UNIFIED APPROACH TO VERIFICATION, VALIDATION AND ASSURANCE OF **SINGLE FAULT TOLERANCE** IN DYNAMIC POSITIONING SYSTEMS

JDP01 Rev1

A Joint Development Project (JDP) by OCIMF, IMCA DP Committee & MTS DP Committee

CONTRIBUTING ORGANISATIONS

Information on the contributing organisations can be found at the following links:

- American Bureau of Shipping (ABS)
- Bureau Veritas (BV)
- Det Norske Veritas (DNV) Maritime
- Dynamic Positioning Committee of the Marine Technology Society (MTS DPC)
- International Marine Contractors' Association (IMCA)
- Lloyds Register (LR)
- Oil Companies International Marine Forum (OCIMF)

TERMS OF USE

CONTENTS

FIGURES

TABLES

APPENDICES

HISTORY OF DOCUMENT CHANGES

Rev. No.	Description of changes

SUMMARY

The 'Unified Approach to Verification, Validation and Assurance of Single Fault Tolerance (SFT) in DP Systems' document is comprehensive, detailed and technically focused necessitating DP system domain expertise in its readership and application. This summary section provides a high-level overview for stakeholders who may not be required to be DP experts as they would be ably supported by competent DP SMEs.

Promoting standardisation, transparency and collaboration in the verification, validation and assurance process is a key enabler for successful DP newbuildings and conversions. Visibility into the process allows all stakeholders to participate more effectively and more efficiently. Standardisation of processes and deliverables in an assurable format allows all stakeholders to understand and align on expectations and obligations.

The 'Unified Approach to Verification, Validation and Assurance of Single Fault Tolerance (SFT) in DP Systems' enables the systematic application of guidance published by the DP community to design information for DP systems of Equipment Classes 2 and 3. The process described herein is titled Evidence Based Comprehensive Verification and Validation (EBCV^2). It provides an enhanced basis of confidence in a DP vessel's ability to deliver predictable, incident free DP operations and serves the needs of diverse stakeholders.

The adoption of a comprehensive evidence - based approach to proving SFT in absolute terms represents a discernible shift from processes focused on the relative merits of configurations based on open and closed bus ties. EBCV^2, supplemented by improvements in verification and validation technology and progressive insights, improves the predictable delivery of incident free DP operations and business performance objectives including GHG Emission reductions.

EBCV^2, as described in this document, is well suited to a new build DP vessel or a major conversion. This statement does not preclude selected elements from being applied to existing DP vessels.

Deriving maximum value from this guidance (6.1.2 – 6.1.3)

Maximum value can be derived from the processes described in this document if they are used to:

- Understand which specific elements are to be extracted from published technical guidance into specifications.
- Understand which guidance documents need to be applied to the design information at each point in a newbuilding or major conversion DP vessel project.
- Establish the requirements for analysis and testing to be achieved by those required to comply with them.

Such an approach can lend itself in establishing the basis of confidence that the design is SFT and capable of being verified and validated using the tools currently available to the DP community.

Applicability (6.2)

This guidance is intended to be of use to the entire supply chain for DP new buildings and major conversions.

- **Vessel owners** can use it in the development of specifications for DP system designs that meet their expectations/contractual obligations.
- **Project teams can** use it to understand and monitor verification and validation progress throughout the build cycle and understand which stakeholders have responsibility for deliverables at basic design, detailed design and build stages.
- **Shipyards and integrators** can use it to understand the importance of deliverables, validation testing and the influence of guidance being referenced on the design.

- **Verifiers** Class and DP Failure Mode Effect Analysis (FMEA) providers can use it to deliver verification and validation testing, achieving consistency and standardisation.
- **Original Equipment Manufacturers (OEMs)** can use it understand their part in the verification and validation process of demonstrating SFT and adherence to the redundancy concept.
- **End User Charterer** can use it to develop their functional requirements.

Driving standardisation, consistency and transparency (6.3)

This guidance provides a transparent framework showing the relationships and responsibilities between stakeholders involved in the design, verification, validation and assurance process. Essentially 'who produces what and when' and 'who uses it for what purpose'.

Leveraging guidance and imposing requirements contractually (6.4)

The development of specifications for new buildings and conversions tends to focus on listing relevant codes, standards and industry guidance documents. This is done on the assumption that their inclusion within a contractual framework will ensure that systems are designed and built to comply with the guidance therein. Experience shows that this approach is not as reliable as might be expected. Some attributable reasons are:

- Good intentions at project initiation are compromised by insufficient attention to developing a specification that ensures the design meets expectations.
- Competence is an essential element in a quality verification, validation and assurance process. Lack of competence leads to flaws being overlooked or identified too late.
- Failure to understand the verification and validation burden and ensure the process is adequately resourced with competent personnel who have access to effective tools.

Input for vessel specific familiarisation (1.2)

A byproduct of EBCV^2 is information that can be used to:

- Operationalise output, enhancing comprehension of the DP Redundancy Concept (DPRC), SFT and its dependencies.
- Ensure procedural discipline and facilitate development of vessel specific documents such as A(W)SOGs, DP Checklists, DP Operations Manuals, Sparing Philosophies and vessel familiarisation activities for crew.

Assurance, verification, and validation as part of barrier philosophy (4.4)

EBCV^2 enables the management of other verification, validation and assurance activities. These activities are all barriers to loss of position (LOP). EBCV^2 treats verification, validation and assurance as complementary parts of a holistic process which ensures that the SFT of DP systems is proven in a transparent and assurable form.

EBCV^2 Statement of Assurance (4.5)

- APPENDIX C provides a template for the Statement of Assurance to be completed by the vessel owners or their nominees.
- APPENDIX D provides a completed example based on a fictional newbuild project.

Cross reference to EBCV^2 deliverables (4.5.2)

The EBCV^2 Statement of Assurance provides a cross reference to the key deliverables. The difference between a Statement of Assurance for vessels operating with open bus ties (isolated systems) and those configured to operate with closed bus ties (power transfer) is the number of supporting studies and the extent of the validation testing:

- The supporting studies are referenced from the FMEA & DP System Integration documents.
- The validation test objectives, methods and results are contained in the DP FMEA proving trials.

ABBREVIATIONS

ABS	American Bureau of Shipping
AC	Alternating Current
ASOG	Activity Specific Operating Guidelines
A(W)SOG	Activity (Well) Specific Operating Guidelines
BMS	Battery Management System
BESS	Battery Energy Storage System
BV	Bureau Veritas
CAM/CAMO	Critical Activity Mode/Critical Activity Mode of Operation
C^3EI^2	Commonality, Cross connections External Influences and Interfaces
CTG	Closing the Gap
DC	Direct Current
DP	Dynamic Positioning
DPC	Dynamic Positioning Committee
DNV	Det Norske Veritas
DP MODU	Dynamically Positioned Mobile Offshore Drilling Unit
DPRC	DP Redundancy Concept
DPSI	DP System Integration
$EBCV^2$	Evidence Based Comprehensive Verification and Validation
EMS	Energy Management System
ESD	Emergency Shutdown System
ESS	Energy Storage Systems
F&G	Fire and Gas
FAT	Factory Acceptance Testing
FMEA	Failure Mode and Effects Analysis
GHGER	Greenhouse Gas Emissions Reduction
HEMP	Hazard Effects Management Process
HIL	Hardware in the Loop
HV	High Voltage
IEC	International Electrotechnical Commission
IM	Industrial Mission
IMCA	International Marine Contractors Association
IMO	International Maritime Organization
ISDS	Integrated Software Dependent Systems
ISQM	Integrated Software Quality Management
JDP	Joint Development Project
LIFE	Low Impact Failure Effect
LNG	Liquid Natural Gas
LOP	Loss of Position
LR	Lloyds Register

MBT	Model Based Testing
MDO	Marine Diesel Oil
MOC	Management of Change
MSC	Maritime Safety Committee (of IMO)
MTS	Marine Technology Society
OCIMF	Oil Companies International Marine Forum
OEM	Original Equipment Manufacturer
PMS	Power Management System
RASCI	Responsible, Accountable, Supportive, Consulted and Informed
RCPD	Redundancy Concept Philosophy Document
RDI	Redundancy Design Intent
RP	Recommended Practice
RVT	Redundancy Verification Table
SFPA	Single Failure Propagation Analysis
SFT	Single Fault Tolerant
STPA	System Theoretic Process Analysis
TAM	Task Appropriate Mode
TECHOP	Technical and Operational Guidance (of MTS)
VMS	Vessel Management System
V&V	Verification and Validation
VTO	Vessel Technical Operator
WCF	Worst Case Failure
WCFDI	Worst Case Failure Design Intent
WT	Watertight

GLOSSARY

The following terms are used throughout this document. Additional information on their meaning as used in the context of this document is provided in the table below.

