and system does not deliver its expected service. In terms of *FTA*, it can be appreciated AND gate returns zero value (fault) if any of concurrent blocks return zero. As expected, both diagrams represent same fault dependency.

IAS block location in the *RBD* is convenient, and does not follow the power flow, from generators to users. *IAS* in fact permeates all components, so no strict criteria really apply for its placement, besides functionality. It is worth remembering this is a functional diagram, a specific direction is only chosen for drawing purposes; functional relationship matter.

This level of expansion does not permit drawing conclusion concerning threats mentioned above: a further expansion is needed.

3.4.2 *IPS*, Level One.

Continuing decomposition in accordance with *3.1*, and making reference to modes of functioning discussed in *3.2* and *1.3.1*, diagram shown in Fig. 26 can be drawn. Diagram shows functional dependencies among systems treated in this work in open sea configuration.

[73] To that extent, the “Users” block and the “End” block can be thought as identical to the purpose.

[74] It is worth remembering IAS is the composition of two main entities: direct controls and SCADA. Direct controls are to be made explicit in any diagram; SCADA is more a standalone sub-system, with dedicated hardware and power supply.

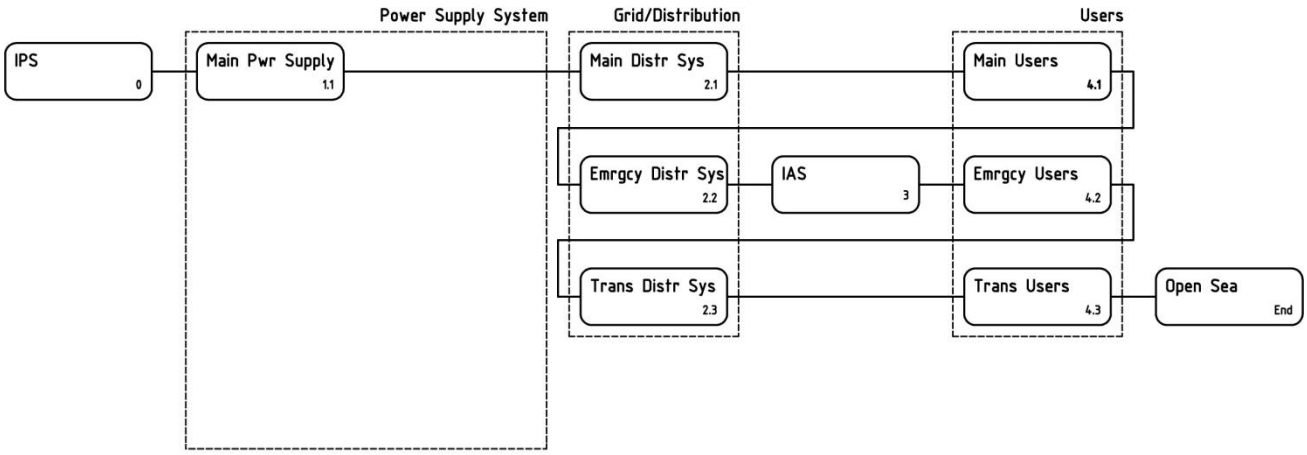

Fig. 26: ***IPS*** **Level 1 Decomposition, Normal Operation, *RBD***

Corresponding *FTA* is shown in Fig. 27.

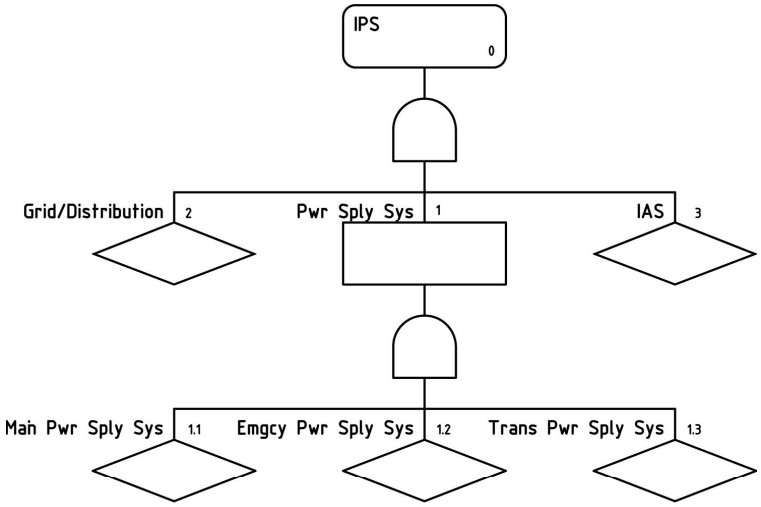

Fig. 27: ***IPS*****, Level 1 Decomposition, Normal Operation, *FTA***

Some explanations are of order:

- As already stated in footnote 73 “Users” blocks could have been placed at the end, and regrouped with the ending block. “Users” blocks could not have placed at all, basing on the consideration that they are entities service is directed to (or, wording differently, users dependability is not subject of this work, but infrastructure dependability). In light of this consideration, they could have been included in the final block. *FTA* is prepared following this latest way of reasoning.
- *IAS* is located within emergency block in the *RBD* for ease of drawings, and in consideration of the fact it is supplied from emergency too. Again functional dependencies are shown here, not topological or other.
- Failures in *RBD* blocks 2.2 and 2.3 would not imply *IPS* reconfiguration, and its consequent ability of delivering the requested service (trading at service speed), but such failures are to be attended at next port of call the latest, if corrective maintenance does not succeed, as safety reasons dictate. Failing to correct the failure would imply the impossibility of continuing trading, and consequently *IPS* failure. Emergency/Transitional power supply system failures can be thought of additional degraded modes *IPS* possesses.
- Numbers in boxes have the meaning explained hereunder:

- First digit indicates zero level system of belonging;
- Second digit indicates first level system of belonging. This means, for instance, that *Grid/Distribution* consists of: *Main Distribution System*, *Emergency Distribution System* and *Transitional Distribution System*; in accordance with *3.1.2*.
- Etc.

In the same line of reasoning, diagram of Fig. 28 can be obtained, when considering emergency operation. As there is no path between beginning (*IPS*) and end (Emergency Operation) passing through blocks 2.1 and 4.1, they are drawn with the only purpose of attracting attention on the necessity of a path that crosses the entire diagram to signify service delivery. The diagram proves, in addition, a certain modularity in obtaining RBDs: once that main system structure is captured, is relatively easy elaborating sub-modes.

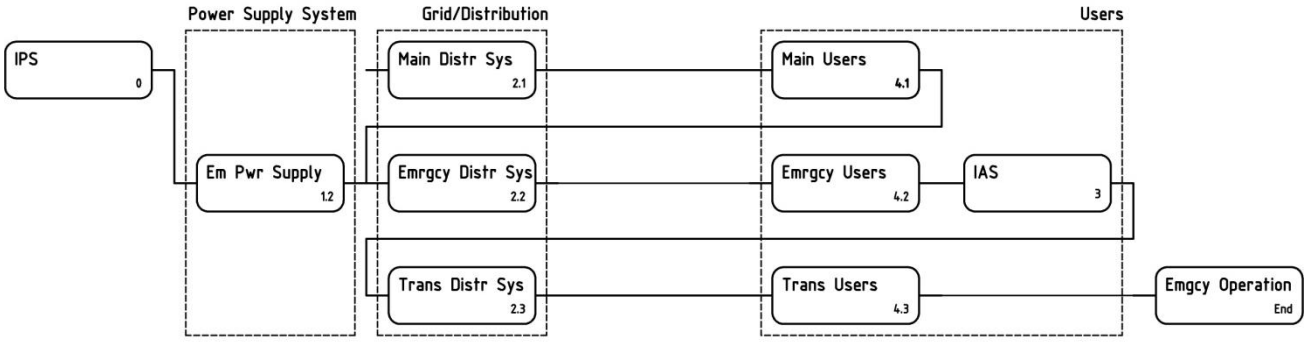

Fig. 28: *IPS*, Decomposition Level 1, Emergency Operation, *RBD*

Again some explanations are of order:

- *IAS* is to be available during an emergency; this is the main reason why it has been located in this way. *IAS* does not perform any control function over *Emergency Electrical Power Supply System* and *Emergency Distribution System*, therefore is appropriate considering it as a user. This point of view only stands as long as *IPS* is considered; in some project, for instance, *IAS* conveys information about flooding conditions to damage control system; those pieces of information are quintessential to emergency management, and must be made available. In this light, and considering a different mode of operation, *IAS* must be moved from its present position to a position so that its complete failure implies abandon ship.
- A failure of blocks 2.3 and 4.3 would force a different planning; in this respect emergency operation is considered aborted in case of such failures given the request of different procedures and management.
- This diagram can be thought as originated from *Main Electrical Power Supply System* failure (corresponding block is indeed removed); in this line of thinking diagram shows a degraded configuration. *Emergency Electrical Power Supply System* can indeed be considered as cold standby power supply for emergency users; which are in turn a sub-set of all users. All users are supplied from either *Main Electrical Power Supply System* or *External Electrical Power Supply System* in all normal situations, or *Harbour*, *Manoeuvring* and *Open Sea.* Being *Main Electrical Power Supply System* and *Emergency Electrical Power Supply System* part of *Electrical Power Supply System*, as per *3.1.1*, degraded configuration refers to *Electrical Power Supply System*.

Fig. 29 shows abandon ship configuration, fruit of the simultaneous failure of *Main Electrical Power Supply System* and *Emergency Power Supply System*. This degraded configuration is maintained for as long as the power supply can be maintained active (*Transitional Power Supply System* consists indeed of a battery bank,

with a limited usable life if not recharged); after that moment vessel is said **dead.** This occurrence is beyond the scope of this work and, in particular, beyond the scope of the analysis in progress; it has been included for illustration purposes on the use of *RBD*s.

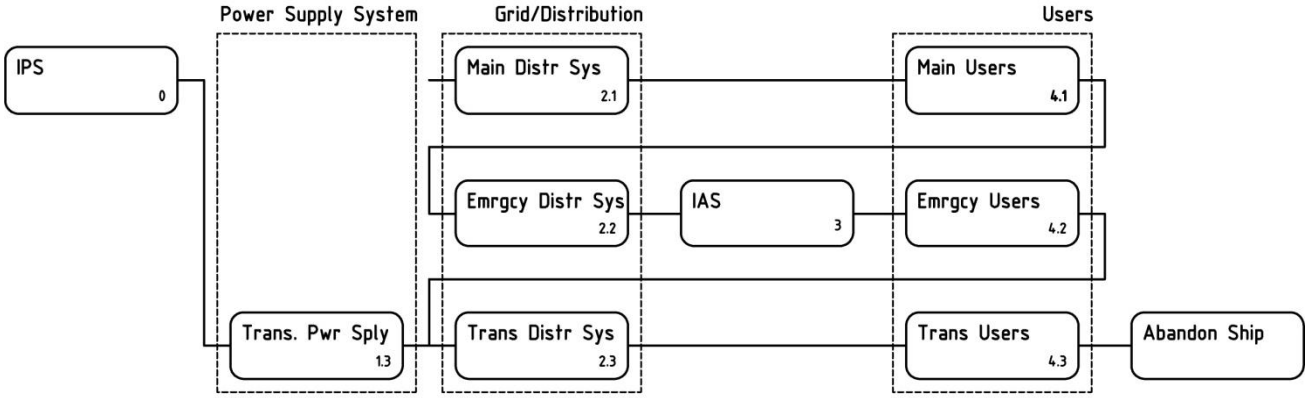

Fig. 29: ***IPS*, Decomposition Level 1, Abandon Ship Operation, *RBD***

IAS block positioning is immaterial in this configuration, as it is not available (no power supply is extended). As already considered, this configuration is entered when both *Main Electrical Power Supply System* and *Emergency Electrical Power Supply System* are failed; this means that no power to actuate controlling devices such pumps or fans is available. Clearly, in that condition, releasing controlling commands would be inessential.

It can be said this configuration is entered when *IAS* fails. In fact, *IAS* failure entails loss of awareness regarding a damage condition, or loss of stability information during a fire fight; without this information vessel is exposed to risk of capsizing, sinking, or enter into a position from which life saving equipment could not be launched successfully. In that condition it would be too dangerous for anybody remaining on board. Another important point of view is to be found in the ability of remote operating devices in the area affected by damage: *IAS* permit continuing fighting the casualty without exposing operators to risks. Should this capacity be lost, then any further fight would expose human life to an unacceptable threat.

Harbour operation is illustrated in Fig. 30. It differs from open sea because of the external power supply and the level of load that can be achieved.

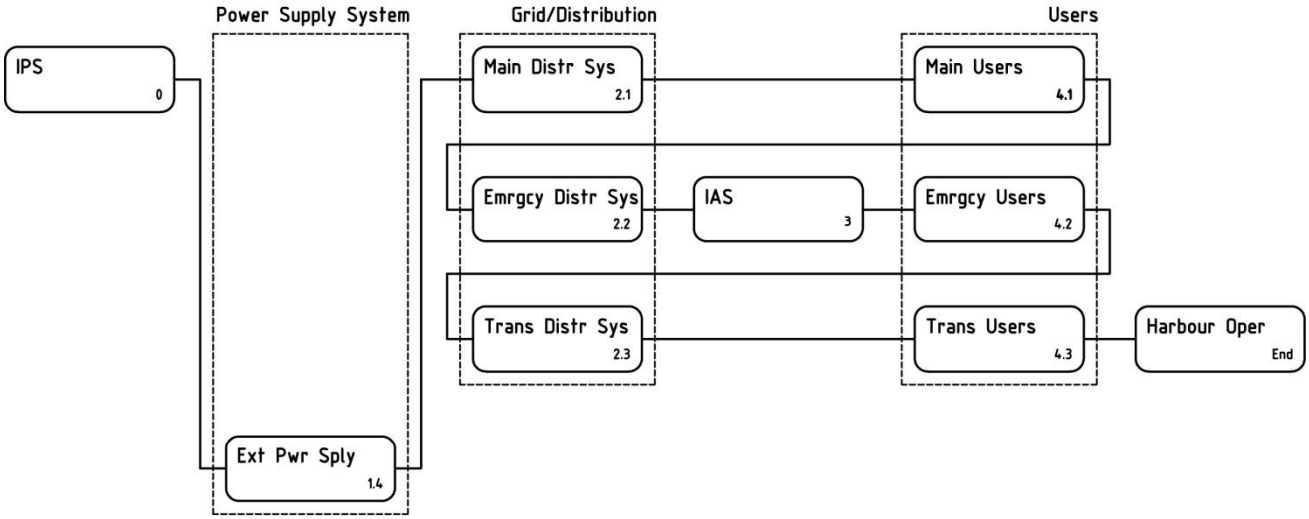

Fig. 30: ***IPS*, Decomposition Level 1, Harbour Operation, *RBD***

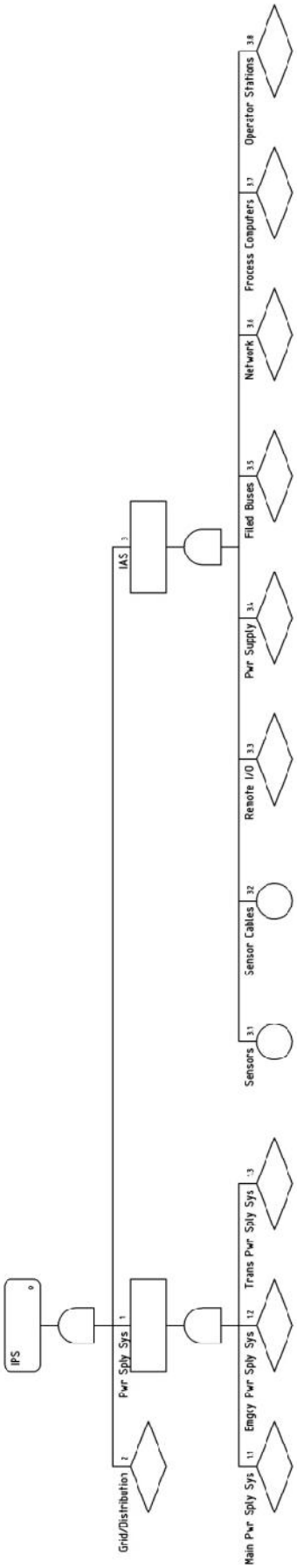

Fig. 31: ***IPS***, Decomposition Level1, ***SCADA***, ***FTA***

SCADA can be decomposed as **Error! Reference source not found.** and Fig. 31 indicate.

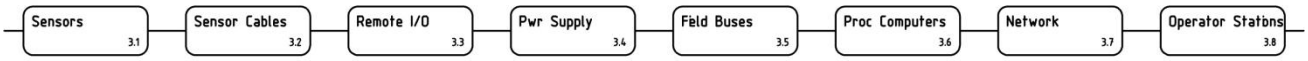

Fig. 32: ***IAS*, Decomposition Level 1, *SCADA*, *RBD***

Diagram is drawn following information path, to which power supply is unessential. Power supply block location, in turn, is immaterial. Its placement is suggested by the consideration that first supply apparatus is the remote *I/O* unit. Still, it is worth stressing the fact these are functional diagrams, and the position of power supply block is to be chosen according to functional dependencies; in this case if that block fails, all other do; fact that coincides with system way of functioning. The fact that power supply fail would not include sensor or cables fail can be retained, but in terms of sub-system functioning, it does not subvert the fact that the information is not relayed, which is sub-system function.

SCADA code is not explicitly mentioned in this decomposition, albeit frequently mentioned in this work. *SCADA* code is indeed software application process computers run. That application permit operator interface and executes programmed control logic, featuring functions described in *3.1.3.8*. Analysis of application code is briefly started in this work, to offer a further possible application of decomposition technique but; in its fullest development cannot be treated here.

3.4.3 *IPS*, Level Two.

Iteration is continued one more step, following direction set forth in *3.1.1.1*, focusing on **Power Supply System** block (item 1.1, Fig. 26), consistently with assumptions. Resulting diagram is shown in Fig. 33.

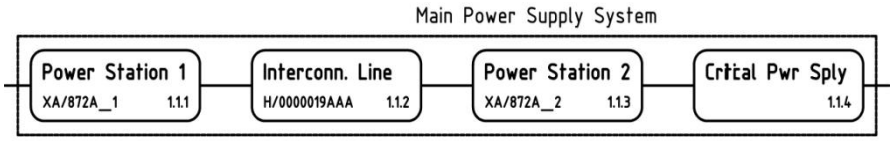

Fig. 33: ***IPS*, Decomposition Level 2, Main Power Supply System, *RBD***

Relevant *FTA* is reported in Fig. 34.

Main Electrical Power Supply System consists indeed of two independent power stations, as requested in *1.3.1.1*, separated by an interconnecting line. For the service under investigation, it is requested both power stations and interconnecting line deliver their correct service.

FTA can as well be developed in **modules**, or group of blocks representing a specific part of the diagram, as done for *RBD*.

IAS is further decomposed as illustrated in Fig. 35 and Fig. 36.

Comments are of order:

- Diagram refers to **sensors** (block 3.1), and it represents the acquisition chain, or the process undertaken to convert sensor measure in a piece of information suitable for processing. Consequently, if a function *RBD* is to be constructed, it is paramount knowing the number of

measures used and their location within *RIO*s. In the case under examination, load dependant start function would require sensors indicated under *3.1.3.8*; diagram is then to be completed putting in series any sensor which measure is required, together with its relevant *RIO*, and connect the series so formed to the acquisition chain, which starts with block 3.4.X. To the extents of this work, a single **Sensors** block suffices (as it can represent a long series, with the same cumulative effect), connected to a single *RIO*. Great majority of signals requested for power management functions are in fact located within switchboard rooms, so two *RIO*s collect them (one per power station); as there is no duplication for *RIO*s, a single block fulfils the purpose, as it can be thought of the series of two equal blocks; the cumulative effect does not change.

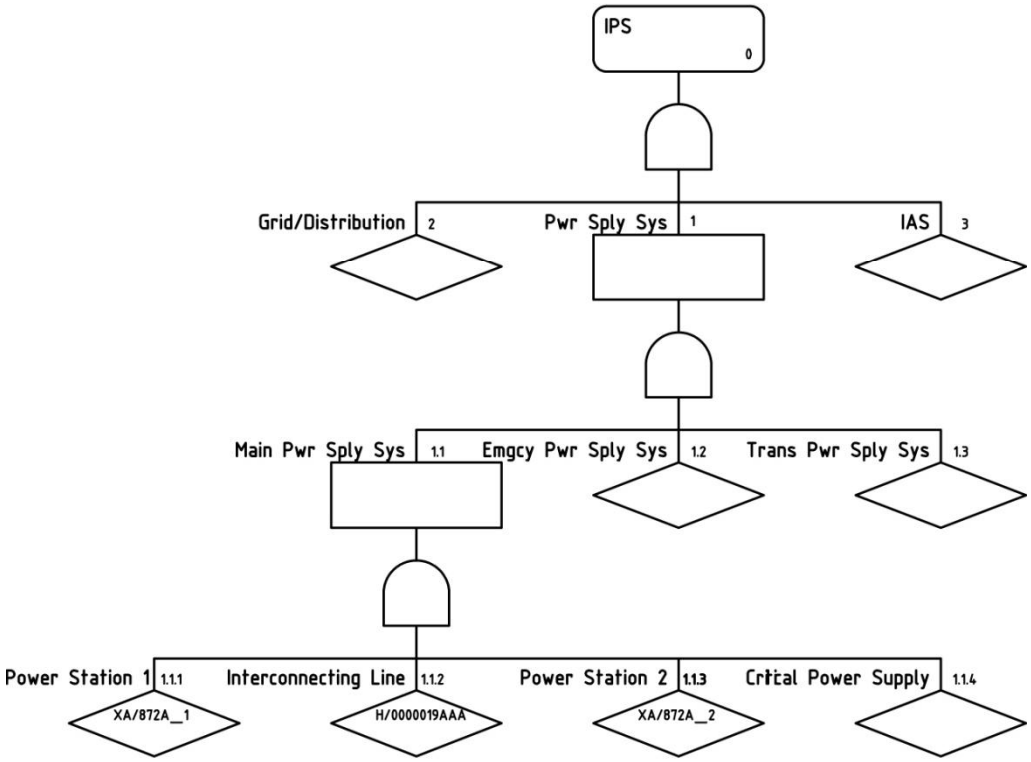

Fig. 34: *IPS*, Decomposition Level 2, Main Power Supply System, *FTA*

- *SCADA* power supply sub-system (Block 3.4) provides power for all components. It is indeed an independent power supply sub-system, with its sources of power and its distribution network, as commented below.
- A Power Supply and Grid/Distribution block could have been imagined to synthesise *IAS* power dispatching service, similarly to what done for remaining systems. This could have led to a further level of expansion[75], but, in the end, components would have been same.
- Supply breaker and cable for *IAS UPS*1 and 2 are thought to be included in relevant power distribution systems, as per conventions laid down in *3.1*.

[75] Block 3.4 would have been split into two blocks connected in series, say *IAS* power supply (3.4.1) and *IAS* power distribution (3.4.2). Block 3.4.1 would have coincided basically with *IAS UPS*1 and *IAS UPS*2 in parallel, and so on. Modularisation would have been preserved, together with a consistent decomposition, with an appreciable value; document conciseness would have suffered.

- "Path N" blocks represent path a piece of information is to travel, through a ring network, to reach its final destination, or the operator stations (at least one of them). Model shows operator stations are only "one switch away" from process computer in both directions, which is an oversimplified case. Actual complexity may be rendered adding in series as many network hops (network cable and network switch) as required for the physical implementation (which details are not entirely disclosed) to reach final destination following the two possible paths. As a matter of fact, adding identical blocks in series makes model improving in terms of fault combination, but does not introduce new failure modes; this supports the simplification made here.
- Ring network, relevant pieces of hardware and operator stations are not essential to system functioning, but they are to allow interaction with user and, above all, system performance monitoring, as requested by rules. Operator, ultimately, is called to judge upon *IAS* dependability.

3.4.4 *IPS*, Level Three.

A further iteration executed on blocks shown in Fig. 33 leads to the diagram in Fig. 37.Some explanatory considerations are of order:

- Power station counting stand by generator needs re-configuring, in case an active generator fails. Upon fault nature, generator may be kept on line until standby is not loaded or it may be immediately shut down. It is then logical saying that *Main Electrical Power Supply System* does not deliver its intended service as long as power limitation is active, and if *SCADA* and *Generator Connection Control* are not delivering their expected service. Furthermore, *Main Electrical Power Supply System* **temporarily** fails delivering its expected service if a generator failure materialises
- Critical power supply. This system serves equally *Generator Connection Control*, *Generator Protection*, *Interconnecting Line Protection*, *Grid/Distribution Protection* and *Grid/Distribution Control*; it is then natural considering it an individual entity, not part of any previously listed sub-system[76]. Without it no breaker control would be possible (*Generator Connection Control* takes power from generators or power station), as well as protection. This sub-system can be decomposed further later on, using the well explained procedure adopted so far, if needed.
- *FTA* model will not be elaborated for this structure, as the equivalence between those two representations has been proven exhaustively.
- *SCADA* is fully decomposed at level 2, so no further decomposition is considered necessary. Control code structure is analysed further in *3.4.6* and *3.4.7*.

[76] Some further explanations are of essence in supporting this assumption. Hardware (battery chargers, battery banks and distribution panels) is indeed co-located with power stations, and this would eventually support a different approach (considering two halves, belonging each one to a power station); functioning, as opposed, is such that (both power supplies kept in hot standby on a made common bus bars, as the interconnecting line is kept always closed) is impossible perceiving separation, unless a fault causes common bus bar to split. Still, in that condition, users are common. User point of view has here prevailed, and critical power supply has been considered as a standalone sub-system.

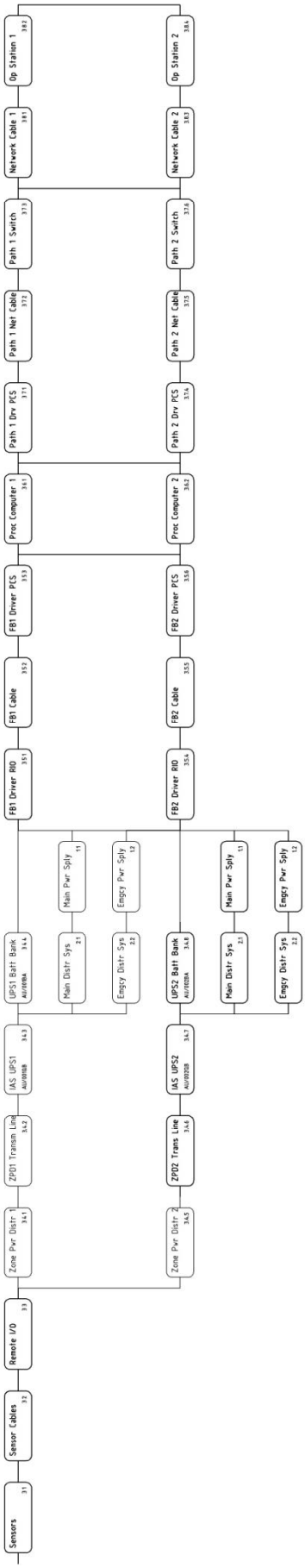

Fig. 35: ***IPS***, Decomposition Level 2, ***SCADA***, ***RBD***

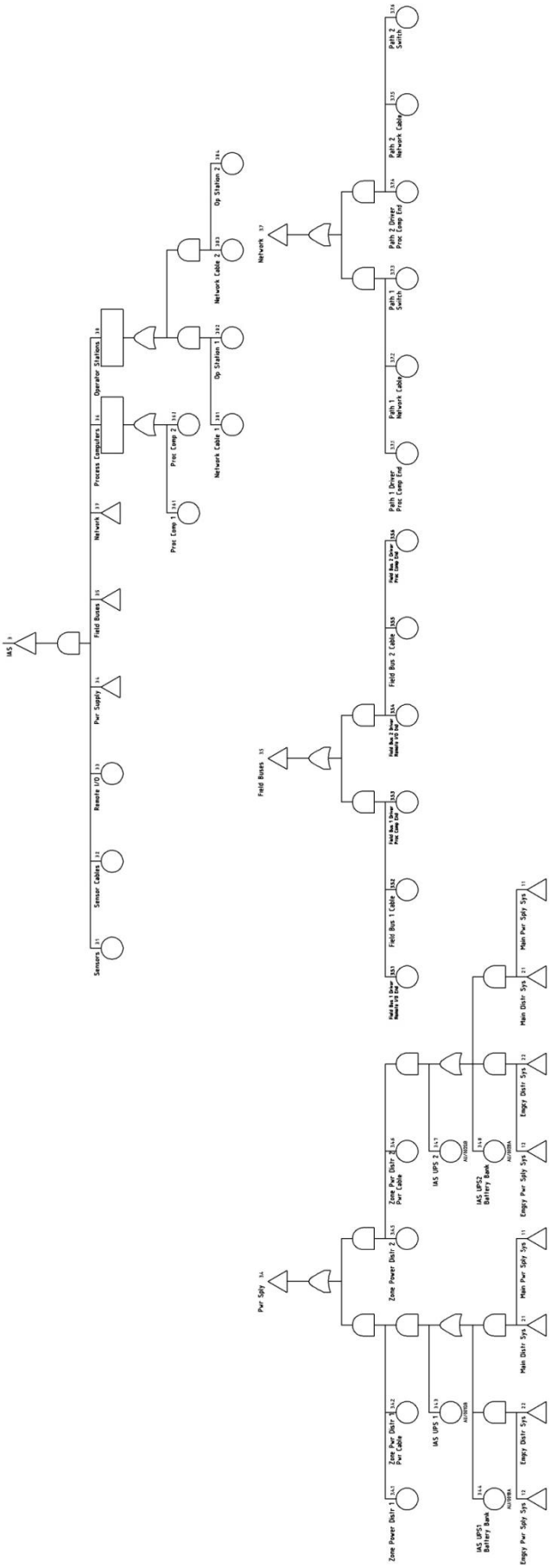

Fig. 36: ***IPS***, Decomposition Level 2, ***SCADA***, ***FTA***

- **Common Resistor** blocks. They are two different blocks, belonging to different power stations. An explanation may be found in Fig. 22: earthing resistor cabinet consists of three resistors, connected to their respective generators (and thus functionally belonging to them), and a group resistor (functionally belonging to power station, in the very same fashion branch resistor are functional to their respective generators). This subdivision in subjective, but finds grounds in the way devices are operated: generator resistors are used when their respective generators become active, whereas group resistor is active whenever a generator is active

3.4.5 *IPS*, Level Four.

This further decomposition involves generators only. Result is illustrated in Fig. 38. Direct controls (voltage and frequency controls) have been further expanded in the same picture. Comments are of order:

- High Voltage Switchboard Cubicle. As discussed in *3.1* this piece of equipment is partitioned in functional areas: cable and circuit breaker compartment belongs to *Main Electrical Power Supply System*, bus bar compartment belongs to *Main Distribution System* and auxiliary compartment belongs to *Integrated Automation System* (subdivided between direct controls, such as protection relay, and *SCADA*, with its sensor terminations). In this section, high voltage switchboard refers to cable and circuit breaker compartment.
- Sensor function and position is detailed in *3.1.1* and *3.1.3*, inasmuch sub-systems of interest are concerned.
- Prime mover safety system is supplied from the same source of frequency control; for this reason blocks have not been repeated.
- Cable connecting alternator neutral point to its resistor has been omitted for readability reasons. Being its block in series with the resistor itself, it may be thought as lumped together with it, without loss of generality.
- *IAS* battery charger (block 1.1.1.6, piece nr AU/002BA) is equipped with its own battery bank, independent from FZ/UB5QB.
- Prime mover instrumentation and safety system do not form part of this work; they are mentioned because *IAS* reads their status to determine prime mover readiness to start.
- Arc detection system, detects arc developing by monitoring light emission (photo-detection). There is a different implementation, based upon shockwave detection (pressure detection). Both implementations have same component list, albeit different components (pressure detectors as opposed to light detectors); clearly diagram does not change. Detectors are usually placed within cable compartment (so becoming part of main power supply system direct controls), circuit breaker compartment lower connections (so becoming part of main supply system direct controls), circuit breaker higher connections (so becoming part of main power distribution direct controls) and, finally, within bus bar compartment (so becoming part of main power distribution direct controls). Different sensor activation causes different tripping action, according to protected zone.
- Alternator block (piece nr XA/274A) could be further decomposed, in the same manned shown in [**12**].