Assurance Process	Assurance Process means **an objective examination of evidence for the purpose of providing an independent, and positive declaration** intended to give confidence. In the context of this document, 'Assurance' is the term used to describe the action of confirming that the verification and validation (V&V) processes have been executed competently. Note: 1. Independent in the context of this document is intended to mean separate from the V&V activities. 2. Use of the word 'independent' in this document is not meant to imply the requirement for a different organisation from that which undertakes an activity (unless explicitly stated as a requirement by the accountable stakeholder or as a contractual obligation). 3. Independent verification is expected to be undertaken by competent personnel with the required domain knowledge and system engineering approach.
Assurable Form	With reference to documentation and other information provided to support the V&V processes. The information is said to be in an 'assurable form' if it is presented in a way that allows the recipient to draw their own conclusions, independently of the information provider. This typically requires the provision of supporting and corroborating evidence.
Bus Tie Circuit Breaker	A bus tie circuit breaker is used to isolate one independent power system from another.
Competence	The combination of appropriate training, current skills, knowledge, and experience so that a person consistently applies them to perform tasks safely and effectively. Competence is a combination of practical and thinking skills, experience, and knowledge. Note: IMCA's definition of competence is used in this document.
Crash Synchronisation	Crash Synchronisation occurs when a generator is connected while its voltage, frequency, and phase are not aligned.
Data Centric	Data Centric information is defined as that which is derived from independently verifiable data (including that gathered and or recorded by digital means). Note: The oft used term 'as expected', does not meet the definition of data centricity.
DP System Integration (DPSI)	DPSI is a process which conforms to the recommended practice produced by a Joint Development Project (JDP) initiated to create a suitable means to address the interaction between software-based controllers within a DP system. The purpose being to identify integration issues between controllers supplied by (the same or different) OEMs that have the potential to defeat the redundancy concept. The JDP was hosted by DNV Maritime and published as a recommended practice RP 0684.

Drift off	Loss of position (LOP) incidents involving drift off are typically characterised by **insufficient thrust** and associated with certain types of power or control system failures (system performance deficits).
Drive off	LOP incidents involving drive off are characterised by **erroneous thrust** (excess or insufficient) and are typically associated with certain types of control system failures and/or position reference systems.

Engineering Basis	An engineering basis is required to establish the range of associated verification and validation (V&V) activities which provide the basis of confidence to conclude that the severity of failure effects does not exceed those predicted (for both benign and aggressive failure modes):
	• Domain knowledge (of how a system works and fails) is an essential element in the process of establishing an engineering basis.
	• Establishing the range of V&V activities will require a clear and unambiguous understanding of not only the local effects but the global effects as they pertain to preventing loss of LOP position and/or heading.
	• An engineering basis cannot be claimed if a clear and unambiguous identification of the attributes of performance, protection and detection, upon which station keeping integrity depends, is not linked to the redundancy concept and transparently documented.
	• An imperative of demonstrating an engineering basis is a comprehensive analysis, validated by testing and supported by substantiating and corroborating data centric evidence in an easily understood and transparent manner.
	  • The analysis and validation testing should encompass hardware and software, system integration, dependencies and influences, etc.
	  • Elements that could impact system functionality and performance should be considered.
	• The documented evidence should clearly identify which attribute of performance, protection and detection is being validated against which specific failure effect.
	  • This will require well documented test objectives.
	  • Test results should be clearly and unambiguously linked to those objectives.
	In the context of this document, the term Engineering Basis means that the V&V activities are based on the objective application of engineering principles and are not solely reliant on preferential or experiential knowledge.
	It is emphasised that a systems engineering approach is to be followed when establishing an engineering basis.

Evidence Based Comprehensive Verification and Validation (EBCV[2])	Effective assurance requires substantiating and corroborating evidence delivered in a data centric and easily understood form which allows the assurance provider to draw their own conclusions, independently of the information provider.

Fault Ride Through	In DP, 'fault ride through' is the property of a power system that allows it to continue in operation without malfunction exceeding the WCFDI after being exposed to the effects of a fault that has been removed from the system by the protection scheme.
Force off	LOP incidents involving force off are characterised by **insufficient thrust** to compensate for the environmental forces that the vessel is being subjected to. It should be noted that typically, no equipment failure is necessary for a vessel to be forced off.
Hardware in the Loop	Hardware-in-the-loop (HIL) simulation is a testing method that integrates actual hardware components into a virtual environment to validate and test control systems. It allows engineers to test algorithms and system interactions before deployment.
Intuitive	Easy to use and understand, typically in reference to Human Machine Interfaces (HMI). In the context of this document the term intuitive is used to mean easily understood without the need for specialist knowledge to enable comprehension and application.
Model Based Testing	Model Based Testing (MBT) is the use of a mathematical model to represent part of the system to be verified and validated. It is typically used to minimise the need for the actual vessel to be used as a test bay for subsystem testing. In the context of this document, it is one of the methods used, in combination with others, to verify the efficacy of the installed protective functions. MBT allows some of the protection system verification to be performed without the need for the power plant (or other system being subject to verification and validation (V&V)) to provide the test stimulus to activate the protection. Note: *a)* For power plants, this is typically achieved by secondary current and voltage injection of mathematically produced waveforms which are analogous to real/realistic fault conditions. *b)* It is emphasised that such MBT is supplemental to the live testing carried out to meet requirements (statutory, class, owners, charterers, etc.).
Parasitic Impedance	Parasitic impedance refers to unwanted resistance, inductance, or capacitance in a circuit or component that affects its performance and is not part of its intended function.
Parametrisation of Protection	The basis for the parameters used to develop protective functions is to be credible and established to cover a comprehensive range of fault conditions (aggressive and benign failures) to which the system being protected is likely to be exposed. MBT may be necessary to supplement other verification and validation V&V activities associated with protective function parameters (processes used for model based testing should be harnessed to parameterise the design of protective functions).

Predictability	Predictability, in the context of this document, is the achievement of a consistent repetition of a state, course of action, behaviour, or the like, making it possible to be known, seen, expected or declared in advance. Predictability can be both qualitative (such as predictable behaviours) and/or quantitative (such as the statistical prediction of results based on data). In the context of this document, it is used to mean that the effects of single failures are known/expected. In other words, they have been correctly predicted by the DP system FMEA and DPSI processes.
Project	A project in the context of this document means the activity of designing, building or converting a DP vessel. It is not intended to mean the work the DP vessel will undertake.
Single Fault Tolerance (of DP systems)	Single Fault Tolerance (SFT) is the property of a DP System, by design, which allows it to continue to maintain position and heading within a defined environmental envelope for long enough to safely terminate the DP operation following the occurrence of any single fault/failure. Notes: a) Applicable failure criteria are defined in IMO MSC 645 & 1580 and by classification society notations. b) Classification society notations may have additional requirement for SFT /fail safe requirements over and above IMO requirements to minimise consequences and make systems more robust. This is a response to the assertion that a relatively crude DP redundancy concept (DPRC), in which many failures give rise to effects equivalent the worst case failure, is adequate so long as there is time & capacity to safely terminate the DP operation. Such failure responses are reasonable for low frequency failure effects but less acceptable for more frequent failures. c) It is acknowledged that not every fault compromises the SFT of a vessel. It is emphasised that operations should not be continued or resumed when the vessel is no longer SFT.
Supply Chain	In the context of this document, the term ‘supply chain’ is used to indicate all those organisations that contribute, in some way, to the performance of an activity or undertaking using a DP vessel. (As examples, vessel designers, original equipment manufacturers (OEM’s)/suppliers, integrators, independent third-party assurance providers, vessel owners, vessel technical operators (VTO’s), service providers (DP system related), engineering, procurement, and construction contractor (EPC) contractors, etc).
Systems Engineering	Systems engineering is a field that combines engineering and management to design, integrate, and manage complex systems. It's an interdisciplinary field that uses **systems thinking** to organise knowledge.
Systems Thinking	Systems thinking is a way of thinking about complex situations by looking at the relationships between parts rather than just the parts themselves. It's a holistic approach to problem solving that can help with innovation and decision making.

Validation	Confirmation by examination (including testing) and provision of objective evidence that the functionality for a specific intended use is fulfilled. Note: This is significantly different from verification which focuses on confirmation by examination (including testing) and provision of objective evidence that specification/requirements have been fulfilled. In a DP context - will the design of DP system fulfil its intended purpose/functional requirements.
Verification	A process that is used to evaluate whether a product, service, or system complies with regulations and/or specifications. The above is a dictionary definition. In a DP context, has the DP system actually been built to the design, rules and redundancy concept?
Vertical/Horizontal Dependencies	The terms **vertical** and **horizontal** dependencies are described in the 'Recommended Practice for DP System Integration DNV 'RP-0684'. The terms were developed to differentiate between the 'horizontal' fault propagation paths that exist between redundant DP equipment groups (those that are the subject of analysis in hardware focused DP system FMEAs) and the hierarchical 'vertical' dependencies that exist between controllers within a DP system that can influence system behaviour in the intact and failed conditions in all redundancy groups. Note: The term 'vertical dependencies' is a relatively new concept that has evolved from progressive insights of DP incidents where lack of transparency, comprehensive analysis and a system engineering approach to validation testing of software functionality, in integrated systems, has been a significant causal and contributory factor. The recommended practise (RP) is intended to provide guidance on identifying and managing the influence of such dependencies.