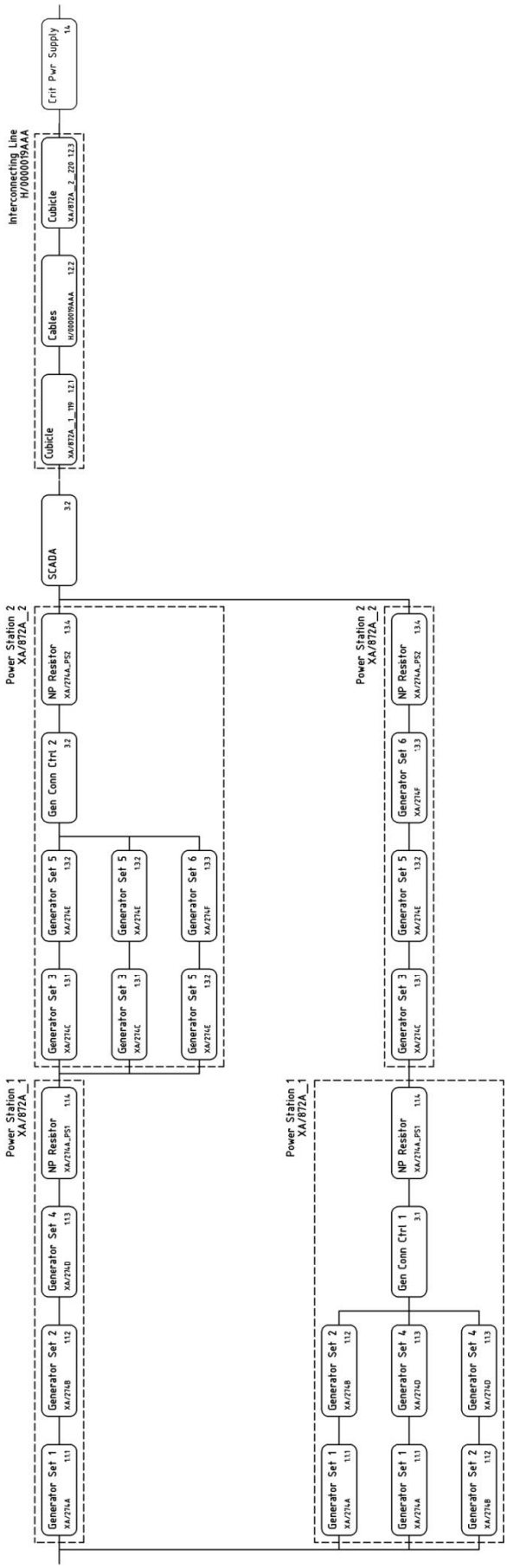

Fig. 37: ***IPS*, Level 3 Decomposition, Main Electrical Power Supply System**

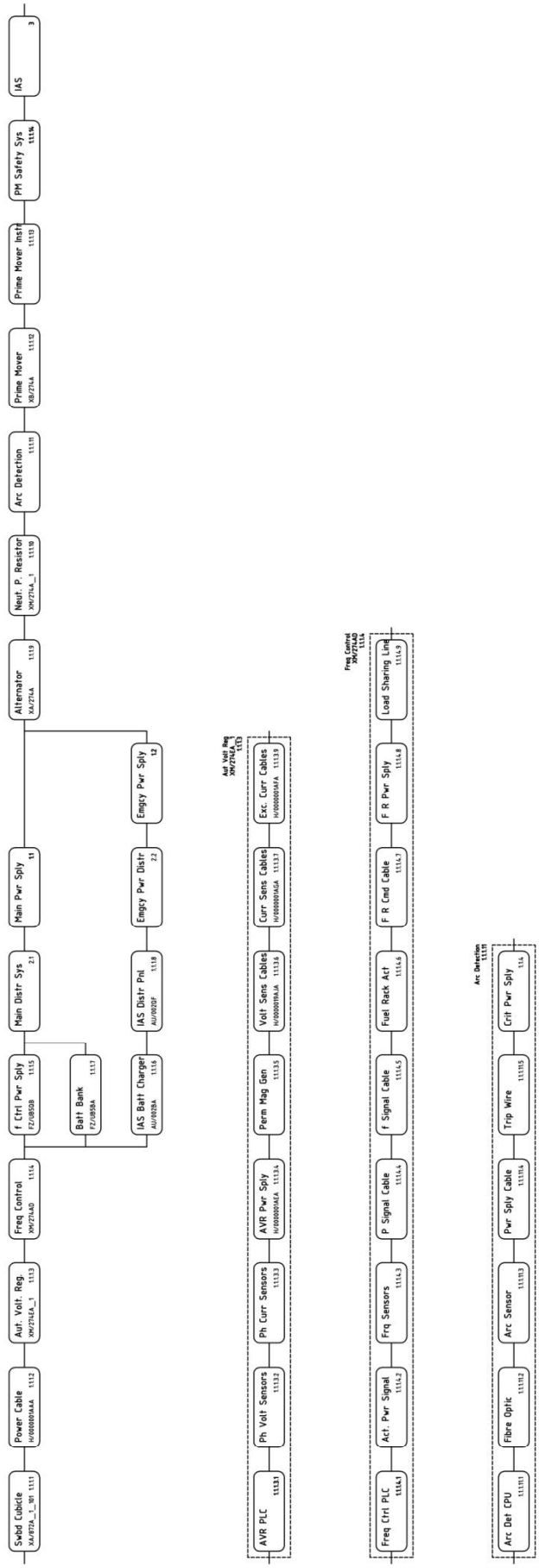

Fig. 38: ***IPS*, Decomposition Level 4, Generators, RDB**

3.4.6 Control Code, Level Zero.

Aim of this section is providing insight on application control code to enable assessing importance of pieces of information to the performing of intended function. This insight is not meant to provide an analysis on the code itself, rather than providing an analysis of interactions code causes. These interactions are conditioned by information, so information is sensible to the process. Process structure may in turn affect information dependability requirements, and this is pertinent to the scope of this work.

IPS control code, as described in *3.1.3.8*, may be conveniently illustrated and decomposed following procedure already adopted in previous sections. Resulting diagram is shown in Fig. 39

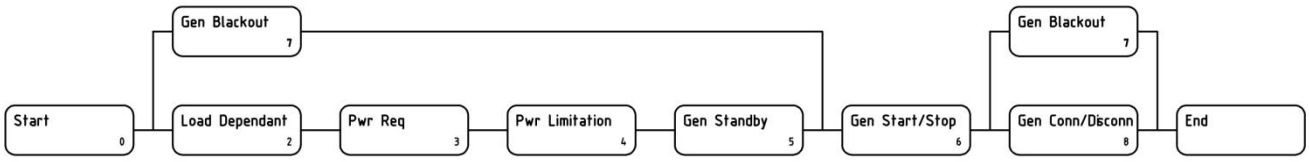

Fig. 39: Control Code, Level Zero Decomposition, *RBD*

A start/stop action is initiated by the four blocks (1[77], 2, 3 and 7[78]); *IPS* power consumption is controlled (block 4) until action is completed (End), which happens if there is a standby generator set (block 5). In case of a blackout, all available generators are started and the first reaching rated speed is connected to dead bus. Generator Connection/Disconnection sub-routine is deactivated by black out routine to this extent; paralleling is not possible as one source would be missing in a black out situation.

Both power stations are managed according to this same routine.

There is an intentional coincidence in names among direct control and control code routines; in most case control code activates direct controls, if they are available, and waits for a successful conclusion signal, before deactivating them.

3.4.7 Control Code, Level One.

Level 1 decomposition is still quite general. Resulting diagram is illustrated in Fig. 40.

[77] Block 1, generator replacement, as described in 3.1.3.8, is not included in the diagram, even though it is a power management function. Its function is entirely backed up by other blocks, albeit with possible longer power limitation timeframes. On the other hand, generator replacement sub-routine does not back up any other block. Generator shutdown caused by a minor alarm become critical, a typical occurrence that happens if generator replacement sub-routine fails, causes a load increase in remaining generators, thus activating load dependant and power limiting sub-routine; in this regard generator replacement routine failure does not affect power management. As opposed, if load dependant sub-routine fails, active generators are kept running within their design limits by power limitation routine, causing no change over alarm; generator replacement routine would not react bringing back *IPS* to its correct service.

[78] In fact, this block initiates a start action only.

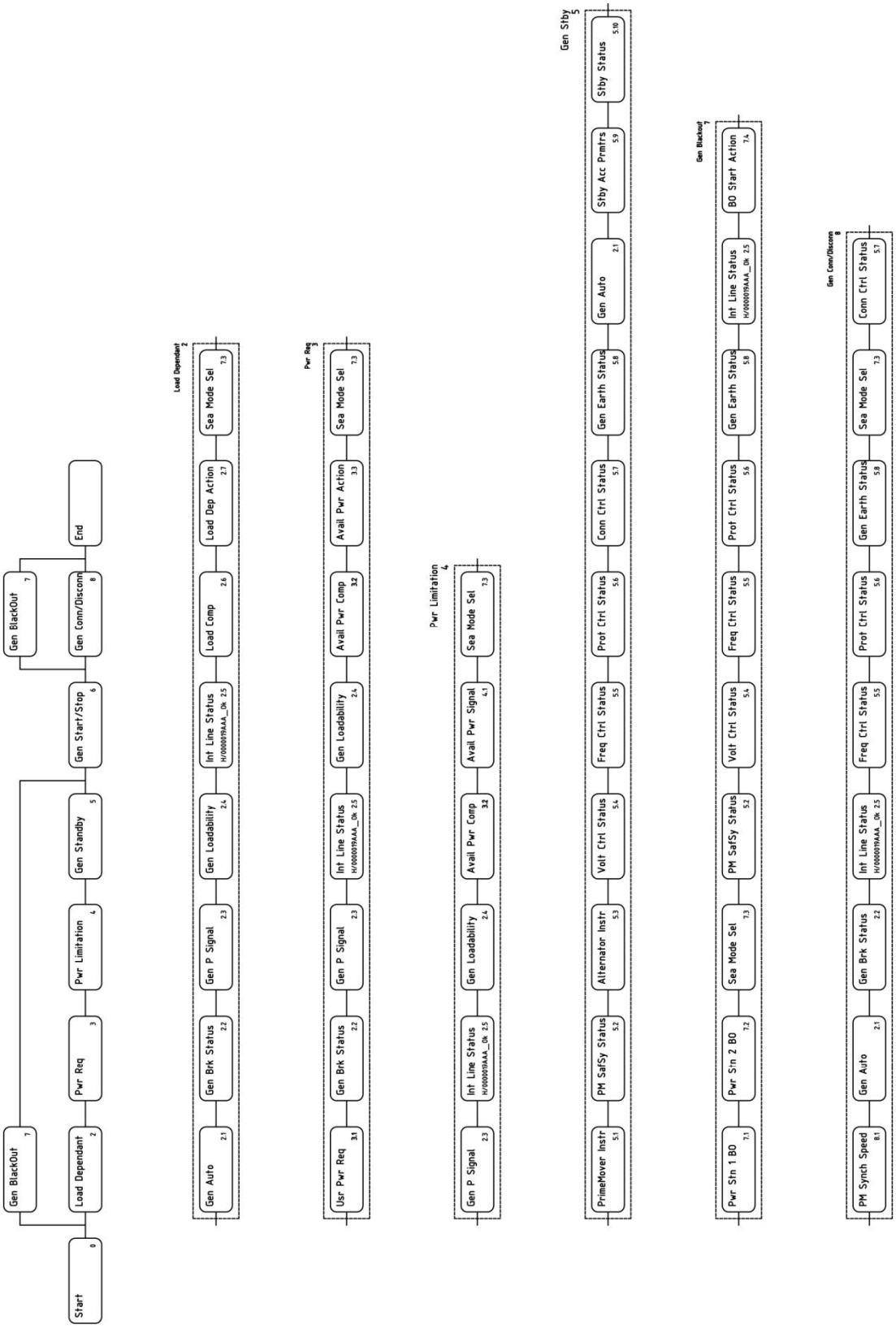

Fig. 40: Control Code, Decomposition Level 1, ***RBD***

Level zero is repeated on top, followed by block expansions. Some comments are of order:

- Automatic control condition has been made explicit. Albeit often overlooked because listed in the hypotheses, this signal is quintessential to *IAS* to discriminate whether to act or not. This signal is a

basic rule requirement in order to decide unambiguously who is in command of a certain system in a certain moment in time; should this signal fail, there could be no automatic action or an unexpected automatic action. In any case, system fails delivering it expected service. At this decomposition level, where concepts are of essence, this block represents a generic generator; should a deeper detail be required, then this block is to be replaced with parallel connection of same signals (GenAuto) pertinent to all standby generators. In the case under investigation, only one generator is assumed to standby, therefore one single block suffices.

- Generator Breaker Status (block 2.2). This signal indicates which generator is active and which is standing by. Power signal alone does not serve this purpose. Power signal different from zero could have been used to the same extent, but with remarkable loss in precision. On the other hand, being power signal a 4-20mA, it could be monitored for physical damages, as opposed to a status contact. In fact, this signal is quintessential to power management routine. Needles to say, this signal serves the purpose of engaging *Generator Frequency Control* and its relevant load sharing lines, and *Generator Voltage Control*. It is irrelevant to *Generator Protection*, as it reads electrical values only.
- Generator Active Power signal (block 2.3). This information gives generator actual load. At this level of decomposition suffice to highlight its importance, quite obvious indeed, in calculating generator loading point; should a more accurate model be needed, then this block should be replaced with a parallel of same blocks, relevant to active generators. Being correct and accurate loading calculation paramount for the function, which description can be found in *3.1.3.8*, failure in retrieving and/or processing it causes system failure.
- Generator Loadability value (block 2.4). This information is provided by operators, and differs from a hardcoded value, generally the rated value, in case of any maintenance operation or anomalies in auxiliary systems. As already explained in previous point, this value concurs in defining actual loading index, defined as:

$$\text{Actual Loading Index } [\%] = \frac{\text{P (block 2.3)}}{\text{Loadability (block 2.4)}}$$

- Interconnecting Line Status (block 2.5). This information instructs system on which action undertaking in case of a load dependant occurrence. Load may in fact be different on generators belonging to non-interconnected power stations, therefore actions shall adapt to configuration. At this decomposition level a common signal represents the overall status of this equipment; should a more detailed view be needed, then it is easy observing that interconnecting line status is the series of its components statuses[79].
- Load Computations (block 2.6). This block includes calculations and time delays relevant to power management. Basic calculation happens comparing actual load index with a preset value; if index exceeds preset (load dependant start threshold) for a predetermined amount of time, then a new generator is started; if, as opposed, index falls below a different preset (load dependant stop threshold) for a predetermined amount of time, a generator is stopped. Calculation accounts for the *IPS* status, split or joined, in order to decide on which power station initiating actions. Thresholds are evaluated for consistency, especially load dependant stop. Further calculations are run to determine whether new configuration, after load dependant stop action, would require a

[79] Cable status can only be ascertained when it is energised, in this project. This fact is quite important because no information on system readiness is available before its use.

load dependant start or not. This further verification is necessary to avoid unnecessary start/stop actions due to an inaccurate preset choice. To the extent of this section, suffices considering one load dependant routine only, should a more in depth analysis be required, then routine should be duplicated to account for the presence of two power stations.