Glossary entries for the following terms are not provided as they their meaning is widely understood in industry and described in other guidance.	
Aggressive Failure Modes	The terms listed to the left have their usual meanings. Reference can be made to other sources such as the glossary in the OCIMF DP FMEA Assurance Information Paper for formal definitions.
Assurance Document	
Benign Failure Modes	
Common Cause Failure	
Common Mode Failure	
Common Points	
Compensating Provisions	
Comprehensive - Analysis	
Comprehensive and Intuitive Documentation	
Configuration	
Data Centric	
Design to Test	
DP Design Philosophy	
Failure Modes and Effect Analysis	
Hidden Failure	
Interfaces and External Influences	
Redundancy	
Redundancy Design Intent	
Redundancy Verification Table	
Redundant Equipment Group	
Reliability	
Resilience	
Single Failure Propagation Analysis (IEC 60812)	
Supporting and Substantiating Documentation	
Test on Demand	
Verification and Validation Processes	
Vessel Technical Operator	
Worst Case failure	
Worst Case Failure Design Intent	

BIBLIOGRAPHY

The following publications are relevant to the subjects discussed in this document:

International Maritime Organization – IMO

MSC.1/Circ. 1580 Guidelines for vessels and units with dynamic positioning systems (2017)

MSC/Circ. 645 Guidelines for vessels with dynamic positioning systems (1994).

Oil Companies' International Marine Forum

Dynamic Positioning Assurance Framework, Risk-Based guidance (First Edition: 2016)

DP FMEA Assurance Framework Risk-Based guidance (First Edition: 2020).

Classification Societies

ABS *Guidance Note on Failure Mode and Effects Analysis (FMEA) for Classification (2018)*

DNV *RP-E306 Recommended Practice Dynamically Positioned Vessel Design Philosophy Guidelines*

DNV *RP-D102 Recommended practice for FMEA of redundant systems (2012)*

DNV *RP-0591 Redundant Dynamic Positioning Systems with Closed Bus-ties (2024)*

DNV *RP-0684 DP System Integration (2024).*

International Marine Contractors Association – IMCA

M103 Guidelines for the Design and Operation of Dynamically Positioned Vessels – June 2021

M166 Guidance on Failure Modes and Effects Analysis (FMEA) – May 2024

M190 Code of Practice for Developing and Conducting DP Annual Trials Programmes - July 2023

M191 Code of Practice for DP Annual Trials for Mobile Offshore Drilling Units – July 2023

M247 Guidance on Identifying DP System Components and their Failure Modes (Supersedes IMCA 04/04) – Nov 2018

M250 Introduction to Battery Hybrid Systems for DP Vessels – Sept 2020

M259 Guidelines for the management of DP system network storms – Sept 2022.

Marine Technology Society – MTS (Downloadable from MTS DPC Website)

DP Vessel Design Philosophy Guidelines (April 2021)

Technical and Operational Guidance (TECHOPS)

TECHOP (G-03 - Rev1 - Jan21) Continuous Trials for DP MODUs

TECHOP (D-01 - Rev1 - Jan21) Addressing C³EI² to Eliminate Single Point Failures

TECHOP (D-02 - Rev1 - Jan21) FMEA Testing

TECHOP (D-05 - Rev1 - Jan21) FMEA Gap Analysis

TECHOP (D-07 - Rev1 - Jan21) A Method for Proving the Fault Ride-Through Capability of DP Vessels with HV Power Plant

TECHOP (D-08 - Rev1 - Jan21) Software Testing

TECHOP (D-10 - Rev1 - Jan21) DNV RP D102 FMEA Gap Analysis)

TECHOP (D-11 – Rev3 - Mar24) Redundancy Concept Philosophy Document

TECHOP (D-12 - Rev1 - May23) Management of Intermittent Faults in DP Systems

TECHOP (O-02 - Rev1 - Jan21) Annual DP Trials and Gap Analysis

TECHOP (D-14 - Rev1 - Jan25) Guidance on Model Based Testing
to be completed by Q1 2025.

1 INTRODUCTION

1.1 Overview

1.1.1 Dynamic positioning (DP) assurance activities and investigations into loss of position (LOP) incidents have revealed significant opportunities for improvements in the verification and validation (V&V) processes applied to DP systems by bringing focus to the validation of single fault tolerance (SFT) of DP vessels.

1.1.2 Conventional and proven practice of opening the bus ties removes one very obvious fault propagation path, by which the effects of several failure modes can propagate. However, the bus tie is only one of many potential fault propagation paths that are capable of defeating the DP redundancy concept (DPRC). It is imperative that all potential fault propagation pathways are identified, analysed and effectively mitigated.

1.1.3 Bringing focus back to SFT and establishing it as an 'absolute' requirement could potentially address the misconception that the act of opening the bus ties would render the DP system immune to common cause failures. Such misconceptions are believed to have contributed to a lack of comprehensiveness in the V&V activities required to demonstrate that DP vessels operating with open bus ties were actually SFT.

1.1.4 Nothing in this document is intended to replace the need for a comprehensive and robust commissioning and survey process. It is expected that all activities necessary to prove the DP system is installed correctly and operating to design specification will have been carried out prior to the commencement of validation testing performed on the vessel as part of the DP verification, validation and assurance process. It is emphasised that the Evidence Based Comprehensive Verification and Validation (EBCV^2) process described in this document is supplemental to established, effective commissioning processes.

1.1.5 One of the primary purposes of this guidance is to provide a transparent framework that shows the relationships and responsibilities between stakeholders involved in the design, V&V process. Essentially 'who produces what and when' and 'who uses it for what purpose'.

1.2 Input for vessel specific familiarisation

1.2.1 A byproduct of the V&V process is vessel specific design information that may be used to ensure procedural discipline in documents such as Activity (Well) Specific Operating Guidelines (A(W)SOG), DP Checklists, DP Operations Manuals, Vessel Specific Sparing Philosophies, and Vessel Familiarisation activities for new crew.

1.2.2 The combined deliverables produced at the end of the process represent foundational information that can be used to operationalise output and so enhance comprehension of vessel operational teams and shore-based technical support teams on the DPRC, SFT and its dependencies, of the vessel.

1.2.3 Newbuild vessels that complete EBCV^2 should have a lower burden and risk of the following and enhance the robustness of their Management of Change (MOC) processes:

- Remedial modifications to demonstrate SFT.
- Upgrades to achieve SFT.
- Major conversions.

1.3 Development of Technologies and Tools

1.3.1 Progressive insights from LOP events have enabled the development and deployment of technologies and tools capable of providing effective V&V of DP vessels operating in both open and closed bus configurations.

1.3.2 Comprehensive V&V practices capable of demonstrating SFT of DP vessels may provide opportunities to pursue the objectives of enhancing reliability, delivery of predictable incident free DP operations and achieving the objective of reducing greenhouse gas emissions without compromising DP station keeping integrity, i.e. agnostic to bus configuration.

1.3.3 The methods described in this Unified Approach to Verification, Validation and Assurance, guide the user through the application of proven processes and provide means to confirm they are effective and transparent in demonstrating SFT of the DP system's redundancy concept.

1.3.4 Failure Modes and Effects Analysis (FMEA) plays a central role in EBCV^2 along with DP System Integration (DPSI) in proving the SFT of DP systems. The objective of FMEA of redundant systems in a specified unit is to provide objective evidence of required redundancy and fault tolerance.

2 METHODOLOGY

2.1 Introduction to Verification and Validation

2.1.1 The terms V&V are sometimes used interchangeably, but they mean different things:

- Verification is the process of confirming something was built to the design (or rules).
- Validation is the process of determining if something meets its design objectives.

2.1.2 EBCV^2 is a systematic approach to ensuring that a DP system meets its requirements and is fit for purpose. It is based on:

- The application of established industry guidance to basic and detailed design information.
- The use of evidence to support and substantiate the verification, validation and assurance activities that underpin it.

The feedstock to the EBCV^2 process can come from a variety of sources, including but not limited to:

- Industry guidance.
- Codes & recommended practices.
- Design documentation.
- Company requirements documentation.
- Testing results.
- Operational data.
- User feedback and lessons learned.

2.1.3 The methodology for comprehensive V&V in EBCV[2] is expected to be executed in line with the specified guidance. Typical steps for any V&V process include:

a. Define the system requirements: Identify the system's functional requirements clearly and unambiguously. This may be accomplished by generating a functional requirements document that outlines the functionality, performance, and other properties of the system.

It is expected that these functional requirements will drive the development of specifications. Clear specifications, in form of class requirements/notations and contractual requirements, are very important.

b. Develop a V&V plan: Create a V&V plan that details the actions that will be carried out to ensure that the system satisfies its specifications and meets the functional requirements. The following should be included in the plan:

- The specific V&V techniques that will be used.
- The criteria that will be used to determine whether the system meets its requirements.
- The resources that will be needed to perform the V&V activities.

c. Conduct verification activities. Confirm that the system that is delivered meets specifications. Examples of such activities are reviews, walk throughs, inspections, simulations and testing.

Verification activities include class approval of the design, DP system FMEA and DPSI and survey of the vessel during construction. FMEA proving trials will provide some information on the validity of the design and verify the conclusions of the FMEA and DPSI process.

d. Conduct validation activities. The validation activities are performed to ensure that the system delivers the desired functionality and is fit for purpose. These activities can include factory acceptance testing, commissioning testing, system integration testing, customer acceptance testing, operational testing, site acceptance testing, vessel delivery testing, and end-user charter acceptance testing, etc.

The bulk of the validation process should be commenced before construction begins. The validation activities will continue through the project phase until the vessel is delivered and accepted as ready to be deployed in operation.

e. The use of supporting studies, mathematical models and model-based testing (MBT), at factory acceptance testing (FAT) and proving trials, can help derisk the potential for the DP system design failing to meet its objectives and contractual obligations.

f. Analyse the results of the V&V activities. Identify any areas where the system does not meet its specifications and functional requirements. Corrective action should be taken as required and subjected to further validation to demonstrate efficacy of remediation.

g. Document the results. Document should support the system's acceptance per established criteria.

2.1.4 The applicable technical guidance, design documentation and deliverables will vary depending on the system but the EBCV[2] process remains largely the same.

Additional considerations for approaching V&V methodology:

- Tailored to the specific system being developed.
- Flexible enough to accommodate changes to the system requirements.

- Cost-effective.
- Repeatable and scalable.
- Achieves the intent of transparency.
- Facilitate effective assurance for all stakeholders.

2.1.5 Central to the success of EBCV^2 is the concept of an engineering basis for design decisions supported by comprehensive substantiating and corroborating evidence delivered in a data centric and easily used form.

2.2 Evidence Based Comprehensive Verification and Validation as a framework

2.2.1 A comprehensive DP Assurance process is one that considers Design, Operations, People and the Processes that bind them together. This document focuses on 'Design' given that design has the predominant influence in the development phase of a DP system and its redundancy concept. It is important that the Industrial Mission (IM) is considered from the outset and any conflicts between requirements for IM and DP are resolved. See Section 3 for further EBCV^2 information.

2.2.2 EBCV^2 is a framework intended to:

- Provide a credible basis for confidence in the fault tolerance of a DP system.
- Control and monitor the development and delivery of a fault tolerant DP system.
- Drive transparency and produce deliverables in a manner that facilitates assurance.
- Encourage and harness participation of all pertinent members of the supply chain to meet the objectives of a diverse range of stakeholders.

2.2.3 The DP community has, over the years, developed a wealth of technical and operations guidance that can be applied at various points in the DP system's design and testing phase to ensure that SFT is achieved, demonstrated, and documented. This document indicates when and how the existing guidance and tools should be applied. It is not intended to provide technical guidance within this document, but to point the user to relevant existing technical guidance, from a wide range of sources, which is appropriate at each stage of the process.

2.2.4 The EBCV^2 flowchart in Appendix A provides a detailed overview of EBCV^2. The process can be understood by review of the simplified, (condensed) chart in Figure 2-1 below.

It is emphasised that the flow chart for EBCV^2 is not intended to communicate that all activities are sequential. Several of the activities are carried out concurrently throughout all phases of the project.

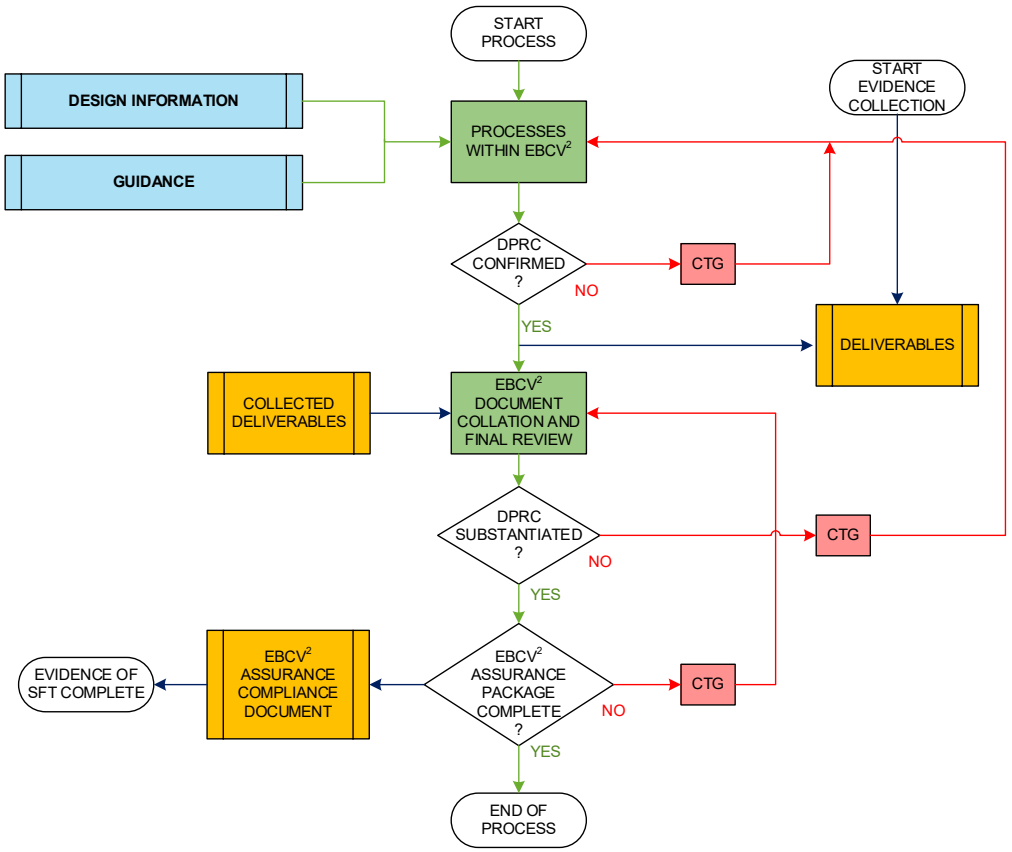

Figure 2-1 Simplified Embedded Guidance in Evidence Based Comprehensive Verification and Validation Process

2.2.5 There are four basic elements to the EBCV² flowchart colour coded Red, Blue Green and Yellow:

- The **Green** elements represent the processes. These processes are the familiar V&V activities such as DP system FMEA and FMEA proving trials etc. These are lumped together as a single process in Figure 2-1 for simplicity but specified individually in the flowchart in APPENDIX A.
- The **Blue** elements are the feedstock to the processes and comprise the detailed design information and the guidance to be used in each step of the process.
- The **Yellow** elements represent the deliverable or output from each process which are collected to form the EBCV² assurance documentation package that contains the proof of the SFT of the DP System.
- The Red elements represent the review process and corrective actions which may be required at each stage. At the end of each process are decision points where the requirement is to confirm the DP systems' redundancy concept has not been compromised. This is determined by the findings from the process that has just been executed but also by quality checks on the process itself such as the various FMEA and proving trials gap analysis tools. EBCV² does not proceed to the next process until identified gaps have been closed.

2.3 Division of Processes

2.3.1 EBCV^2 consists of several process elements. Most of these are recognisable as existing elements of any DP V&V process:

- Redundancy Concept Philosophy Document (RCPD).
- DP System FMEA (hardware related).
- DPSI (software/functionality related).
- DP FMEA proving trials including tests generated by supporting studies and activities such as live short circuit and ground fault testing and MBT.
- EBCV^2 is the designation given to the overall verification, validation and assurance process but is also used to describe the activity of collecting all the evidence indicating that the process has been followed.

Refer to DNV 'RP-0684'.

2.3.2 RCPD, DP System FMEA and DPSI are analytical in nature. DP FMEA proving trials is the repository for all the validation testing although some of this testing may be performed at other times and test opportunities, where appropriate.

2.4 Redundancy Concept Philosophy Document

2.4.1 Development of a DP Redundancy Concept Philosophy Document (RCPD) is the first and most important of all the processes in EBCV^2. Errors in developing an RCPD may have undesirable effects which propagate through to the final design. The MTS TECHOP (D-11-Rev.3-March 24) 'Redundancy Concept Philosophy Document' contains guidance on how to create and evaluate a DP redundancy concept. A valid RCPD is an important deliverable which then becomes an input to all the subsequent processes such as DP FMEA and Proving Trials. It also sets the acceptance criteria for these processes.

The guidance in MTS TECHOP D-11 is designed to deliver comprehensive RCPD which could serve the needs of all the diverse stakeholders involved in the delivery acceptance and operation of a DP vessel. It is acknowledged that the classification society may not stipulate such comprehensiveness for compliance with their rules.

2.4.2 When developing an RCPD, reference should be made to technical guidance such as the MTS DP Vessel Design Philosophy Guidelines, IMCA M103, IMO MSC/Circ. 645 or IMO MSC.1/Circ. 1580. The MTS TECHOP (D-01 - Rev1 - Jan21) on 'Commonality, Cross Connections, External Interfaces, and Influences' (C^{3}EI^2) can be used to fully understand the consequences of design choices made in the RCPD. This TECHOP provides many real-life examples of the effects of unmitigated fault propagation so that designers and OEMs can decide whether the benefits these common points introduce are worth the risk and additional verification burden they impose. Should the common point be retained, the information in C^{3}EI^2 can also be used to understand the type of protective functions and other performance attributes that are needed to mitigate its failure effects. This information confirms the importance of designing and testing those protective functions and other compensating provisions upon which the DPRC relies for its SFT.

2.4.3 The RCPD should be issued along with the basic design information to Classification Societies, shipyards, OEMs, integrators and third-party assurance providers involved in the development of the detailed design. It may accompany invitations to tender for the delivery of the vessel.

2.4.4 It is important that all those involved in the development of the DP System (i.e. the entire supply chain) have a sound understanding of the DPRC and the compensating provisions, protective functions, and performance attributes upon which it relies for its SFT. It is incumbent on these stakeholders to ensure that there is nothing within their scope of supply/deliverables that would compromise or violate the redundancy concept.