- Load Dependant Action (block 2.7). Once correct load dependant action is elaborated, appropriate signals are transmitted to standby or active generators, and relevant sub-systems. Once again, to the extent of this section, suffices considering one load dependant routine only, should a more in depth analysis be required, then routine should be duplicated to account for the presence of two power stations.
- Sea Mode Selected (block 7.3). This block receives input from operators that vessel is not supplied from its *External Power Supply System*. This block/signal has a central importance in the routine, as it acts on interlocks and *IPS* configuration; should this condition be incorrectly detected, there would be no power management action, as stated in *3.2.1*. This signal is unique, and therefore affects *IPS* in its entirety. Control code, at least in this project, is not sophisticated enough to manage one power station as main power supply source and the other being connected to external power supply.
- User Power Request (block 3.1). This block/signal indicates a power request, or the intention to start a heavy user. According to user being started, actions are different: generator load index is computer adding a predetermined power reserve and compared against thresholds. If index exceeds threshold, then a further standby generator is added and start signal is transferred to requesting user when index achieves appropriate values (i.e. when additional generator has completed starting sequence, and *IAS* has received breaker closed signal), otherwise start signal is directly transferred. Once again, failing in detecting power request or in connecting power request with right requesting signal implies wrong action, with possible service disruption. More detailed analysis would imply listing of so called “heavy users”, together with the power station to which they are connected to; those inputs should be lead in parallel to a block symbolising the routine associated with its power station (as one power request failure does not imply all other power requests failing, if failure is associated to physical causes)[80].
- Available Power Computations (block 3.2) and Available Power Actions (block 3.3). Those blocks are quite similar to block 2.6 and 2.7; block 3.2 acts slightly differently from block 2.6 performing a “power forecast”, i.e. computing expected load index after request has been satisfied. To that extent it is common assuming that “reserved power” coincides with “rated user power”, leaving the burden of managing the resulting condition to block 2.6, after the request has been satisfied. In essence, power request routine overrides load dependant only during starting of heavy users.
- Generator Start/Stop (block 4). Those blocks/signals enclose all tasks relevant to starting and stopping a prime mover. They can be exemplified with this brief list, valid for a diesel generator:
    - Open starting air inlet (by means of prime mover control system),
    - Position fuel rack (by means of *Generator Frequency Control*) to starting fuel supply (slightly higher than idling fuel supply),

[80] This assumption needs be confirmed by appropriate testing, as error may be located in the code. Wrong programming may connect wrong user data with a certain request, causing system to fail.

  - Detect self sustaining speed (by means of prime mover control system) and consequently interrupt starting air supply and ramp up to synchronous speed (*Generator Frequency Control*)
  - Detect synchronous speed condition (*Generator Frequency Control*) and consequently start excitation (*Generator Voltage Control*)
- Prime Mover Instrumentation (block 5.1). Prime mover instrumentation is required to detect readiness condition (for normal or emergency start). These two conditions are different in terms of requirements, being less stringent for emergency start, as expected. Readiness condition needs be maintained executing actions on auxiliary. Should a more in depth analysis be required, then this block should be replaced with parallel connection of same blocks relevant to standby prime mover in the configuration being considered, in the hypothesis of auxiliary laid out so that services to different prime movers are independent.[81] Needles to say, failing in detecting stand by condition affects automatic operation (no generators available for starting on load conditions or generators failing to start due to their failure conditions) and may lead to service disruption.
- Prime Mover Safety System Status (block 5.2). This signal/block indicates there is no shut down active, or the prime mover stopped in its normal way, following commands received by *IAS*. More in depth analysis would require considering that stand by status belongs to generators, therefore stand by pool is to consist of parallel connection of as many sequence as the one depicted as many stand by generators in the configuration. This consideration applies, in fact, to all 5.X blocks hereunder.
- Alternator Instrumentation (block 5.3). Similarly to what discussed for prime mover, same considerations apply to generators. In this very same fashion alternator safety system, or block 5.6, may be mentioned here.
- Auxiliary Systems Status (block 5.4, 5.5, 5.7 and 5.8). Their capability to deliver expected service is needed to infer generator capability to deliver its expected service; therefore their readiness status is a pre-condition to confirm generator readiness status.
- Standby Acceptable Parameter Values (block 5.9). Those parameters are commonly hard coded, and define stand by condition in terms of thermodynamic performances. As already discussed, generator is expected to start and take load without further delays; if to this result there are conditions that need be maintained, then this is a task falling within *IAS*. Failing to detect or maintain stand by condition leads to failing to execute power management actions.
- Stand by Status (block 5.10). This information shall activate and control all sub-systems relevant to maintaining stand by acceptable parameters values, mentioned earlier. An erroneous generation of stand by status can compromise power management service.
- Power Station 1 Black Out (block 7.1) and Power Station 2 Black Out (block 7.2). Both those two signals are necessary to detect a black out (service failure) situation to *IAS*. Black out information has the sole purpose of activating restarting sequence. Black out information affects the entire *IPS*, therefore there is no multiplication following power station number. Black out actions (block 7.4) may indeed be different according to interconnecting line status: if interconnecting line is closed then the first generator coming online is to connect directly without synching, as opposed to all that follow; differently, if interconnecting line is open, the first generator connecting to a power

[81] For this project, this is not the case. Engine starting air sub-system is in fact common to power station, so common to three generators.

station interlocks for synching all the following on the same power station. Again, failing in detecting this situation may cause undesired starts and/or connections.

3.5 Analysis of the Model.

Models elaborated in *3.4* will be analysed making use of techniques described in *2.4*. Beyond a certain decomposition level, comprehensive analysis cannot be done without computer application support, given the high number of items to handle; here it will be shown that some interesting results can be achieved even without IT resources, proving the effectiveness of methods.

Scope of analysis is anyway is system architecture, rather than components; in the case under analysis system level identifies with piece marks. System integration stops at component level; any further analysis is demanded to sub-contractor. Still this delimitation brings is a noticeable quantity of object, and still numeric elaboration support will be required, even though to a lesser extent.

3.5.1 *IPS* Level Zero, Direct Inspection.

At this level the process of generating, distributing and controlling electrical power supply is described. The information provided is that *IPS* is dependable if *Electrical Power Supply System*, *Grid/Distribution* and *Integrated Automation System* are dependable. Necessity of Integrated Automation System to *IPS* service is highly debated, and in general not reflected in classification rules. Classification rules tend to identify *IAS* with remote automatic control, as defined in *1.3.4*. Remote automatic control is intended as a set of means enabling operators to perform same actions they would as if they were on local control post, but remotely. In fact reality is indeed more complicated: there is no memory of operators balancing load among generators manually in recent years; this task has always left to either direct controls or *IAS*. Rules in fact request a manual backup, or way of keeping *IPS* delivering its service, even though assisted by operators, is present, without assessing its real effectiveness and without considering the real level of embedding of "automation" in systems. Perhaps a definition of automation nearer to class rules is that automation is the system in charge of generating set points to controlled sub-systems; still this definition lacks consistency when applied to propulsion: automation "modifies" temporary reference to overcome anomalies, but it does not generate a reference, being this generated by operators.

In the same rules there are no requirement concerning direct control layout in relation to their "automation" function: *Generator Frequency Control* for instance, is required to have R0 power supply redundancy, but nothing is said about any different possible causes of failure, and the expected behaviour. No redundancy requirements are drawn, as opposed to *IAS*, having a long series of built in redundancies or fault managing features. In this respect rules accept redundancy in having multiple generators, but it does not require redundancy in controlling a multiple generator system; not to mention the fact that a single generator is very seldom sufficient to sustain all main functions. This fuels the confusion inherent in the rules as regards to the definition of an appropriate backup/redundancy level. This question is not trivial and has a definite impact

on safety. At present, ship manning is designed upon automation level, the highest the level, the lower the manning. Should automation fail; chance that manning cannot effectively assist sub-systems is present.

This simple analysis has shown that terms are, at present, at least lacking a stringent definition, and that failures need be better specified to be in condition of formulating manning requirements coherent with situations that are considered as likely to happen.

3.5.2 *IPS* Level Zero, Dependability Indexes.

Index/Reference	Calculations	Notes
Qos/*2.4.4.1*	$MTTF_{IPS} = \frac{1}{\lambda_{Power\ Supply} + \lambda_{Grid/Distribution} + \lambda_{IAS}}$ $R_{Power\ Supply}(t) = e^{-\lambda_{Power\ Supply} * t}$ $R_{GridDistribution}(t) = e^{-\lambda_{GridDistribution} * t}$ $R_{IAS}(t) = e^{-\lambda_{IAS}(t)}$ $\frac{1}{\lambda_i} = \int_0^{\infty} R_i(t)dt$	As specified in *2.4.4.1 QoS* can be calculated as an *MTBF*, considering disruptions producing an appreciable deterioration in service, as perceived by users. Considering, as a safe measure, most sensitive users, such as IT equipment, can take no longer than 1s power quality lower than specified, then 1s is the threshold for sensitive disruptions.
Operability/*2.4.4.2*	$O_{Service\ Speed,IPS}(t) = \begin{cases} 0 \\ 1 \end{cases}$ $\overline{O_{Service\ Speed,IPS}} = \int_0^{t_0} O_{Service\ Speed,IPS}(t)\,dt$	The three systems in consideration, electrical power supply, grid/distribution and *IAS*, are all commanded to be on at any given time and for any specified time frame in the given configuration. This makes so that operability can take two values only. Average value may be calculated over a certain time frame [0, t_0], to obtain average operability. A convenient value for t_0 may be chosen as 14 days, a typical cruise trip.

Index/Reference	Calculations	Notes
Vectorised Dependability Metric/*2.4.4.3*	$\vec{v} = (14, p_{SL0}, p_{FSL}, MTTF_{IPS})$	Figures have following meaning: 14 = number of days system stays in state zero, or fully operational. 14 days is the usual duration of a cruise, but this number can be chosen according to different principles. p_{SL0} = System in consideration has 2 possible states, full service and failed. This number accounts for probability system has to remain in state 0. p_{FSL} = probability of system being in FSL states $MTTF_{IPS}$ = *IPS* mean time to failure, defined above

Table 17: ***IPS*, Decomposition Level Zero, Indexes.**

3.5.3 *IPS* Level Zero, *FMEA*.

This section has the sole scope of maintaining approach consistency, as there is no point in elaborating a *FMEA* table for system at this level of decomposition. Every failure has fatal consequences, and its causes and mechanisms cannot be explored in a sensible way. *FMEA* anyway is a bottom up approach, as stated in *2.4.3.3*, and it finds its most natural application when decomposition level is high (ideally, *FMEA* should be done when decomposition is concluded, and only atomic components are present populating blocks).

3.5.4 *IPS* Level One, Direct Inspection.

This decomposition level provides more refined pieces of information as regards to the configuration under inspection, but does not allow drawing any additional consideration concerning dependability. In reality, some other considerations of statutory nature should be accounted for:

- *Emergency Electrical Power Supply System*. A vessel is not authorised to leave port if this sub-system is not ready for service. Albeit this power source condition does not affect configuration under investigation, its failure reduces the time duration it may be considered dependable. Assuming emergency power supply system fails at sea, open sea trading speed mode can be kept to the next port of call, but no longer. Fault must be repaired by that time, otherwise ship must discontinue its trading, so failing in delivering its expected service, and it is safe stating reason for ship service failure is located with *IPS*, and coincides with the hypothesized failure.

- *Transitional Electrical Power Supply System*. Same considerations stated for *Emergency Electrical Power Supply System* apply to this sub-system.

Statutory considerations hereabove reported go beyond the scope of this work, as they specify testing and maintenance requirements, typical of the use phase. Still, method brought to attention facts that are intrinsic in systems, and must be catered for. In this respect, scope of present work is fulfilled, in the sense of demonstrating the effectiveness of proposed method on all aspects of product life. In this instance the careful analysis of class requirements this method requires has brought to light aspects that are more connected to ship management, but affect design deeply, as an efficient management generates revenues.

Model as elaborated in Fig. 26 and Fig. 27 is consistent with the hypotesis of a trading ship during its voyage, between two ports of call, but it would not if the hypotesis “at sea, between two ports of call”, was removed.

Direct inspection of model does not provide further information in addition to a list of sub-systems in which *IAS* can be decomposed. In that specific instance hypotesis relevant to ship state of being engaged in a voyage may be discontinued, as it is inessential for the system in consideration. Overall effect is anyway negligible, being this sub-system in series with other sub-systems for which the hypotesis is standing as necessary.

Generally speaking, this decomposition step provides clarifications upon the necessity of certain hypoteses, and their effect on dependability of systems.

3.5.5 *IPS* Level One, Dependability Indexes.

Dependability indexes do change due to a different component count, offering a lesser level of approximation. Table 18 can be compiled.

Index/Reference	Calculations	Notes
Qos/*2.4.4.1*	$MTTF_{IPS} = \frac{1}{\lambda_{MPS} + \lambda_{MDS} + \lambda_{IAS} + \lambda_{EDS} + \lambda_{TDS}}$ $R_{Main\ Power\ Supply}(t) = e^{-\lambda_{MPS} * t}$ $R_{Main\ Distribution\ System}(t) = e^{-\lambda_{MDS} * t}$ $R_{IAS}(t) = e^{-\lambda_{IAS}(t)}$ $R_{Emergency\ Distribution\ System}(t) = e^{-\lambda_{EDS}(t)}$ $R_{Transitional\ Distribution\ System}(t) = e^{-\lambda_{TDS}(t)}$ $\frac{1}{\lambda_i} = \int_0^{\infty} R_i(t)dt$ $R_{IAS} = \prod_{i=1}^{8} R_{3.i}$ $MTTF_{IAS} = \frac{1}{\sum_{i=1}^{8} \lambda_{3.i}}$	As specified in *2.4.4.1 QoS* can be calculated as an *MTBF*, considering disruptions producing an appreciable deterioration in service, as perceived by users. Considering, as a safe measure, most sensitive users, such as IT equipment, can take no longer than 1s power quality lower than specified, then 1s is the threshold for sensitive disruptions. Inasmuch as *IAS* is concerned, reliability functions have the form of an exponential, as already done for *IPS*; consequently system reliability function and *MTTF* is calculated as shown.
Operability/*2.4.4.2*	$O_{Service\ Speed,IPS}(t) = \begin{cases} 0 \\ 1 \end{cases}$ $\overline{O_{Service\ Speed,IPS}} = \int_0^{t_0} O_{Service\ Speed,IPS}(t)dt$	Systems in consideration are now five, but final result does not change as all five are required for operability. Decomposition level under study does not allow degradation. Average operability can be calculated, as already shown
Vectorised Dependability Metric/*2.4.4.3*	$\vec{v} = (2, p_{SL0}, p_{FSL}, MTTF_{IPS})$ $\overrightarrow{v_{IAS}} = (350, p_{SL0}, p_{FSL}, MTTF_{IAS})$	Following on discussion in *3.5.4* minimum requested duration has modified to two days, a typical distance between two ports of call in case of Caribbean or Mediterranean cruises, but number can be chosen according to different considerations. Important noting vector length has considerably reduced (keeping remaining parameter values unchanged). Inasmuch as *IAS* is concerned, an expected duration of 1 year is decided, being this requirement common for computer applications running under Windows environment.

Table 18: *IPS*, Decomposition Level One, Indexes.

3.5.6 *IPS* Level One, *FMEA*.

This section has the sole scope of maintaining approach consistency, as there is no point in elaborating a *FMEA* table for system at this level of decomposition. Every failure has fatal consequences, and its causes and mechanism cannot be explored in a sensible way. *FMEA* anyway is a bottom up approach, as stated in *2.4.3.3*, and it finds its most natural application when decomposition level is high (ideally, *FMEA* should be done when decomposition is concluded, and only atomic components are present populating blocks).

3.5.7 *IPS* Level Two, Direct Inspection.

This decomposition level includes *Main Electrical Power Supply System* and *Integrated Automation System*, the part of which relevant to Main Electrical Power Supply System, is often called Power Management System, as shown in Fig. 33 and Fig. 35. Direct inspection here indicates a possible dependability hazard in the block called **Interconnecting Line** (block 1.1.2). It must be remembered this block is not duplicated, as opposed to block **Critical Power** (block 1.1.4), as Fig. 23 illustrates. Necessity of **Interconnecting Line** is stated in *3.3.1*, therefore any failure in it would imply failure in delivering expected service. Same can be said of power stations, but it is shown there is a higher duplication level in *Main Electrical Power Supply System* (one stand by generator) than in interconnecting line.

As far as Integrated Automation System is concerned, Fig. 35 and Fig. 36 show all components are duplicated, exception made for sensors and their cables, and *RIO*s. This consideration leads to the fact that sensor role must be carefully evaluated, in terms of impact to dependability. The most appropriate part of process for this evaluation appears the control code.

3.5.8 *IPS* Level Two, Dependability Indexes.