2.4.5 Low Impact Failure Effect (LIFE) concept is a form of DPRC focused on minimising the number of failure modes that can lead to the worst case failure in a vessel operating with its bus ties closed. APPENDIX E provides a list of functional and verification requirements that can assist in developing a specification for a vessel designed to the LIFE concept.

2.5 Dynamic Positioning Failure Mode Effect Analysis

2.5.1 The next process in EBCV[2] is the DP System FMEA. This process takes the RCPD and the relevant class rules as acceptance criteria and analyses the detailed design to determine whether the DP System fails in a manner that ensures the desired post failure DP capability remains available after an occurrence of the worst case failure. The FMEA will typically identify opportunities for improvement and/or gap closure pathways to establish a basis of confidence in DP station keeping integrity by demonstrating SFT and providing data centric elements in an assurable form.

2.5.2 There are numerous industry guidance documents on the subject of executing and evaluating DP System FMEA including:

- ABS Failure Mode and Effects Analysis (FMEA) for Classification.
- DNV FMEA of Redundant Systems, RP-D102.
- IMCA M166, Guidance on Failure Modes and Effects Analyses (FMEAs).
- MTS DP FMEA Gap Analysis Tool (can be used as guidance for development as well as verification).
- OCIMF DP FMEA Assurance Framework Risk-Based Guidance.

Notes:

a. The methods developed from the theory in DNV ‘RP-D102’ FMEA of Redundant System’ are leveraged in the development of the OCIMF ‘DP FMEA Assurance Framework Risk-Based Guidance’. These graphical methods are highly recommended and include Redundancy Verification Tables (RVT), colour coded sketches and Single Failure Propagation Analysis (SFPA) tables.

b. The MTS Gap Analysis tools are intended for use primarily by DP FMEA practitioners. The OCIMF ‘DP FMEA Assurance Framework Risk-Based Guidance’ is intended for use by DP assurance providers.

c. Classification society rules for DP notations do not usually specify an intact or post failure DP capability only that the defined post failure DP capability be maintained after the worst case single failure. However, it may be in the vessel owner’s interest to adopt design principles such as the LIFE concept that ensure that failure effects have as little effect on station keeping capability as possible and that higher probability failures do not lead to an occurrence of the worst case failure. Non-critical redundancy is often specified for this purpose. Information on the LIFE concept can be found in the MTS ‘DP Vessel Design Philosophy Guidelines’.

2.5.3 The DP System FMEA becomes the second major deliverable to form part of EBCV[2]. The DPSI process should start in parallel with the FMEA.

Notes:

a. Non-critical redundancy is applied to a DPRC to improve reliability and reduce the severity of failure effects, usually to maximise the availability of the vessel to carry out its IM while being SFT. Failure of non-critical elements of redundancy has no effect on SFT or post failure capability.

b. It is important to understand the limitations of the DP FMEA process:
   - FMEA, as it is traditionally practiced by the DP community, is essentially a 'book-keeping' exercise in which undesirable/unacceptable failure effects are addressed by compensating provisions.
   - It is not capable, nor intended to be capable, of fully confirming the efficacy of the compensating provisions or other performance attributes upon which SFT depends.
   - Proving the efficacy of compensating provisions and performance is the role of Supporting Engineering Studies and associated validation testing. See section 2.6.

c. It is also to be understood that the DP System FMEA is a living document and should be updated in line with industry guidance. This drives the EBCV[2] process to be applicable throughout the vessel lifecycle.

2.6 Supporting Engineering Studies

2.6.1 Supporting studies are an input to the DP FMEA process and not identified as a process in their own right within EBCV[2]. Exactly which supporting studies are required to support the DP System FMEA depends on the detailed design, the presence of common points, cross connections, and the configuration of the power system. In particular, more supporting studies are required for designs that employ battery energy storage systems (BESS), alternate fuels and/or power transfer between redundant DP equipment groups as a means to improve power plant efficiency and thus reduce greenhouse gas emissions. Typical supporting studies for vessels employing power transfer, (example closed bus ties or cross-feeding mode, commonality introduced to achieve specific functionality, etc.) include:

- Protection co-ordination study:
  - Comprehensive, including all functions which can impact DP
  - To be proven by simulation, live testing and MBT.
- Power system computer simulation modelling the response to fault conditions.
- Harmonic distortion in all relevant operating configurations including post worst case failure.
- Power system stability
  - Load acceptance & rejection
  - Crash synchronisation
  - Analysis and computer simulations
- Load balance in all relevant operating configurations, including post worst-case failure.

In addition to the above, additional safety studies as pertinent may be required. For example, arc flash study and protective grounding study.

2.7 Dynamic Positioning System Integration

2.7.1 DPSI methodology was developed around the same time as the industry initiative focusing on SFT. DPSI shares common roots with established methods such as System Theoretic Process Analysis (STPA) through the discipline of System Theory. DPSI is the subject of the Recommend Practice (RP-0684) developed by DNV as the outcome of a JDP intended to identify vulnerabilities related to dependencies which exist between software-based controllers within the same redundant DP equipment group and shared across redundancy groups. The concept of Horizontal and Vertical Dependencies was developed to help visualise the DPSI process as shown in Figure 2-2.

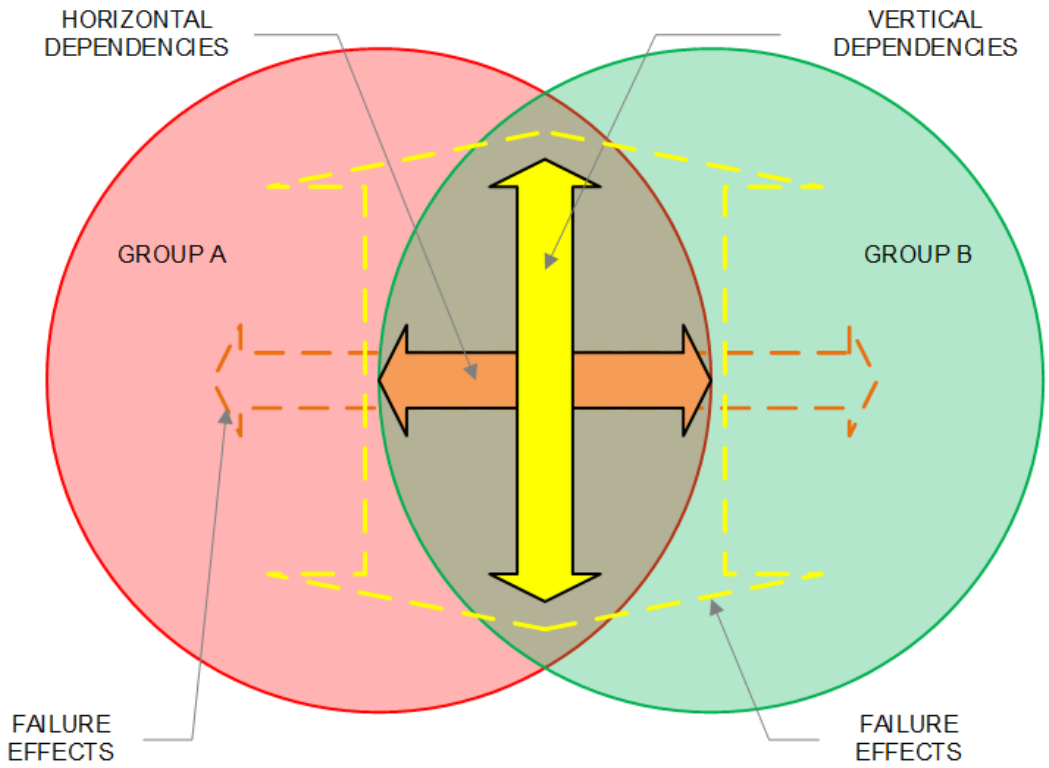

Figure 2-2 DP System Integration – Horizontal and Vertical Dependencies

2.7.2 Dependencies are categorised as follows:

- Horizontal dependencies are those that exist between redundant DP equipment groups. They are typically physical links. For example, cross connections in control power and data communication networks and are the subject of DP System FMEA.
- Vertical dependencies are those logical links and physical links, that exist between controllers within each redundant DP equipment group. These are the subject of analysis by DPSI. It is important to understand that the dependencies may be the same dependencies in both groups and therefore not independent between redundant groups.

  The dependencies are typically contained with the intersection of redundancy groups (A & B in the case of a two-way split) but their failure effects are capable of affecting the performance of the entire system. Physical links are intuitively obvious, and draw attention, but logical links are not. Conscious effort and discipline are thus required to probe for such logical links.

2.7.3 Fault tolerance in DP Systems is achieved by the provision of redundant systems. Most subsystems are divided along the lines of the split in the DPRC and rely on active redundancy to ensure station keeping continues uninterrupted following failure. That is to say, all redundant elements are in operation and the surviving units simply assume additional load when one redundant equipment group fails. Alternatively, redundant control systems often rely on standby redundancy and operate in a duty – standby mode in which there is one controller in overall control, until the duty controller fails, and the standby controller takes over. Thus, there is a single controller in command of the DP System at any one time. Therefore, the split that is established in the physical system does not exist to the same extent in the logical system. Thus, faults and design flaws in the control system will affect all redundant groups. The DPSI process makes logical links and control authority visible so that their failure effects can be evaluated.