Index/Reference	Calculations	Notes
Qos/*2.4.4.1*	$$MTTF_{MPS} = \frac{1}{\lambda_{PS1} + \lambda_{IL} + \lambda_{PS2} + \lambda_{CPS}}$$ $$R_{Power\ Station\ 1}(t) = e^{-\lambda_{PS1} * t}$$ $$R_{Interconnecting\ Line}(t) = e^{-\lambda_{IL} * t}$$ $$R_{Power\ Station\ 2}(t) = e^{-\lambda_{PS2}(t)}$$ $$R_{Critical\ Power\ Supply}(t) = e^{-\lambda_{CPS}(t)}$$ $$\frac{1}{\lambda_i} = \int_0^\infty R_i(t)dt$$ $$R_{IAS\ PS1} = 1 - (1 - R_{2.1} * R_{2.2}) * (1 - R_{1.1} * R_{1.2}) * (1 - R_{3.4.4})$$ $$R_{IAS\ PS2} = 1 - (1 - R_{2.1} * R_{2.2}) * (1 - R_{1.1} * R_{1.2}) * (1 - R_{3.4.8})$$ $$R_{IAS\ ZPD1} = R_{3.4.1} * R_{3.4.2} * R_{3.4.3} * R_{IAS\ PS1}$$ $$R_{IAS\ ZPD1} = R_{3.4.5} * R_{3.4.6} * R_{3.4.7} * R_{IAS\ PS2}$$ $$R_{IAS\ ZPD} = 1 - (1 - R_{IAS\ ZPD1}) * (1 - R_{IAS\ ZPD2})$$ $$R_{FB1} = R_{3.5.1} * R_{3.5.2} * R_{3.5.3}$$ $$R_{FB2} = R_{3.5.4} * R_{3.5.5} * R_{3.5.6}$$ $$R_{FB} = 1 - (1 - R_{FB1}) * (1 - R_{FB2})$$ $$R_{PC} = 1 - (1 - R_{3.6.1}) * (1 - R_{3.6.2})$$ $$R_{PCS1} = R_{3.7.1} * R_{3.7.2} * R_{3.7.3}$$ $$R_{PCS2} = R_{3.7.4} * R_{3.7.5} * R_{3.7.6}$$ $$R_{PCS} = 1 - (1 - R_{PCS1}) * (1 - R_{PCS2})$$ $$R_{NC} = 1 - (1 - R_{3.8.1} * R_{3.8.2}) * (1 - R_{3.8.3} * R_{3.8.4})$$ $$R_{IAS} = R_{3.1} * R_{3.2} * R_{3.3} * R_{IAS\ ZPD} * R_{FB} * R_{PC} * R_{PCS} * R_{NC}$$	As specified in *2.4.4.1 QoS* can be calculated as an *MTBF*, considering disruptions producing an appreciable deterioration in service, as perceived by users. Considering, as a safe measure, most sensitive users, such as IT equipment, can take no longer than 1s power quality lower than specified, then 1s is the threshold for sensitive disruptions.
Operability/*2.4.4.2*	$$O_{Service\ Speed,IPS} = \begin{cases} 0 \\ 1 \end{cases}$$ $$O_{Service\ Speed,IAS} \begin{cases} 0, failure\ of\ non\ replicated\ component \\ 1, failure\ of\ replicated\ component \\ O(t), failure\ of\ interface\ level \end{cases}$$	*IAS* has a degraded mode, already mentioned, that consists in the complete loss of main ring, operator station or dedicated switches. This degraded mode causes operator interaction inhibition, but allows functioning with last parameter set, that has proven effective till the failure moment. This metric shows system can carry on delivering expected service even in presence of a fault that would be judged as fatal, under a strict interpretation of the diagrams.

Index/Reference	Calculations	Notes
Vectorised Dependability Metric/*2.4.4.3*	$\vec{v} = (2, p_{SL0}, p_{FSL}, MTTF_{MPS})$	This decomposition level does not change substantially the dependability value according to the metric. Inasmuch as *IAS* is concerned, some considerations are of order: • There are 37 components in the system. • There are at least 116 possible failed states, originated by two failures per group on a different line. Consequently, there are at least 116 elements populating failed service layer. Adding 3 single fatal failures elements would be 119 • There are at least 34 single failures not compromising system service, so 34 components in the service layer 0. Dependability vector would then have at least 156 elements.

Table 19: ***IPS*, Decomposition Level Two, Indexes.**

Table 19 shows indexes computation soon becomes too onerous. For this reason, many computer applications have become available. From now on, indexes will not be calculated any longer, unless in special cases, and for small sub-systems, trusting the procedure has been sufficiently exemplified.

3.5.9 *IPS* Level Two, *FMEA*.

A tentative *FMEA* can be done on *IAS*, being its decomposition completed, at least to the level defined in *2.4.2*. Still at this level chart contains pretty general statements, which are useful to set design guides and general rules. Result of this task is illustrated in Fig. 41 to Fig. 46.

Item list comes directly from *RBD*, and Mechanism of Failure is extracted from *2.3* (in facts 2.3 shall be used as fault check list, to make sure “no stone is left unturned”, or any possible fault scenario has been considered).

System: Design Verification Process
Subsystem: IAS
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date:

FMEA Number:
Prepared By:
FMEA Date:
Revision Date:
Page:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Analogue Sensor	Miscalibration	Untimely automatic action	7	Production Defects (thermal drift), Hardware Errata (inaccurate circuit, wrong range).	2	Environmental conditions Rating plus overspan Accuracy & Repeteability	5	**70**	Certified Calibration					
Analogue Sensor	Miscalibration Rise time too long	Untimely automatic action	3	Hardware Errata (wrong transducer chosen)	2	Acceptability of delay for protection purposes	5	**30**	System simulation in fault condition Sensor replacing					
Analogue Sensor	Open circuit	No feedback, no control action	7	Production Defects (circuitry failure)	2		1	**14**	Fault tolerance					
Analogue Sensor	Short circuit	Wrong feedback (out of range), no control action	7	Production Defect (circuitry failure)	2		1	**14**	Fault tolerance					
Digital Sensor	Miscalibration	Untimely automatic action	7	Production Defects (thermal drift), Hardware Errata (inaccurate circuit, wrong range).	2	Environmental conditions Rating plus overspan Accuracy & Repeteability	5	**70**	Certified Calibration					
Digital Sensor	Miscalibration Rise time too long	Untimely automatic action	3	Hardware Errata (wrong transducer chosen)	2	Acceptability of delay for protection purposes	5	**30**	System simulation in fault condition Sensor replacing					

Page 1 of 8

Fig. 41: *IAS*, Decomposition Level 2, *FMEA* Page 1

System: Design Verification Process
Subsystem: IAS
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date:

FMEA Number:
Prepared By:
FMEA Date:
Revision Date:
Page:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Digital Sensor	Open circuit	Wrong feedback, wrong control action	8	Production Defects (sezed contacts), Hardware Errata (insufficient current carrying capability)	3		10	**240**	Fault removal (change sensor to analogue) Fault tolerance.					
Digital Sensor	Short circuit	Wrong feedback, wrong control action	8	Production Defects (sezed contacts), Hardware Errata (insufficient current carrying capability)	3		10	**240**	Fault removal (change sensor to analogue) Fault tolerance.					
Sensor Cable Analogue Sensor	Open circuit	No feedback, no control action	7	Production Defects (circuitry failure)	2		1	**14**	Fault tolerance Fault Removal					
Sensor Cable Analogue Sensor	Short circuit	No feedback (out of range), no control action	7	Production Defect (circuitry failure)	2		1	**14**	Fault tolerance Fault Removal					
Sensor Cable Digital Sensor	Open circuit	Wrong feedback, wrong control action	8	Production Defects (sezed contacts), Hardware Errata (insufficient current carrying capability)	3		10	**240**	Fault removal (change sensor to analogue) Fault tolerance.					
Sensor Cable Digital Sensor	Short circuit	Wrong feedback, wrong control action	8	Production Defects (sezed contacts), Hardware Errata (insufficient current carrying capability)	3		10	**240**	Fault removal (change sensor to analogue) Fault tolerance.					
Zone Power Distribution Cabinet	Short Circuit	Loss of 1 power source to RIOs	2	Physical damage (water ingress, fire) Natural Fault (loss of insulation)	1	Creepage Distances IP grading Insulation Test Material Certification	1	**2**						

Page 2 of 8

Fig. 42: *IAS*, Decomposition Level 2, *FMEA* Page 2

System: Design Verification Process
Subsystem: IAS
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date:

FMEA Number:
Prepared By:
FMEA Date:
Revision Date:
Page:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Zome Power Distribution Cabinet	Open circuit	Loss of 1 power source to RIOs	2	Physical damage (loose connections, fire) Natural Fault (loss of insulation)	1	Proper bolting and securing	1	**2**						
Zone Power Distribution Interconnecting line	Short Circuit	Loss of 1 power source to RIOs	2	Physical damage (water ingress, fire) Natural Fault (loss of insulation)	1	Creepage Distances IP grading Insulation Test Material Certification	1	**2**						
Zone Power Distribution Interconnecting line	Open circuit	Loss of 1 power source to RIOs	2	Physical damage (loose connections, fire) Natural Fault (loss of insulation)	1	Proper bolting and securing	1	**2**						
IAS UPS	No Output	Loss of 1 power source to RIOs	2	Internal fault Production Defect Hardware Errata	2	Climatic Certification Fitness to environment	1	**4**						
IAS UPS	No Main Input	No effect (emergency and battery backup)	1	Main Power Supply System failure Main Power Distribution System failure	3		1	**3**						
IAS UPS	No Emergency Input	No effect (main and battery backup)	1	Emergency Power Supply System failure Emergency Power Distribution System failure	2		1	**2**						

Page 3 of 8

Fig. 43: *IAS*, Decomposition Level 2, *FMEA* Page 3

System: Design Verification Process
Subsystem: IAS
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date:

FMEA Number:
Prepared By:
FMEA Date:
Revision Date:
Page:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
IAS UPS	No Battery Input	No effect (main and emergency backup)	1	Battery failure (see IAS UPS Battery bank)	2		1	**2**						
IAS UPS	No Main & Emergency Input (Black Out)	No effect (battery backup)	1	MPSS failure and EPSS starting	3		1	**3**						
IAS UPS	No Main & Emergency Input (Black Out)	No effect (battery backup)	1	MPSS and EPSS failure (Abandon Ship)	1		1	**1**						
IAS UPS Battery Bank	No Output	Loss of 1 power source to RIOs	2	Production Defect (battery fuse trip due to overcharge and consequential overhating)	2	Charging current limitation Temperature Compensation	1	**4**						
IAS UPS Battery Bank	Insufficient stored energy	Loss of 1 power source to RIOs	5	Hardware Errata (Insufficient sizing)	2	Load Balance	1	**10**						
Field Bus Driver RIO	No communication	Loss of communication through field bus channel	1	Production Defects	2		1	**2**						
Field Bus Cable	Cable interrupted	Loss of communication through field bus channel	1	Physical Fault	1		1	**1**						

Page 4 of 8

Fig. 44: *IAS*, Decomposition Level 2, *FMEA* Page 4

System: Design Verification Process
Subsystem: IAS
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date:

FMEA Number:
Prepared By:
FMEA Date:
Revision Date:
Page:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Field Bus Cable	Cable shorted	Loss of communication through field bus channel	1	Physical Fault	1		1	**1**						
Field Bus Driver PCS	No communication	Loss of communication through field bus channel	1	Production Defects	1		1	**1**						
Processor Computer	No output	Loss of control	1	Production Defects	1		1	**1**						
Processor Computer	Wrong Output	Defective control	6	Software flaws Logic Bombs	6	Flow Charts Strong Code Programming	6	**216**	Fault removal (Testing) Fault tolerance.					
Main Ring Board 1 PCS	Component failure	Loss of communication through main ring channel 1	1	Production Defects	2		1	**2**						
Main Ring Board 2 PCS	Component failure	Loss of communication through main ring channel 2	1	Production Defects	2		1	**2**						
Switch Board 1	Component failure	Loss of communication through main	1	Production Defects	2		1	**2**						
Switch Board 2	Component failure	Loss of communication through main ring channel 2	1	Production Defects	2		1	**2**						

Page 5 of 8

Fig. 45: *IAS*, Decomposition Level 2, *FMEA* Page 5

System: Design Verification Process
Subsystem: IAS
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date:

FMEA Number:
Prepared By:
FMEA Date:
Revision Date:
Page:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Network Cable 1	Component failure	Loss of communication through main ring channel 1	1	Physical Fault	1		1	**1**						
Network Cable 2	Component failure	Loss of communication through main ring channel 2	1	Physical Fault	1		1	**1**						
Operator Station 1	Component failure	Loss of control Interface	2	Production Defects	2		1	**4**						
Operator Station 2	Component failure	Loss of control Interface	2	Production Defects	2		1	**4**						
Operator Station 1 & 2	Component failure	Loss of control Interface	5	Production Defects	1		1	**5**						
Main Ring	Component failure	Loss of control Interface	5	Production Defects	1		1	**5**						

Page 6 of 8

Fig. 46: *IAS*, Decomposition Level 2, *FMEA* Page 6

Effect	SEVERITY of Effect	Ranking
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe system operation without warning	10
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe system operation with warning	9
Very High	System inoperable with destructive failure without compromising safety	8
High	System inoperable with equipment damage	7
Moderate	System inoperable with minor damage	6
Low	System inoperable without damage	5
Very Low	System operable with significant degradation of performance	4
Minor	System operable with some degradation of performance	3
Very Minor	System operable with minimal interference	2
None	No effect	1

PROBABILITY of Failure	Failure Prob	Ranking
Very High: Failure is almost inevitable	>1 in 2	10
	1 in 3	9
High: Repeated failures	1 in 8	8
	1 in 20	7
Moderate: Occasional failures	1 in 80	6
	1 in 400	5
	1 in 2,000	4
Low: Relatively few failures	1 in 15,000	3
	1 in 150,000	2
Remote: Failure is unlikely	<1 in 1,500,000	1

Detection	Likelihood of DETECTION by Design Control	Ranking
Absolute Uncertainty	Design control **cannot** detect potential cause/mechanism and subsequent failure mode	10
Very Remote	**Very remote** chance the design control will detect potential cause/mechanism and subsequent failure mode	9
Remote	**Remote** chance the design control will detect potential cause/mechanism and subsequent failure mode	8
Very Low	**Very low** chance the design control will detect potential cause/mechanism and subsequent failure mode	7
Low	**Low** chance the design control will detect potential cause/mechanism and subsequent failure mode	6
Moderate	**Moderate** chance the design control will detect potential cause/mechanism and subsequent failure mode	5
Moderately High	**Moderately High** chance the design control will detect potential cause/mechanism and subsequent failure mode	4
High	**High** chance the design control will detect potential cause/mechanism and subsequent failure mode	3
Very High	**Very high** chance the design control will detect potential cause/mechanism and subsequent failure mode	2
Almost Certain	Design control **will** detect potential cause/mechanism and subsequent failure mode	1

Table 20: ***IAS*, Decomposition Level 2, *FMEA* Definitions**

FMEA in subject covers the development phase; therefore it is a design process *FMEA*. Development phase shall consider development faults and failures, but it cannot disregard faults and failures typical of use phase with potential to impact dependability; that is the reason why physical faults have been included in this sheet.

Numerical values come from author experience, and can be highly debatable. Those values should be the result of a team effort, supported by business intelligence providing statistical data. Despite this fact, and the assumption that this specific *FMEA* is quite general in nature, some comments can be stated.

- Digital sensors fault poses the highest risk on the process, due to its undetectability. Many examples have been brought in this work of contacts serving important purposes (one example, to represent them all, the so called **Ship/Shore Selector**, that indicates *External (Shore) Electrical Power Supply System* is active, and therefore deactivates most of *IAS* functions, as shown in *3.2.1*) which status of health cannot be discerned. Analogue sensors have better performances in terms of fault detection, due to the fact that they are always providing one value within a predetermined range (4-20mA, for instance); any other value indicates fault.
- Digital sensor cables, with their failure modes, may generate erroneous signals, impossible to be discriminated from real. A cable, due to its potential length, is quite exposed to physical damages; from that the increase risk of using digital signals and long cables. Hardwired digital logic shall be used with judgement.
- Wrong control code (wrong action in present of accurate inputs) may cause high potential damages, to service and to equipment. Complicated routines are difficult to verify and therefore must be thoroughly tested (commissioning).

- Wrong information (un-calibrated sensors) affects control code action. Sensor calibration is quintessential to delivering expected service. This case is defined, in taxonomy, as **signal error.**
- Absence of information affects control code action, preventing a sensible calculation. Absence of information though, when detected, can be handled more effectively than wrong information, generally much harder to detect.
- Hardware duplication contributed mitigating consequences of physical failures, but increased consequences of software flaws and logic bombs. More switches with a defective firmware generate more failure mode for the network, as entity.

FMEA can be used to investigate multiple failure effect on system, as done here treating black out; its effectiveness still is to be demonstrated, as it requires as many lines as many combinations of couples of components that can fail in the same time frame. A computer application should detect all possible alternative paths after a first fault or failure, in order to identify couples which can produce important effects. Same procedure should be followed with triples, and so on. This task poses a noticeable burden to team and to computational resources.

3.5.10 *IPS* Level Three and Four, Direct Inspection.

Attention is focused on "common mode branches", or parts of the diagram that collect output from more than one block[82]. Those elements are the most evident potential cause of service disruption.

Direct inspection of relevant diagrams indicates following components as "common branches":

- Block 1.1.4, neutral point resistor, common part, power station 1 (XM/274_PS1)
- Block 1.3.4, neutral point resistor, common part, power station 2 (XM/274_PS2)
- Block 3.1, generator connection sub-system, power station 1
- Block 3.2, generator connection sub-system, power station 2
- Interconnecting line
- Critical power

They are indeed common services for all generators belonging to one power station; their failure implies failure of multiple pieces of equipment. Following comments may be made:

- Failure of block 1.1.4 or block 1.3.4 may be due to natural causes, such as resistor wire breaking, or human made non-deliberate actions, such as loose connection to ship's hull. In any case, as Fig. 22 illustrates, any fault on that specific component jeopardise equi-potential connection and, in case of insulation fault, selective discrimination (protection 67N inactive) and perturbation control (over-voltage due to arcing is higher). Failure severity is quite high, and may be assigned a value of 6 or 7, given the potential harm in an overvoltage.

[82] This consideration is justified by the superficial level of analysis performed here, and does not replace a thorough and systematic work.

- Failure of blocks 1.1.4 and 1.3.4 appear not probable as resistor wire is stored in an IP44 cabinet, therefore protective against external agents (interactions). Connections anyway need be made safe (fault removal) by torque testing. Failure probability appears low; a value of 2 is given.
- Failure of blocks 1.1.4 and 1.3.4 cannot be detected once installed, even though the consequent failure mode appears clear. This solution permits certain savings in alternator initial costs, savings that are to be sacrificed in case of risk mitigation. This case appears a clear trade-off, supported by the assumption that damage is generated when two different faults are active, or an insulation fault and a system fault. To the author the argument seems void, as system failure is dormant. In force of this consideration, detectability value is 10.
- Total *RPN* index is then 120
- Failure of blocks 3.1 and 3.2 may materialise due to check synch relay failure, due to production defects, for instance. It is more unlikely that potential transformer fail. In force of those considerations probability value is assigned as 2[83].
- Failure modes of interest concern check synch output contact, that can be stuck open (open when it should be closed) or stuck closed (closed when it should be open). Failure severity has different ratings according to occurrences: the former causes no generator to connect, resulting in a severity rating of 5; the latter may cause severe damages to equipment, raising the severity rating to 8.
- Failure of blocks 3.1 and 3.2 is not detected in this project, even though the consequences are well known. Class requirement force generators to be built to face such a stress, but this stress does not form part of typical *FAT* schedule, so fulfilment is not proven beyond manufacturer reputability. For those reasons, the assigned detectability value is 10.
- Failure of blocks 3.1 and 3.2 has then an *RPN* index of 160 or 100.
- Failure of interconnecting line may happen as the result of a physical interaction fault (cable damaged) or a natural fault (loss of insulation, water ingress, fire). Those occurrences are not frequent; therefore a probability rating of 2 is assigned.
- Failure of interconnecting line is considered at design stage, and protections are put in place to cater with the occurrence. Should the interconnecting line fail, then *IPS* fails, in the configuration under discussion, fails in turn. Severity rating is assigned as 5.
- As already stated, interconnecting line failure is a well appreciated occurrence, therefore its detectability rating is assigned as 1
- Interconnecting line failure has a *RPN* of 10.
- Critical Power Supply Sub-system is a highly duplicated system as Fig. 23 exemplifies. Failures within this system have negligible chance to propagate.

3.5.11 Control Code, Direct Inspection

Fig. 40 suggests some considerations:

- Black out branch is not considered, as not pertinent with case under investigation.

[83] Indeed the author has never seen such a case.

- Code is duplicated and executed on two different machines at the same time, only one writing outputs.
- Signals are not duplicated, therefore any loss of signal implies *IPS* power management (*IAS*, to keep consistency with diagrams, albeit power management is a part of *IAS*) failure.
- Signal failures imply different failure modes[84]:
    - Loss of stand by status if lost signal measures were to confirm stand by status. This failure mode does not necessary imply *IPS* failure: *IPS* delivers its expected service until a further failure happens on an active generator. On the other hand, the presence of a stand by machine grants the capability of fulfilling power requests. Accounting for the hypothesis of positive capability for five generators to sustain vessel load in given configuration and present conditions, diagram may be modified as per Fig. 47. It might appear perhaps more correct stating that stand by failure leads to a degraded mode rather than a failure.
    - Loss of status (active generators). Any failure in blocks 2.1, 2.2, 2.5, 7.3, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 7.1, 7.2 and 8.1 implies affected generator is not longer available for power management, and it must be replaced. This control code action is expected, so control code has not failed, *IPS* has, as superior system.
    - Loss of control. Block 2.3 failure implies loss of control over affected generator. Generator must be replaced, causing power limitation and temporary *IPS* failure.
- Inasmuch control code is concerned, following must be noted:
    - Diagram reflects a possible software coding, but not necessary the best possible implementation. Blocks are then representing code routines, and their failure is defined as no output to following dependent block, or routine. Treating software failures goes beyond the purpose of this work.
    - Decomposition level is still not entirely adequate to capture all possible aspects, as already mentioned in *3.4.7*. Control code *RBD* has, in this work, the function of providing a better insight of system functioning, rather than being an accurate tool to analyse code dependability.
    - Fig. 40 lists control code expected functions; therefore, strictly speaking, a failure of any of them implies failure of control code. Several degraded configurations can then be defined, in which one or more functions can be thought of being unavailable or failed. Pushing the technical aspects to its limit, it can be affirmed that, under hypotheses drawn so far, a complete *IAS* failure could be tolerated, as far as direct controls are delivering their expected service, and no other faults affecting remaining parts are coming; this situation is clearly not acceptable due to loss of awareness about system situation and possible incoming failure consequences. This aspect confirms assumption of *IAS* fully working.
- Status signals are mostly binary in nature, in this project. This fact exposes system to errors, which are most likely to happen when digital signals are used. A wrong status signal may generate wrong actions and thus causing system failure.
- Block 5.8 status is partially detected, as it comes from a sensor detecting XM/274X only. Earthing sub-system consists of two pieces (refer to Fig. 22), of which only one is monitored, for intentional

[84] It is important highlighting those failures are not control code failures, they are failures control code handles in such a way that implies *IPS* failure.

disconnection only (no health controls are made on XM/274X and XM/274_PSX). Block 5.8 failure is, to all extents, **dormant**.

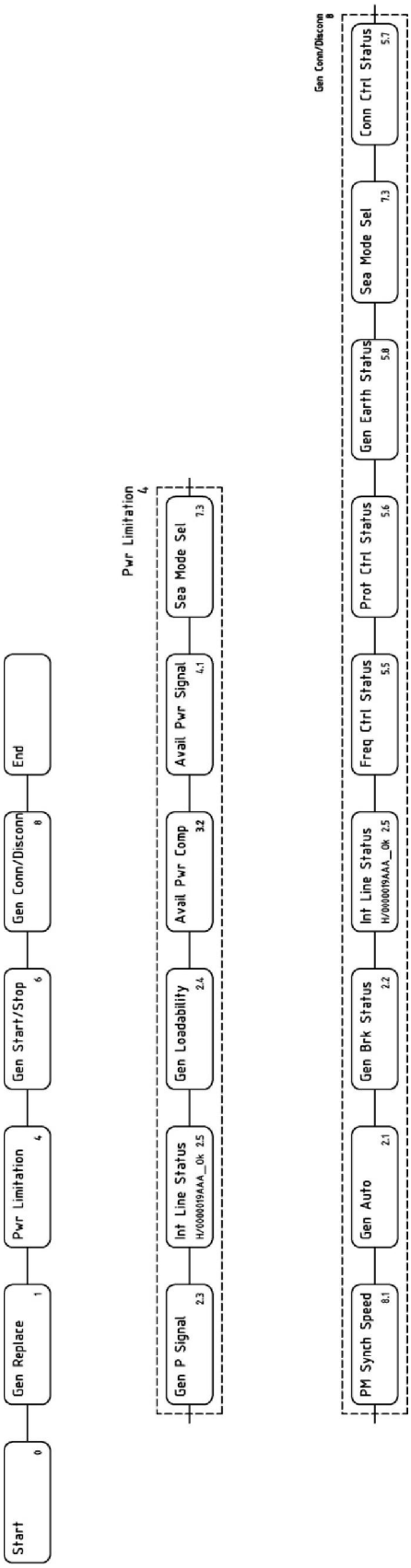

Fig. 47: Control Code, Decomposition, ***RBD***. Modification After Hypothesis Account

4. Analysis Results: Design Improvements.

Now that analysis is complete, and possible dependability hazards are identified, mitigation proposals can be formulated, together with a rough quantification of benefit. Reliability function of new proposed configuration is elaborated and relevant metrics applied in order to do a direct numerical comparison.

4.1 Information Implicit Redundancy.

Section *3.5.11* highlights consequences of sensor loss, in terms of *IPS* failure mode, in the configuration in subject. Failure of two active power feedback signals implies *IPS* failure (in the configuration under analysis). It must be observed that conditions set forth in *1.3.1.1* are fulfilled, so such failure does not bear class consequences (as expected, given the fact that configuration in subject is not classed), but can affect vessel trading ability, thus bearing substantial financial consequences; elimination or tolerance of this failure mode can then offer benefits in terms of risk mitigation.

In this project generator output active power is measured by means of dedicated transducers, fit within generator auxiliary compartment (*IAS*). Those transducers constitute the sole source of that information to the process; should they fail, then the associated function fails as well, with the already anticipated consequences.

Generator active power is measured, although not as prime task, in two other components: *Generator Voltage Control* and *Generator Protection PLC*. The former measures reactive power to calculate voltage droop, and to that extent uses same signals used to measure active power (line voltages, phase currents and their mutual phase displacements); the latter measures generator impedance in terms of active and reactive power to detect loss of excitation and reverse active and/or reactive power.

It is now apparent there is a potential implicit redundancy in active power information: this information is available and can be collected from different sub-systems (and, in this specific case, information is of good accuracy as well); additional values can be used for control purposes with minimal expenditure.

These multiple measures (sensor output) can be used in two different manners:

- 2/3 active redundancy (or **voting**). Measured value is chosen between the two results that are closest each other; third value belongs to a sensor which is to be declared failed.
- 1/3 stand by. All three signals are considered equally valid, despite their difference in values, and are chosen in a predetermined sequence, upon failure (decided when output exceeds given range).

Assuming all three sensors have same reliability, following comparison can be made:

Single Sensor	***2oo3***	**Stand by**
$MTTF = \int_0^\infty e^{-\lambda t} dt = \frac{1}{\lambda}$	$MTTF = \int_0^\infty \left(e^{-3\lambda t} + 3e^{-2\lambda t}\left(1 - e^{-\lambda t}\right)\right) dt$ $MTTF = \frac{5}{6\lambda}$	$MTTF = \int_0^\infty \left(3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}\right) dt$ $MTTF = \frac{11}{6\lambda}$

Table 21: Comparison Among Different Redundancy Schemes.

Table 21 allows an important consideration: *MTTF* is calculated assuming standby unit is healthy; this assumption is not necessary supported, and in this case needs a further explanation. In this case output is considered healthy when its value is within expected range (being sensor output analogue in nature), but nothing can be said on its accuracy. This explains results; indeed *2oo3* is less reliable than stand by due to more failure configurations (in fact two sensors must be healthy at the same time), but *2oo3* is superior in terms of detectability, because sensor inaccuracy can be detected comparing sensor output. This fact adds a further failure condition, in addition to the **consistency check** (the fact that signal is consistent, or its value stays within the expected window): sensor output value must be close enough to another sensor output value.

Should not detectability be a stressing factor (in the end, power signals coming from *AVR* and protection PLC are core, and their failure would coincide with sub-system failure, which is detected), then standby redundancy option should be chosen. In this case, *MTTF* would result higher by a 11/6 factor (1.83) at the expenses of the addition of 2 analogue signals (meaning in this case cables and *I/O* modules, assuming no serial link is established among devices in subject) per each generator, total 12.

4.2 Digital Sensor Duplication, Reflection, Design Diversity.

Arguments discussed under *4.1* may be replicated here, with the remarkable exception that there is no implicit redundancy in most cases for digital sensors; redundancy must be created. Question is finding out which redundancy is most effective. Digital sensors needs be classified into three main categories:

- Behavioural switches: interfaces to operators to activate modes or special configurations (ship/shore, harbour/manoeuvring/open sea, etc.). Those signals are generated by operators, acting on dedicated devices, and directed to *IAS* by means of the acquisition chain explained under *3.1.3.8*.
- Control switches: signals to represent statuses or pieces of information, generated by instrumentation and not by operators, and directed to *IAS* via the acquisition chain.
- Digital outputs. Those signals are generated by *IAS* and directed to controlled equipment via the acquisition chain.

It is quite evident behavioural switches have in general larger scale implications than control switches, therefore they require more attention.

Behavioural switches are best acquired via HMI, given the fact that signal transmission chain (Fig. 35) is not used, except the link between operator stations and process computers. Resulting reliability is expressed as:

$$R_{Behavioural\ Switch} = R_{NC} * R_{PCS} * R_{PC}$$

This value is inherently higher than a field device, owing to the fact that many factors smaller than 1 are not present (see Table 19). Failure detectability may be enhanced by requesting further confirmation before initiating transition, and by using colour code (colour changing on some element in the HMI, technique

known under the name of reflection, as it reflects input status to feedback device, the operator)[85]. Failure probability amounts to that of a memory block losing its information, thus quite low.

Field devices cannot be managed in this way; therefore multiplication appears the only workable way. Still many different approaches may be followed:

- Complete duplication: sensor head, output contact (*DPDT* or *DPCO*, to use a common industrial standard on naming), cable and data acquisition board. Multiplication imposes conditions helping system detecting faults: indication coming from corresponding contacts on different sensor heads must be same at all times; different contacts coming from same sensor head must be different at all times. Former condition informs on sensor head fault or inaccurate calibration (compared to other sensor head), whilst latter informs on cable or digital acquisition hardware status. Should these conditions be violated, the associated sensor pool is declared failed, associated action suspended and an alarm rose to attract operators' attention. Fault detectability level reduces considerably, and so does reliability (now one hardware set is replaced by two same hardware sets, in series, as both sensor assemblies must be fully working to allow detectability), that halves[86]. Reliability level may be enhanced using *2oo3* voting (from 0.5 to 0.833), with well known by now cost consequences.
- Partial duplication: output contact and digital acquisition hardware. This configuration allows partial fault detection (cable and/or acquisition equipment failure), leaving any sensor head failure undetected, or dormant. Detectability rating decreases, and so does reliability (compared to real case scenario), owing to the fact that there are now two contacts that can fail instead of one.
- Signal substitution. Any digital contact can be transformed into an analogue using a resistor network and appropriate acquisition hardware. Open contact situation is now represented by a certain minimum current flow through resistive network, and contact closed situation by a certain maximum. Both these predetermined values must lie within signal integrity threshold. This technique improves cable failure detection in the same way partial duplication did, at the expenses of an additional hardware, or the resistive network, and enhanced data acquisition equipment. On the other hand, it offers savings related to acquisition hardware duplication. Considering acquisition hardware is nowadays self-monitored, fault detectability rating appears consequently low; this consequence permits decreasing rating on that component, focusing on cable failure detection. In this respect, signal substitution seems a better compromise compared to partial duplication.

IAS output signals can be treated in the same fashion input signals have been, giving rise to same considerations and potential solutions, with associated costs and benefits.