2.7.4 DPSI focuses on the logical links between controllers responsible for functions such as:

- Power Management System (PMS), Energy Management System (EMS), Vessel Management Systems (VMS).
- Thruster control systems.
- Switchboard protection and control,
- Safety systems, etc.

The term ‘controller’ is not necessarily synonymous with a computer or physical device. Controllers are logical devices. A computer may have several controllers.

2.7.5 Typical vertical dependencies are load-shedding, examples are; thruster phase back by PMS, thruster command and feedback signals, emergency shutdown (ESD) from centralised ESD or firefighting systems.

2.7.6 The DPSI process is based on requesting OEMs involved in the design of the DP System, to provide information on the links between their system and other parts of the DP System and, in particular, what authority their controllers exercise.

2.7.7 Controller Authority is categorised as:

- External Input Authority - This describes the actions/instructions a particular controller will accept from other controllers.
- Autonomy Authority - This describes what actions the controller can apply to its own operation, for example, shutdown on internal diagnostic failure.
- External Output Authority - This describes the commands/actions a particular controller can apply to other controllers.

2.7.8 OEMs will identify these authorities in standard prescribed templates along with supplementary information which is collated and analysed. It is logical that the DP System FMEA providers perform the evaluation of the information provided by the OEMs as they have an overview of the DP system’s redundancy concept and communicate the outcome to the pertinent stakeholders. The findings of the DPSI process will be integrated into the DP System FMEA. A validation testing procedure may be generated and incorporated within the DP FMEA proving trials.

Notes:

a. A formal DPSI process can be included in specifications and contracts by reference to DNV ‘RP-0684’ which is publicly available.

b. To oversee the integration of the DPSI process a responsible person or organisation, typically the shipyard, is defined.

c. Significant participation from OEMs is required which is more readily achieved during the vessel's construction phase or major upgrades.

d. Although the process of evaluating the information provided and integrating the findings into the FMEA lies with the FMEA provider there is an expectation that OEMs will have considered the consequences of controller authority with respect to their own interfaces. DPSI meetings form an important part of this process. These meeting are held to reveal, understand and resolve potential controller authority conflicts.

e. Although DPSI was developed to fill an identified gap, nothing in this document precludes the use of hardware in the loop (HIL), Integrated Software Dependent Systems (ISDS) and International Standard on Quality Management (ISQM) and their equivalents. There are likely to be project applications where these processes may be more suitable than the simplified DPSI approach.

f. Projects electing to substitute HIL, ISQM or ISDS for DPSI should ensure that the conclusions of these processes are elevated and integrated into the DP System FMEA.

g. Although some FMEAs do provide information on system integration, in the form of functionality provided by software, currently used processes typically do not achieve the level of rigour and formality required by DPSI.

2.8 Dynamic Positioning Failure Mode Effect Analysis Proving Trials

2.8.1 This process is the repository for a large part of the validation testing. The DP FMEA provider is responsible for preparing a trials program that will exercise all the elements of performance, protection, and detection upon which the DP System relies for its SFT. In practice, the detailed elements of some tests may be prepared by other suitably qualified parties, such as the OEMs, and incorporated into the test program. This may include testing to prove the effects of controller actions and failures in logical links identified as part of the DPSI process.

Using the FMEA proving trials more comprehensively, as a repository for other validation testing, may require additional administrative processes and resources.

2.8.2 DP FMEA proving trials may be subdivided, more extensively, into those elements of testing that can be performed on shore, by simulation including MBT and by live testing on full auto DP. The rational and acceptance criteria, including methodology, should be clearly documented and signed off by all accountable parties.

2.8.3 The FMEA proving trials should continue to be the central repository where all test procedures and results are collated and analysed for conformance to the requirements of the DPRC.

2.8.4 Guidance on the content and execution of DP FMEA proving trials can be found in numerous industry resources including IMCA M166 Guidance on Failure Modes and Effects Analysis (FMEA) – May 2024, MTS DP Design Philosophy document and MTS DP FMEA testing TECHOP (D-02 - Rev1 - Jan21).

The above referenced guidance documents have not incorporated progressive insights and evolution of test methodologies such as Model Based Testing.

2.9 Recommended Guidance

2.9.1 Each of the Green processes in the EBCV^2 flowchart is supported by design information and recommended guidance. The list of recommended guidance and supporting studies, appropriate to each subsystem, at each stage, is provided in the EBCV^2 flowchart and in Table 2-1 below.

Table 2-1 Embedded Guidance in Evidence Based Comprehensive Verification and Validation

Colour Key	All concepts/configurations	Closed Bus/Power Transfer	Energy Storage/Hybrid

Key Process	Guidance	Design Information	Supporting studies
	Relevant guidance for the design of DP system and the execution of verification, validation and assurance activities	Detailed design information on all systems that constitute the DP System or can exert influence over it	All engineering studies necessary to establish performance criteria and the efficacy of protective functions
RCPD	RCPD TECHOP MTS D-11	Basic design, vessel specification IM equipment specification.	RCDP Report Preliminary DP capability plots for various scenarios including WCFDI.
	IMCA M103		
	MTS DP Design Philosophy Guidelines		
	IMO MSC/Circ. 645 and MSC.1/Circ. 1580		
	Specified functional requirements, if any.	Typically embedded as a contractual obligation	
DP FMEA	**DP FMEA**		
	See guidance on the execution of DP System FMEAs in M166, M247 TECHOPs D02 & D05 (MTS Gap Tools) – System to be analysed would include those listed in the next column	RCPD report on the redundancy concept.	Seven Pillars Comparator – Available from MTS DPC website and described in RCPD TECHOP Load Balance Capability Plots Harmonics in all operating modes.
	Vendor FMEAs DP/PMS/ESD	Engines & Marine Aux Systems	
	DPSI Templates	Power Distribution Systems	
	ABS FMEA Guide	Power Generation	
	DNV - RP D102	Power Management	
	IMCA M166	Energy Management (BESS)	Time to Terminate (BESS)
	IMCA M247	Data Networks	All Open Bus Studies Coordination Studies Model Based Testing Transient Stability Short Circuit Withstand Ride Through Analysis
	OCIMF DP FMEA Assurance Framework	Thrusters	
	IMCA M250 Hybrid	DP Control Systems	
	DNV RP-0591	Safety Systems	
		IM Equipment	
		A60 WT Segregation	
		Safety Systems	
		Firefighting Systems	DP Control System FMEA VMS/PMS/EMS FMEA ESD FMEA Vessel specific DP consequence analysis functional description.

Key Process	Guidance	Design Information	Supporting studies
	Relevant guidance for the design of DP system and the execution of verification, validation and assurance activities	Detailed design information on all systems that constitute the DP System or can exert influence over it	All engineering studies necessary to establish performance criteria and the efficacy of protective functions
DPSI	**DPSI**		
	DPSI Templates	DP Control System	Output from OEM participation in DPSI – Completed templates, etc.
	RP on DPSI DNV RP- 0684	PMS/EMS/VMS/BESS/BMS	
		Thruster Control	
		ESD	
		F&G	
Validation Testing	**Validation Testing**		
	MTS TECHOP (D-02) FMEA Testing	All design information used for DP FMEA and DPSI	DP FMEA report.
	IMCA M190/191 Note: 190 & 191 are for annual trials but contain useful general guidance on testing	None	All supporting studies generated for DP FMEA.
			Computer simulation of power plant
	IMCA M259 Management of Network Storms	Data communication networks	Netstorm Test Report (may be in FMEA Proving Trials)
	IMCA TECHOP (D-07 - Rev1 - Jan21) A Method for Proving the Fault Ride-Through Capability of DP Vessels with HV Power Plant.	None	Protection coordination study for validation by MBT & live short circuit testing.
EBCV^2	**EBCV^2**		
	This document	None	All EBCV^2 Deliverables.

2.10 Evidence Based Comprehensive Verification and Validation Package

2.10.1 The final step in the EBCV^2 assurance process is to collate all the deliverables from the other process elements including:

- The results of the gap analysis.
- Gap closure remediation which demonstrates the processes were executed in line with industry guidance.

2.10.2 The organisation responsible for oversight of the EBCV^2 process will:

- Complete the DP system assurance checklist in APPENDIX C.
- Assemble the assurance package documentation.
- Make it available for review by stakeholders in the distribution matrix.

2.10.3 Section 4 provides more detail on the EBCV^2 assurance process and its deliverables.

3 EVIDENCE BASED COMPREHENSIVE VERIFICATION AND VALIDATION

3.1 Process

3.1.1 The EBCV^2 process as outlined in section 2 is intended to provide a basis of confidence by confirming that critical V&V processes, and their deliverables, are executed competently.

3.2 Content

3.2.1 The main deliverable from the overall EBCV^2 process is a 'Statement of DP System Assurance' issued by the organisation responsible for EBCV^2. APPENDIX C shows a typical EBCV^2 Statement of DP System Assurance which lists the documents associated with the main process:

- RCPD.
- DP System FMEA including references to all supporting studies.
- DPSI findings and conclusions, as part of FMEA.
- DP FMEA proving trials – collating all validation testing.