To turn these suggestions into factual management decisions, reliability indexes need be known and trusted. By means of those numerical values real benefits can be calculated, and a cost associated. *FMEA* proves useful in this respect: providing a prioritized list of action, according to their *RPN*; this priority list can be

[85] Using operators as feedback sensors should be a discouraged practice, given their unpredictability; still rules make wide use of this strategy.

[86] Strictly speaking overall reliability reduces more than that, as a sensor head carries two contacts, driving each one a cable and acquisition hardware. Final setup consists of four contacts, four cables (albeit a multi-core cable can be adopted) and four IO boards, as opposed to one contact, one cable and one IO board. Hardware count has more than doubled, with known consequences on reliability.

translated into a management tool to plan expenditures. Assuming that every items exceeding *RPN* 200 are "must do", then budget must be allocated as the *FMEA* is compiled and approved, and so forth.

Oil and Gas sector, for instance, attaches great importance to safety sensor failure detection, therefore *2oo3* multiplication scheme is used when comes to fire and gas detectors, fire dampers, etc. Cruise sector, for instance, does not have same consideration of those issues, and uses simple detection (one sensor head, one output contact, one cable and one data acquisition card) for fire dampers, and loop detection (can be thought of digital substitution) for fire and smoke sensors[87]. This different sensitivity may be explained with different fire risk, quite high due to quantity and nature of combustible material on an O&G installation, quite reduced on a cruise vessel.

4.3 *Generator Connection Control* Redundancy.

This project is equipped with two such sub-systems, described under *3.1.3.3*. *FTA* in Fig. 48 illustrates their functioning principle. The figure in question is obtained observing drawings and following information flow, making it resembling more closely physical implementation. Current implementation foresees bus bar potential transformer signal, one phase only, is distributed along one power station switchboard to reach all generators; signal distribution line is electrically protected by a miniaturised automatic circuit breaker.

Fig. 48 can be rearranged in a different form simply using Boolean operators. This new form indicates in a more immediate fashion the importance of certain components. Fig. 49 shows effects of rearrangement.

Here bus bar connection control is not considered, as seen as a sub-mode within the system. Five different failure modes can be identified:

- Bus bar potential transformer failure.
- Bus bar potential transformer signal distribution line failure.
- Generator potential transformer failure.
- Check synch relay failure.
- Synchroniser failure.
- Critical Electrical Power Supply System failure

First and second failure mode affects entire power station, as bus bar voltage signal is detected in one place only; remaining affect one generator only. Last failure mode affects entire power station, but system in consideration has a high level of redundancy implemented already. Main focus is then directed towards failures affecting the entire power station, tentatively, for its larger reward in terms of dependability, clearly pointed out in Fig. 49.

[87] It must anyway be said cruise ship adopt a failsafe principle with safety systems: dampers, for instance, are kept in unsafe position by powering a coil, and they are spring-loaded: any power failure (induced by fire or not) causes damper to close. In addition, a melt link is installed: this link melts as the air temperature in the duct increase by effect of fire; if link melts, damper closes. Should all other means fail, this will actuate. Inasmuch fire detectors are concerned, a failure in a head will trigger fire alarm.

Fig. 49 does not make evident a further aspect, in the physical implementation, that corroborates even further previous statements: bus bar voltage is distributed by means of inter-panel wirings, jointed at each panel. As a consequence, wiring has different extension and composition according to panel considered. Fig. 49 contains then a simplifying assumption, made to tune model to worst case scenario: wiring is indeed the longest leg, with most joints. This fact, compared with generator wiring, corroborates the statement that bus bar voltage signal is more critical than generator voltage signal, as anticipated.

Resulting *FMEA* sheet is shown in Fig. 50. Loss of signal is strongly connected to failure in physical wiring, and to potential transformers, albeit to a lesser extent. Most of mentioned failures are undetected; the only one detected is actually automatic circuit breaker trip, which causes are short circuits induced by production defects or natural causes.

Both these failure causes may be tolerated duplicating bus bar potential transformers, or using check synchronisers capable of managing more than one phase. Installing additional potential transformers could be done within generators bus bars cubicles, and would carry further benefits connected with shorter wiring length and ease of troubleshooting (no inter-cubicle wiring, less joints and self-containment); detectability factors would reduce to 1 (duplicated detection) and so would severity.

Multiphase parallel detection could save additional potential transformer installation, but would increase in turn chances of failure connected to natural causes (loose connections due to vibrations, for instance), the most common. Detectability would reduce as per previous case, thus enabling timely corrective maintenance, and so would severity. Unfortunately, after a first and approximate market research, no such component appears available; complete synchroniser assembly should be duplicated. This would add synchroniser failure detection if *IAS* could detect synchroniser output contacts and synchronisers were connected as ***1oo2*** set, or in logical OR (at least one synchroniser shall grant permission); in that case *IAS* could declare synchroniser not generating output as failed. Check Synchronisers could be triplicated, so that all phases are covered; in this case a *2oo3* scheme may be used. Benefits in terms of dependability are well known by now.

There are many other possibilities, among which one deserves attention: synchroniser sends its closing signal to *IAS*, which sends as a consequence an appropriate closing pulse. Reliability calculation ought to include now *IAS*, input detection and output confirmation, but other factors can impact balance: stuck closed signal could be detected as “untimely”: clearly generators are very unlikely to be in synch before actual synchronisation starts, for instance. If *IAS* reliability is much greater than components, then this option can be appealing.

ACB missing trip (un-detected short circuit or failure in opening contacts) represents a present threat, which should be mitigated consistently with what done for threats having lower *RPN*. This threat may be mitigated by selecting a synchroniser which detects input signal level and activates if that level exceeds a pre-determined level (say 85% of rated voltage, in this case), under the assumption that a short circuit would only reduce voltage level, leaving waveform unaltered. Still fault would not be detected before use (and this is most unwanted failure effect), but severity rating would reduce from 6 to 5, lowering *RPN* to 50.

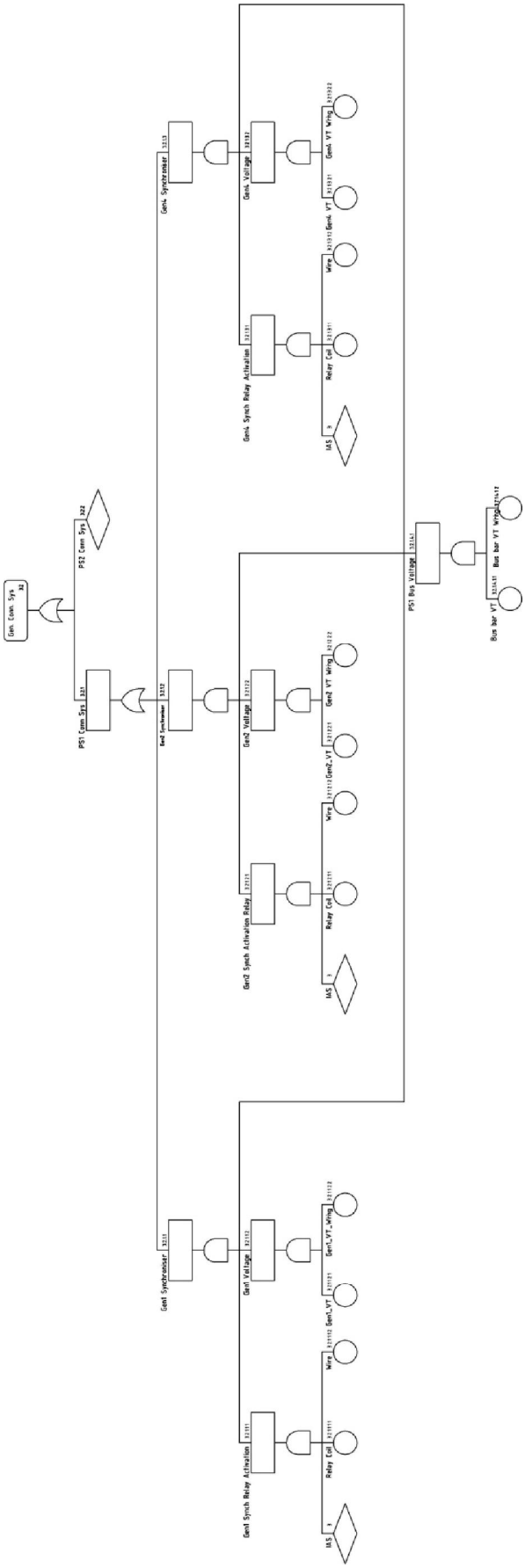

Fig. 48: ***Generator Connection Control, FTA***.

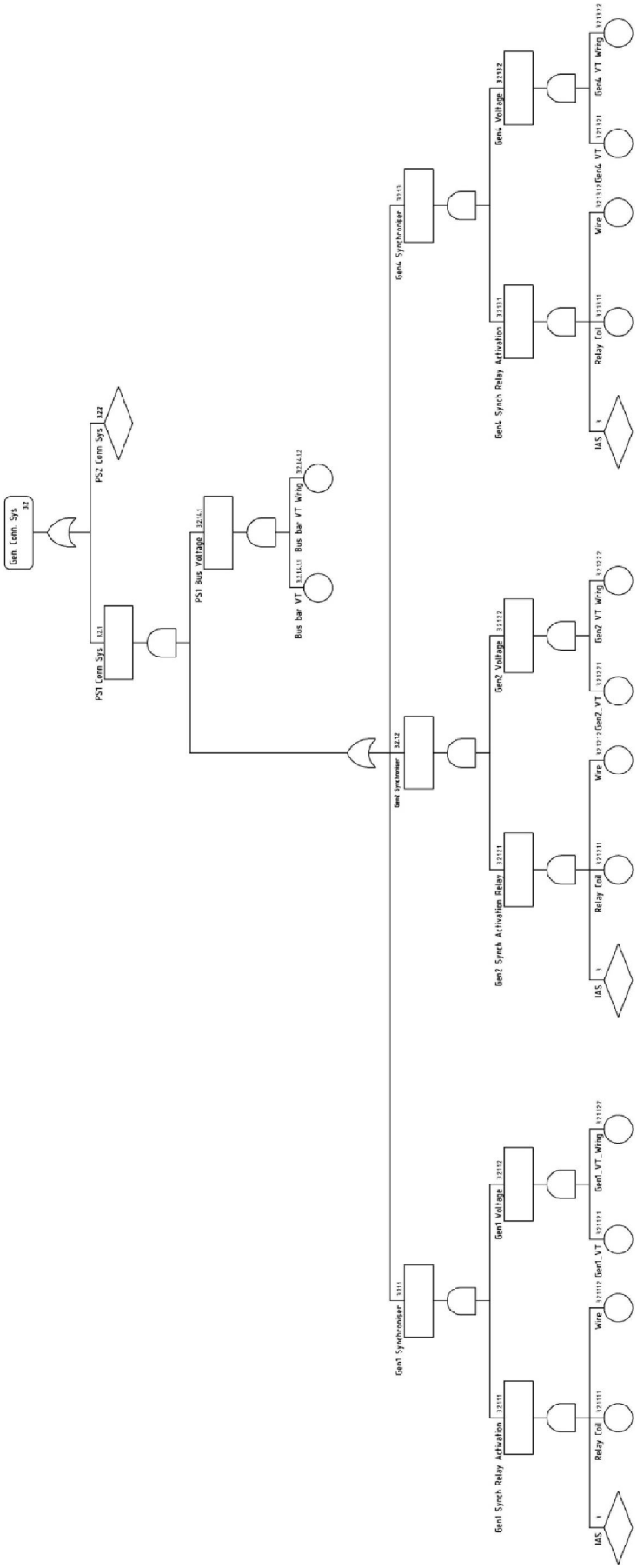

Fig. 49: ***Generator Connection Control*, *FTA*, Rearranged**

System: IAS
Subsystem: Generator Connection Control System
Component:
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)
Key Date:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN
Bus Bar Potential Transformer	Coil wire rupture	No signal No Parallel	5	Production Defect	1	Testing Routine	10	**50**
	Loss of Insulation	No signal No Parallel	5	Ageing (Natural Factor) Product Defect	1	Testing Routine	10	**50**
Miniaturised Automatic Circuit Breaker	Spurious Trip	No signal No Parallel	5	Production Defect	1	Testing Routine	1	**5**
	No Trip	Bad Parallel signal	6	Production Defect (MACB)	1	Testing Routine	10	**60**
Signal Distribution Line	Short Circuit	Absent Parallel Signal	5	Insulation failure (Production Defect)	1	Testing Routine	1	**5**
Signal Distribution Line	Open Circuit	Absent Parallel Signal	5	Loose of bad connection	4	Testing Routine	10	**200**

Fig. 50: ***Generator Connection Control*** Sub-system, ***FMEA***

4.4 Generator Neutral Point Earthing System Failure Detection.

This system is active only during earth faults affecting *Main Electrical Power Supply System*, high voltage users and part of *Main Distribution System*; rest of time is inactive. There is no instrumentation monitoring its state of readiness.

In terms of *FMEA*, referring to Fig. 22, following considerations may be drawn:

- Failures with higher *RPN* are those implying total circuit opening, or missing earthing connection. Those failures bear potentially heavy consequences in terms of machinery maintenance; they relative importance is quite apparent.
- *FMEA* has been elaborated assuming that more than one generator is active on both power stations (coherently with case study). Should this assumption be removed, there would be no difference between common resistor generator and cable failures, as all would imply circuit opening.
- Failure of one out of two or three generator resistor would only change zero sequence impedance, slightly changing network impedance; effects are less than complete circuit opening.
- Sub-system failures are **dormant** (highest detectability score); they are not detected before sub-system use.

This failure can be removed by upgrading all component insulation level, so they can withstand addition stress deriving from keeping neutral point un-earthed. This option carries important technical consequences

in terms of catering with earth failure selective discrimination, and financial consequences, as it affects many pieces of equipment.

System: Main Power Supply
Subsystem: Power Station
Component: Generator Earthing Sub-system
Design Lead:
Core Team:

Potential Failure Mode and Effects Analysis (Design FMEA)
Key Date:

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN
XM/274X	Open circuit	Over Voltage in case of Insulation Loss	4	Production Defects Hardware Errata	3		10	**120**
Cable from XA/274X to XM/274X	Open circuit	Over Voltage in case of Insulation Loss	4	Production Defects Hardware Errata	3		10	**120**
Cable from XA/274X to XM/274X	Earth Fault	Over Voltage in case of Insulation Loss	4	Production Defects Hardware Errata	3		10	**120**
Maintenance switch	Open circuit	Over Voltage in case of Insulation Loss	4	Production Defects Hardware Errata	3		10	**120**
Maintenance switch status sensor	Open detection of closed switch	Generator start inhibited	3	Production Defects Natural Causes Hardware Errata	3		10	**90**
Maintenance switch status sensor	Closed detection of open switch	Over Voltage in case of Insulation Loss	4	Production Defects Hardware Errata	3		10	**120**
Cable from maintenance switch status sensor to IAS	Open Circuit	Generator start inhited	3	Production Defects Natural Causes Hardware Errata	3		10	**90**
Cable from maintenance switch status sensor to IAS	Short Circuit	Over Voltage in case of Insulation Loss	7	Production Defects Hardware Errata	3		10	**210**
Cable from XM/274X to XM/274_PSX	Open circuit	Over Voltage in case of Insulation Loss	7	Production Defects Hardware Errata	3		10	**210**
Cable from XM/274X to XM/274_PSX	Intermittent Earth Connection	Over Voltage in case of Insulation Loss	7	Production Defects Hardware Errata	3		10	**210**

Fig. 51: Generator Neutral Point Earthing Sub-System, *FMEA*

This failure can be tolerated reducing its *RPN* within to more acceptable values detecting circuit continuity. Detection circuit, a Wheatstone bridge, for example, would need special precautions, given the possibility that voltage rises to kV level during earth faults, but would enable sub-system failure awareness before use. Such detecting circuitry could measure overall resistance in any given configuration, backing up maintenance switch sensor information.

Equipment capable of performing requested monitoring is available on the market. Its use would reduce detectability rating to 1, reducing in turn *RPN* down to 21, rather acceptable. Of course, its reliability and failure mode should be investigated.

4.5 Interconnecting Line Failure Handling.

This failure, albeit being similar to ones treated in Sections from *4.1* to *4.4*, bears more important implications. For this reason, a dedicated section has been created, with relevant sub-sections.