3.2.2 The EBCV^2 statement of DP system assurance is intended to facilitate additional assurance activities by stakeholders, confirming that each of these deliverables was evaluated to verify the extent to which it was:

- Competently executed, in line with current industry guidelines and,
- Ensuring conformance with the requirements of the DPRC, necessary remedial work was implemented and subject to validation testing.

3.2.3 The activities described in the bullets above applied at each decision point on the main spine of the EBCV^2 flowchart. See APPENDIX A.

3.3 Responsibility

3.3.1 Oversight of EBCV^2 is assigned at project inception and the assigned organisation is accountable for ensuring that the requirements of EBCV^2 are implemented in a transparent and assurable form. The assigned organisation is also accountable for:

- Confirming the required technical documentation and analyses are generated and delivered to users.
- Final production of the EBCV^2 assurance table and statement.

3.3.2 It is anticipated that suitable organisations accountable/responsible to provide oversight of the EBCV^2 process would include the vessel owner's technical team or third-party verifiers nominated by the vessel owner such as a DP consultancy or the DP FMEA provider.

Developing the deliverables required for EBCV^2 is the responsibility of the organisations carrying out the verification, validation, and assurance activities with support from suppliers/OEMs. The organisation accountable for administering EBCV^2 is responsible for liaising with the developers of the deliverables to ensure they are produced in a timely manner for use by stakeholders who need them. If the organisation providing the FMEA is expected to be accountable in addition to being responsible for EBCV^2, such an expectation should be clearly stipulated in the defined scope of work.

3.3.3 APPENDIX B provides a table, similar to a Responsible, Accountable, Supportive, Consulted and Informed (RASCI) chart, indicating those stakeholders that are responsible for producing certain deliverables and those stakeholders that require that information to perform verification, validation, and assurance activities.

3.4 Influence of Configuration

3.4.1 At a fundamental level, there are two reasons that any DP power plant can blackout, or exhibit failure effects > Worst Case Failure Design Intent (WCFDI), as the result of a single failure:

- The DP System is in good order, but the design is not SFT.
- The DP System design is SFT, but the system is not in good order.

The former is a design V&V issue to be remedied by implementation of the pertinent design guidance and effective V&V. The latter is an assurance and periodic reverification issue to be addressed by improved periodic reverification and when warranted, enhanced redundancy by design.

Progressive insights from incidents have revealed the existence of DP Systems that were neither fault tolerant nor in good order.

3.4.2 The current practice, based on guidance from many industry bodies, in some cases imposed by regulators and/or by requirements from end user charterers, is to conduct critical DP operations in open bus configuration. This position is a pragmatic recognition of the fact that the design, verification, validation and periodic reverification of much of the DP fleet is not yet at a point where equivalent power system integrity in closed bus configurations can be demonstrated as required by IMO MSC/Circ. 645 and MSC.1/Circ. 1580 without conscious and considerable effort.

3.4.3 Neither configuration is without failure scenarios that can lead to LOP if not properly managed. Closed bus power systems require additional compensating provisions as shown by the fault tree in Figure 3-1.

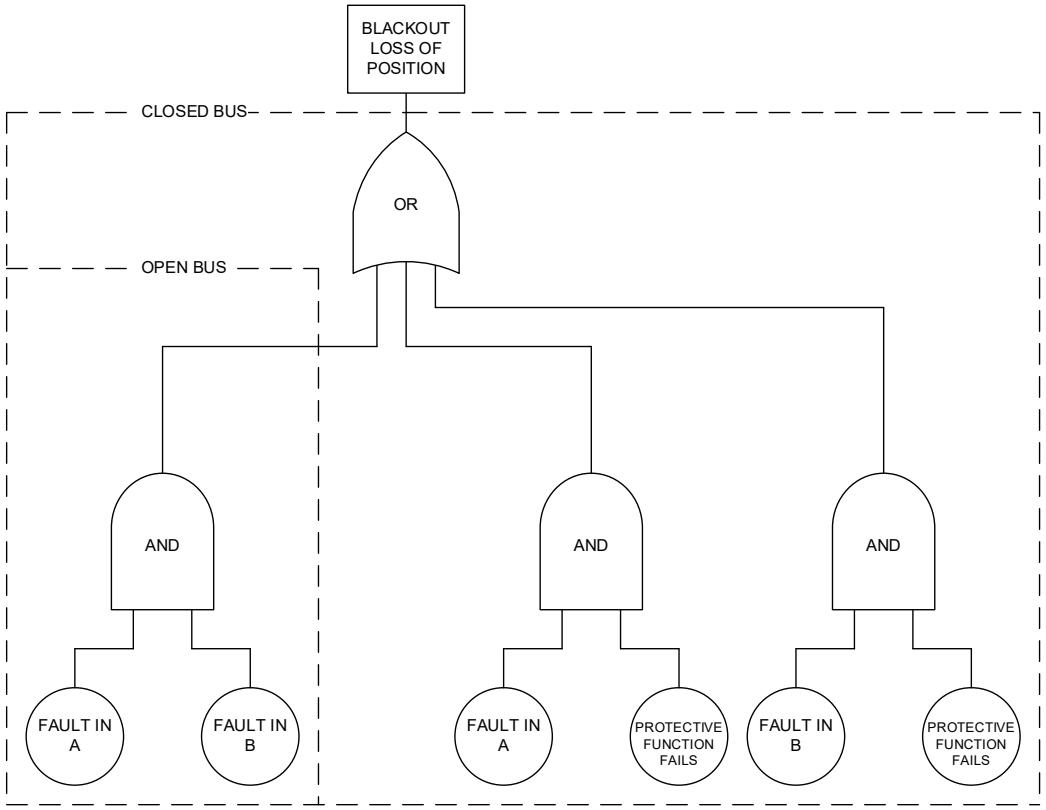

Figure 3-1 Fault Tree for Open and Closed Bus Power Systems

3.4.4 In a DP power plant that is designed to be fully fault tolerant, LOP can occur because of hidden failures in each configuration as follows:

- Open Bus: A fault occurs in Redundant DP group A when there is a hidden failure in Redundant DP Group B. Typically, B is unable to accept the load transfer when group A fails, and a cascade failure ensues.
- Closed Bus: The same failure scenario exists as for open bus but there are two other paths to the top event:
  - There is a fault in A that is not prevented from propagating to B by a faulty protective function.
  - There is a fault in B that is not prevented from propagating to A by a faulty protective function.

3.4.5 In a validated fault tolerant DP System design, the relative station keeping integrity of open bus and closed bus depends on:

- The probability of occurrence of a fault in one redundancy group combined with the probability that a hidden failure exists in the other redundancy group for open bus.
- The probability of occurrence of a fault in one redundancy group combined with the probability that a hidden failure exists either in the other redundancy group or in a protective function for closed bus.

Notes:

a. Hidden failures can manifest themselves as a performance degradation/limitation or failure of an on-demand function.

b. It is a central principle and accepted approach of risk management in DP operations that the probability of experiencing a second truly independent failure in the time it takes to suspend DP operations is low enough to be neglected.

3.4.6 The DP community records incident data in a manner that is well suited to deriving lessons learned but less well suited to the provision of statistical insight. The largest publicly accessible data base is the IMCA annual DP events report, published since 2000. This database has numerous examples of DP vessels losing position and heading in both configurations.

3.4.7 As a general principle, for any activity, the practice of assigning a low probability of occurrence to an event based solely on the frequency of similar historic events should be avoided.

3.4.8 Assigning low probability may only be justifiable when it has been confirmed that the factors that ensured this type of event did not occur frequently in the past, will be present when the same activity is undertaken in the future.

3.4.9 In the latest industry guidance and classification society rules for closed bus DP notations, the process of demonstrating equivalent integrity is focused on evaluating and mitigating:

- The risk that the design is not SFT. This is addressed by more extensive and stringent requirements for V&V including those in EBCV[2]. By new designs with reduced potential to propagate faults and improved design guidance and philosophy.
- The risk of a hidden failure of a protective function. This is addressed by requirements for fully redundant protection schemes to reduce the probability of there being no protection when a fault occurs (in defined DP notations). Other means include improvements in methods for initial verification and periodic reverification, such as:
  - MBT
  - Monitoring of protective functions
  - Build-to-test philosophies and functionalities
  - Healthy-to-operate philosophies and functionalities.
- The risk of a hidden performance limitation. This is addressed by annual DP trials, improved condition monitoring, data logging and self-diagnostics. It is also addressed by the DP assurance processes of Vessel Technical Operators (VTO's) and end-user charterers' requirements.

3.4.10 Ultimately, each DP System should be proven to be SFT in all its defined and intended operating configurations. Only when station keeping integrity has been proven, in absolute terms, is it valid to compare the station keeping integrity in different configurations. Comparison between configurations should only be made when the risks are properly understood and managed.

3.4.11 A validated and documented, as per EBCV², open bus configuration will generally have lower reliance on 'on demand' functions but greater reliance on performance attributes. These factors may influence the decision to adopt an open bus configuration for a specific mission risk profile.

3.4.12 Implementing the guidance in this document and focusing on demonstrating SFT and EBCV[2] is expected to enhance the predictable delivery of incident free DP operations in all configurations and reduce the integrity gap, both perceived and/or real, between open and closed bus configurations. This integrity gap exists in practice, not because of fundamental differences in the way in which SFT is achieved, but rather how it is proven by V&V.