4.5.1 Redundancy.

Interconnecting line can be simply duplicated; and duplicated used as stand by component. Resulting *RBD* is illustrated in Fig. 52.

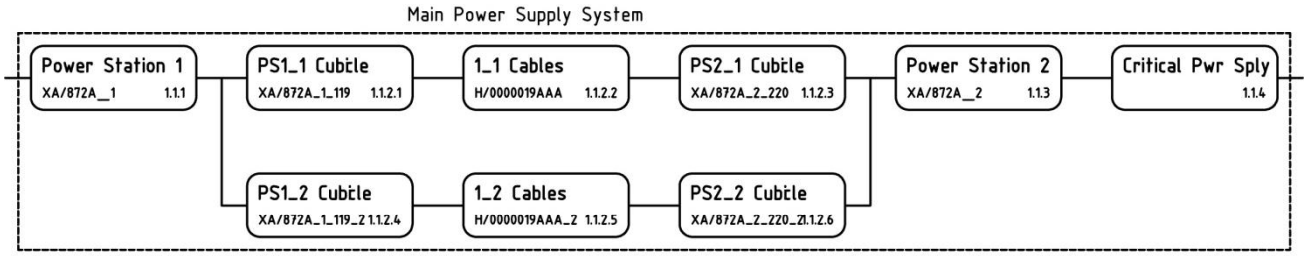

Fig. 52: Interconnecting Line Duplication, *RBD*

Be λ interconnecting line *MTTF*: duplicate set *MTTF* is, according to [**26**]:

$$\lambda_{DuplicateSet} = \frac{5}{2\lambda}$$

MTTF has increased by a factor of 2.5 as a consequence of duplication. Configuration under investigation would then benefit for this upgrade by a factor 2.5.

Management would require dedicated controls, as upon failure, power stations need be synchronised before being able to use spare interconnecting line. Control appliances for this purpose are available on the market and can be easily implemented, with desired level of redundancy.

Failure in discussion is not very frequent, at least on cruise vessels; this may discourage undertaking this modification, which has a sensible impact in terms of costs and space occupancy.

4.5.2 Ring Power Network Topologies.

A ring configuration would have same *RBD* of Fig. 52; second interconnecting line would be permanently energised. This fact would remove need for synchronisation in case of failure, but would worsen reactive power sharing, due to interconnecting line impedance[88]. The amount of worsening depends upon that impedance, and must be quantified to assess adherence to rules in that respect. Clearly, this drawback can be eliminated with a different control strategy, namely reactive power control.

Fault discrimination would require interconnecting line differential protection, to rapidly identifying internal failures and thus open the right interconnecting line, in case of failure. Logic would not be much different from what shown in *3.1.3.4*; any failure external to both transmission lines would case trip of both interconnecting lines; any failure internal to an interconnecting line would cause trip of that interconnecting line, keeping the other active.

[88] In the hypothesis of keeping machine terminal voltage droop controlled.

This solution appears superior to that illustrated in *4.5.1*, as it implies higher failure response readiness. Hardware bill of materials favours this solution too, as parallel arrangements do not need duplication, given the fact that power plant splitting is recovered with one parallel only, after failure has been removed. This save in components is partially offset by the need of twelve current transformers and two differential relays. Again, it can be noted as this increase in instrumentation reduces repairing times, providing unambiguous fault location identification.

4.5.3 Propulsion System Arrangement

Interconnecting line failure causes service failure due to a specific request propulsion system, a user, introduces in virtue of its own architecture. Referring to Fig. 2, and imagining of removing that cross connection making so that each shaft line is supplied from one power station only (converter redundancy, or the ability of providing propulsion in case of one converter failure would not be lost, as well as air gap compensation); this new configuration would not suffer from interconnecting line failure, as power supplies to shaft lines would always be synchronised, as coming from same power station.

Alternatively, if a converter typology capable of managing unsynchronised power supplies (by adopting a controlled rectification stage, for instance) was available, capable of keeping *THD* within specified values, again interconnecting line failure would not be considered a failure mode for *IPS* in given configuration.

Removing cross connection would cause full propulsion to be available on one shaft line, whist the other had no power, during fault conditions; controlling ship course in this condition is perhaps not easy. At the same time it must be retained such a failure, a complete power station failure or grid distribution failure involving one high voltage bus bar system, is an unlikely event if physical faults and/or development faults are considered[89].

Enhanced converter typology or ring network configuration would allow keeping cross supplying arrangement; in this respect they should be favoured.

[89] Conclusion could be different if malicious faults were to be considered.

5. Conclusions.

5.1 Summary and Conclusions.

This work aims at defining and describing a systematic method of evaluating *AES IPS* dependability, as part of standard design procedure. To that extent, following aspects were considered:

- Expected services and threats. Expected services are defined by owners' technical specification, international and marine classification society rule corpus. Additional requirements may be enforced locally, as result of local laws. Expected threats are formalised, although partially, in this very same documentation. *Part 1* is dedicated to this purpose.
- Dependability. Dependability attribute is defined and its importance discussed. Dependability is the objective of systematic method; techniques directed to its measurable achievement are explained. Dependability is directly related to expected service, previously discussed in part 1. *Part 2* is dedicated to this purpose.
- Application to a real case study. This case is described and rearranged to highlight expected services defined in part 1. This case is re-elaborated in a form suitable for investigation, according to part 2. *Part 3* is dedicated to this purpose.
- Analysis of results. Some of results obtained from part 3 are further analysed. Solutions are proposed and their impact to dependability evaluated, according to what presented in part 2. *Part 4* is dedicated to this purpose.

In addition to those key aspects, some other peculiarities have been illustrated:

- Method integration with present design practice. *Section 2.4.2* shows proposed method can be implemented on pre-existing design procedures, without requiring a great extent of additional work.
- Method integration with classification society's way of proceeding and defining entities.
- Business intelligence consolidation. Proposed method promotes an in deep investigation of component properties and way of functioning. Diagrams consolidate visually this knowledge, which is part of design core activity.
- Management tool. Proposed method can be used as management tool to assess design progress. Decomposition level offers a direct insight of design definition, and *FMEA* of design analysis. Meetings with customers may be scheduled using diagrams as agenda, as they reflect present system functionalities and behaviour. Open issues, requests or different implementations may be benchmarked according to their *RPN* and eventually confirmed for design changes or discarded as not offering measurable benefit.

Results presented in this work are far from being considered exhaustive; it has been demonstrated a complete dependability analysis requires numerical elaboration support. On the other hand, said results have been obtained with reduced information and elaboration capacity, giving a clear indication of method potentialities. Once again, principal purpose of present work is not obtaining results, but defining an efficient method to obtain result.

Proposed actions need be considered under different viewpoints, such as financial, time to market, training, etc. Scope of this work is providing methods to increase dependability in a measurable way.

This work covers only certain dependability aspects. Safety, security, confidentiality, maintainability and integrity are left to different disciplines.

This work covers only certain threats, symbolised by faults. Threats covered are ones coming from software flaws, logic bombs, hardware errata, production defects physical deterioration and input mistakes; those coming from physical interference, intrusion attempts and viruses and worms are left to different disciplines. This choice has been dictated by classification society approach, which considers listed faults only.

A comprehensive dependability analysis shall not avoid these multidisciplinary aspects.

5.2 Future Research Directions

This work has proven that dependability, a highly desirable product attribute, relays upon information. Services electrical power supply, grid/distribution and integrated automation system are to deliver must be defined with great accuracy in terms of objectives and means to achieve those objectives. Objectives are set by owners, being the reason why vessel has built; objectives are accomplished by means of users, which are the entities having benefits from services and, in general, are the entities services are directed to.

Classification rules help defining the overall work frame by imposing constraints on both services and users, in terms of quality, quantity and variety of services offered; still many options are available and cases uncovered. Constraints are normally defined in general terms, in order to cover as many different implementations as possible; this lack of precise details often brings discussions, fuelled by interpretations.

Level of process automation fits definitely that description. Rules specify automation levels, but do not state precise requirements in case of failure. Fact that *IAS* may completely fail is contemplated in rule corpus, and measures are indicated to mitigate consequences; such measures do normally resource to operators, whose number, capabilities and competency is undefined. Reduced manning may be sufficient to manage a complex vessel with *IAS* fully functioning, but perhaps may not be in case *IAS* completely fails.

Rules introduced stringent requirements as regards to *IAS* complete failures, demanding all pieces of hardware are duplicated, and application code thoroughly tested; still backup manual provisions haven't been removed. As manning is related to the number of expected simultaneous manual operations, and that number may tentatively calculated by counting all possible manual operations; it can be seen *IAS* level, whichever, should not affect manning, by the simple fact that manual backup is still there and operable. Approach illustrated in this work may provide elements to releasing a guideline in this respect. System functioning may be modelled in terms of components required, and a final reliability index calculated (*RPN*, just to mention one used). Expected faults may be modelled in the same, consistent way, and incorporated in system model to verify consequences and their severity (model verification). Once that *RPN* rating is confirmed, then guidelines may be issued requesting mitigation for occurrences which *RPN* rating exceeds a certain level. Defining that certain level can be an interesting research development.

Manual operation effectiveness needs assessment. Attitude has changed towards manual backup, as *1.3.5* has unveiled. In most of occurrences, direct control duplication is the only viable way to back up a direct control. Generator voltage or frequency control cannot be thought to be made in manual in a network with dynamics comparable with a ship. Still many companies decide not to invest in this solution because not contemplated in rule corpus, therefore not offering any benefit. Interestingly enough, most manual backup solution make use of hardware they should substitute (raise/lower speed switch substitutes reference generator only, not fuel rack actuator). If manual backup was demonstrated to be not equivalent, in terms of

service, to the direct control it was meant to replace, then rules may be updated and level of safety and service effectively restored as intended. Defining a metric for evaluating manual backup effectiveness compared to a control solution can be an interesting research development. *RPN* may be generalised including an effectiveness rating and manual and control replicated solutions compared. Preferred option would be then the one showing lower *RPN*.

Recent rule developments in terms of comfort have introduced new constraints applicable to normal services (usually classification societies put most effort in disciplining emergency service). Environmental rules act in this very same direction, disciplining normal services. Translating those new requirements in terms of model elements may be an interesting field of research.

Bibliography

[1] Horst W. Koehler and Werner Oehlers, "95 Years of Diesel-Electric Propulsion Form a Makeshift Solution to a Modern Propulsion System," in *2nd International Conference on Diesel-Electric Propulsion*, Helsinki, 1998, pp. 1-11.

[2] Norbert H. Doerry, "Powering the Future with the Integrated Power System," *NAVAL ENGINEERS JOURNAL*, pp. 267-279, May 1996.

[3] Joseph Framme, in *ASNE Intelligent Ship Symposium*, 1994, pp. 1-20.

[4] Dr. Z. Oya Özçayir, "THE USE OF PORT STATE CONTROL IN MARITIME INDUSTRY AND APPLICATION OF THE PARIS MOU," *Ocean and Coastal Law Journal*, vol. 14, no. 2, pp. 201-239, 2009. [Online]. *http://mainelaw.maine.edu/academics/oclj/pdf/vol14_2/vol14_oclj_201.pdf*

[5] Det Norske Veritas. (2013, July) DNV - GL. [Online]. *https://exchange.dnv.com/publishing/RulesShip/*

[6] Algidiras, Fellow, IEEE Avizienis, Jean-Claude Laprie, Brian Randell, and Carl, Senior Member, IEEE Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1*, pp. 11-33, JANUARY-MARCH 2004.

[7] Det Norske Veritas, "Standard for Certification No. 2.25," in *Electrical Shore Connections/Cold Ironing*.: Det Norske Veritas, January 2012.

[8] American Bureau of Shipping,.: American Bureau of Shipping, November 2011.

[9] International Maritime Organisation, *SOLAS (International Convention on Safety Of Life At Sea)*, 5th ed. London, UK: International Maritime Organisation, 2009.

[10] Det Norske Veritas, *DNV Statutory Interpretations*. Oslo, Norway: Det Norske Veritas, December 2010.

[11] Germanischer Lloyd Aktiengesellschaft , *Rules for Classification and Construction, Chapter VI Additional Rules and Guidelines, Section 11 Other Operations and Systems, Paragraph 2 Preliminary Guidelines for Safe Return to Port Capability of Passenger Ships*. Hamburg, Germany: Germanischer Lloyd Aktiengesellschaft, 2009.

[12] Giuseppe Buja, Aldo da Rin, Roberto Menis, and Giorgio Sulligoi, "Dependable Design Assessment of Integrated Power Systems for All Electric Ships," in *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS)*, Bologna, 2010, pp. 1-8.

[13] Brad Caldwell, "Shipbuilding Contracts: The Allocation of Risks between Purchaser and Builder," *Western Mariner*, June 2012.

[14] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, 4th ed. Newtown Square, PA, United States of America, 2008. [Online]. *http://pm4id.org/3/1/*

[15] Salvatore Distefano and Antonio Puliafito, "Dynamic Reliability Block Diagrams VS Dynamic Fault Trees," in *Reliability and Maintainability Symposium*, Orlando, FL, 2007, pp. 71-76.

[16] Salvatore Distefano and Antonio Puliafito, "Dependability Modeling and Analysis in Dynamic Systems," in *IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, Long Beach, CA, 2007, pp. 1-8.

[17] IMCA - The International Marine Contractors Association. (2002, April) Guidance on Failure Modes & Effects Analyses. Document M 166. [Online]. *http://www.imca-int.com*

[18] Norbert H Doerry and David H Clayton, "Shipboard Electrical Power Quality of Service," in *IEEE Electric Ship Technologies Symposium*, Philadelphia, PA, 2005, pp. 274-279.

[19] Aaron M Cramer, Scott D Sudhoff, and Edwin L Zivi, "Metric Optimization-Based Design of Systems Subject to Hostile Disruptions," *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS*, vol. 41, no. 5, pp. 989-1000, September 2011.

[20] Erland Jonsson and Søren Asmussen, "A Dependability Measure for Degradable Computing Systems," Chalmers University of Technology, Department of Computer Engineering, Göteborg, Technical Report ISSN 0281-9597, 1992.

[21] Roberto Menis, Aldo da Rin, Andrea Vicenzutti, and Giorgio 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)*, Bologna (I), 2012, pp. 1-6.

[22] The Institute of Electrical and Electronics Engineers, Inc., "IEEE Guide for Synchronous Generator Modeling Practices and Applications in Power System Stability Analyses," IEEE Power Engineering Society, New York, IEEE Standard 1110, 2002.

[23] The Institutio of Electrical and Electronics Engineers, Inc., "IEEE Recommended Practice for Excitation System Models for Power System Stability Studies," IEEE Power Engineering Society, New York, Standard 421.5, 2005.

[24] American National Standard Institution/Institute of Electrical and Electronics Engineers, "Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations," ANSI/IEEE, Washington DC, Standard C37.2, 2008.

[25] Rroberto Menis, Aldo da Rin, Andrea Vicenzutti, and Giorgio Sulligoi, "All Electric Ships Dependable Design Integrated Power System Analysis Using Dynamic Reliability Block Diagram," in *IMarEST - MECSS Proceedings*, Amsterdam, NL, 2013.

[26] Safety and Reliability Society. Safety and Reliability Society. [Online]. *http://www.sars.org.uk/old-site-archive/BOK/Applied%20R&M%20Manual%20for%20Defence%20Systems%20(GR-77)/p4c06.pdf*

[27] Giorgio Sulligoi, Daniele Bosich, Aldo da Rin, and Fabio Tosato, "An Examination of Mutual Influences Between High-Voltage Shore-Connected Ships and Port Earthing Systems During Phase-to-Ground Faults," *IEEE Transactions on Industry Applications*, vol. 48, no. 5, pp. 1731-1738, September/October 2012.

[28] Susan Stanley. (2011) IMC Network. [Online]. *http://www.imcnetworks.com/Assets/DocSupport/WP-MTBF-0311.pdf*

[29] Javier Faulin et al., Eds., *Simulation Methods for Reliability and Availability of Complex Systems*. London, United Kingdom: Springer, 2010. [Online]. *http://marc.bouissou.free.fr/BDMP_DFT_Esrel07.pdf*

[30] Lloyd's Register of Shipping, *Rules and Regulations for the Classification of Ships*. London, United Kingdom, 2006.

[31] American Bureau of Shipping, *Rules for Building and Classing Steel Vessels*. Houston, TX, United States of America, 2011.

Picture Index

Table Index