3.4.13 It is acknowledged that DP vessels designed and accepted for operations in closed bus configurations should have robust processes in place to ensure nothing will preclude them from reverting to an open bus configuration if anomalous or unpredicted behaviours are experienced when operating in a closed bus configuration. Processes should be in place to ensure that this is clearly communicated to vessel operational teams for example, in standing orders, bus directives, crew training, familiarisation and drills, etc.

3.4.14 It is emphasised that the basis of confidence for operating in either configuration should be verified and validated following the principles of EBCV[2].

Any DP vessel of equipment class 2 or 3 should only be considered to be SFT when it has been comprehensively proven to be so. It is essential that the V&V process is competently executed for both open and closed bus configurations.

The fundamental process required is agnostic to configuration. It is emphasised that the additional V&V burden, philosophies and functionalities initial and periodic, associated with proving SFT in DP vessels incorporating power transfer between redundancy groups in their design should not be underestimated.

3.4.15 While the focus should always be on not creating vulnerabilities in the first place, it is typically in the area of validation testing and proving the efficacy of protective functions where V&V fails to identify vulnerabilities.

This philosophy can be summarised as:

- Avoid unnecessary vulnerabilities associated with fault propagation paths. Especially those which do not provide any real benefits and/or cannot be verified and validated.
- Manage and mitigate those vulnerabilities that can be accepted because they bring essential benefits or are necessary to realise other objectives.

3.5 Addressing Commonality Cross Connections External Influences and Interfaces (C^3EI^2)

3.5.1 The subject of this guidance is effective V&V. In particular, the V&V of SFT in DP Systems. All stakeholders across the supply chain have a responsibility for ensuring the systems they deliver meet requirements for single fault tolerance. Classification societies, DP FMEA providers and shipyards, as integrators, have specific responsibility for verifying and documenting that designs meet the relevant rule requirements.

3.5.2 This section discusses:

- The V&V of SFT in DP systems.
- The advancement of V&V tools for complex power and control systems.
- The need for designs that are compatible with these V&V tools.
- The benefits of minimising fault propagation paths and accepting common points and cross connections only when they provide specific benefits, and their failure effects are comprehensively mitigated.

3.5.3 Significant advances in V&V tools have been made to address some of the challenges posed by increasingly complex power and control systems. As examples:

- Mathematical modelling and live short circuit and ground fault testing are now mainstream activities for DP class 3 vessel operating with closed bus ties, when the appropriate notation and qualifier is selected. They can also be specified on DP class 2 designs.
- Model based testing of power system protection fills a gap between live testing and mathematical modelling in which real protection hardware can be tested without using the power plant as a test set.
- Semi-automatic means for testing the effects of fault propagation in control power cross connections. One such example has the ability to automatically apply a range of simulated, but realistic, faults and record their effects.
- DPSI provides a pragmatic risk reduction measure for software dependent systems.
- Gap analysis tools provide semi-automatic methods for cross checking DP FMEAs, proving trials and other key DP documentation.
- The OCIMF DP FMEA assurance framework and DNV ‘RP-D102’ provide efficient means of analysing a DPRC and identifying potential vulnerabilities.

Examples of requirements for a live short circuit and ground test can be found in the ABS EHS-E notations, DNV Dynpos series of notations and associated qualifiers. Guidance on how to perform live short circuit testing on any high voltage (HV) power system can be found in MTS TECHOP (D-07 - Rev1 - Jan21), ‘A Method for Proving the Fault Ride-Through Capability of DP Vessels With HV Power Plant’, January 2021.

3.5.4 Power transfer between redundant elements of a DP power plant is one example of an application in which increased levels of commonality are accepted in order to achieve objectives such as improved efficiency, reduced maintenance costs and greenhouse gas emission reduction (GHGER).

3.5.5 Power transfer may take the form of:

- Hard Ties - Example: closed bus ties in alternating current (AC) and direct current (DC) distribution systems.
- Soft Ties – Examples: power is transferred between ac or dc busses using grid interconnector, power convertor technology or cross feeding modes where power is transferred through a DC link in a hybrid power system. Effective mitigations validated by testing should be in place to prevent fault transfer, unless it is proven that the design is such where the need for testing is negated.

3.5.6 Power transfer methods which introduce fault propagation paths for failure modes and their effects require mitigation by a comprehensive range of protective functions which must be verified and validated.

3.5.7 In addition to the cross connection and common points created by main power transfer, the practice of providing cross connections and backup power sources for control power distribution systems from other redundancy groups remains prevalent. These common points are harder to justify in terms of the benefits they bring to station keeping integrity or achieving environmental goals. They are often provided with the intention of reducing the impact of equipment failures on major equipment availability. But this is rarely achieved without compromising the DPRC. Levels of V&V applied to these 'lesser' common points is historically poor compared to that applied to main power transfer, but the consequences of their failure effects can be just as severe.

3.5.8 The presence of these common points in power distribution systems means that, a very significant part of the V&V effort is associated with proving and documenting the efficacy of any mitigating measures intended to limit the effects of fault propagation:

- Where such unproven commonality is discovered on vessels in service, usually as part of charterer's intake processes, there may be little time to address the V&V shortfall and no time to develop a sound engineering solution. Isolating cross connections, not essential for DP, is often viewed as the most practical solution that can be implemented in a short period of time. This approach should only be acknowledged as an interim measure until an engineered solution is implemented. Such interim measures should not be undertaken without V&V activities which should include proving and documenting the effects of the isolation through the MOC process.
- Efficacy of isolation – The isolations actually achieve the expected effect and have been implemented correctly.
- Penalties of isolation – The isolations do not introduce unforeseen reductions in station keeping integrity.

3.6 Influence of Stored Energy – Energy Storage Systems

3.6.1 In the context of this document, the term 'Stored Energy' typically refers to electrical energy stored within batteries. Other forms of stored energy that may be found in DP applications include flywheels and super/ultra-capacitors.

3.6.2 The use of energy storage systems (ESS) and stored energy in a DP redundancy concept adds an additional design and V&V burden. Battery energy storage systems (BESS), capable of supplying propulsion demand, have a multitude of uses. In DP applications, one of those is to act as an electronic generator providing instant on-demand access to standby generating capacity, i.e. 'spinning' reserve without incurring the losses associated with running a partly loaded diesel generator. In their current state of development, the amount of energy that can be stored in batteries is typically a small fraction of the energy in a fuel service tank. Thus, it becomes important to know accurately how much energy is needed and how much energy is available to safely terminate the DP operation using power from battery energy storage, either alone or in combination with diesel generators. These requirements are typically satisfied by:

- The development of a detailed verified timeline for termination of the DP operation.
- The provision of 'state of health' and 'state of charge' information from the batteries to the DP control system and inclusion in the consequence analyser.
- Provision of additional battery capacity to address uncertainties in estimates and the effects of ageing.

The effects of ageing are to be regularly measured by testing and compensated for.

3.6.3 Other influences, for as example, on the DPRC include:

- The ability of convertors to deliver sufficient current to operate over current protection when there are no generators connected following a failure.
- Effective battery management to ensure that the use of the BESS for other objectives, such as peak shaving, do not invalidate the battery's use as a standby power source at the required power rating and endurance.
- The ability of batteries to enhance ride-though capability. Specifically, when connected directly to the thrusters and not to the main bus.
- The impact of common mode noise due to the interaction of inverters and parasitic impedance in DC Systems.

3.6.4 Such influences add to the V&V activities and the list of supporting studies upon which that activity relies.

3.7 Influence of Alternative Fuels

3.7.1 Power generation systems that can operate on alternative fuels, for example, methanol, ammonia, hydrogen, etc. are being developed to reduce greenhouse gas emissions in DP operations and other fields. Many of these fuels have a lower energy density than traditional marine fuels such as Marine Diesel Oil (MDO). Practical limitations associated with the supply of alternative fuels means that DP vessels using these types of fuels may also have a fuel system based on MDO. On smaller DP vessels, which are typically DP class, it becomes impractical to have four or more fuel systems (four is minimum for dual fuel in a two-way split) such that each fuel system satisfies the requirement for independence and redundancy as required by the DPRC. This is seen as a potential barrier to adoption. To address this concern allowances have been made, by some classification societies, for vessels designed to use alternative fuels in addition to MDO. These allowances influence the DPRC and impose additional V&V requirements. These allowances typically include accepting that post failure DP capability can be based on the use of standby redundancy in those notations that have traditionally required the use of active redundancy.

In practical terms, this means that a common alternate fuel supply system can be provided to serve all generators in all redundant DP equipment groups provided:

- There is an automatic changeover to a backup fuel system based on MDO.
- The changeover is independent, autonomous and automatic for each engine.
- The MDO fuel system is split in line with the DPRC and meets the traditional requirements for DP redundancy, independence and segregation.

3.7.2 Other influences on the DPRC include changes in generator performance when operating on different fuels.

3.7.3 These allowance and compensating provisions add to the V&V activities and the list of supporting studies upon which that activity relies.

Notes:

a. The acceptance by class of a non-redundant alternative fuel source for some DP notations is considered to be a concession to promote adoption of greener power system solutions because if the alternate fuel is not redundant then it requires a switch between fuels when the alternative fuel system fails. It is emphasised that reliance on standby redundancy is not accepted by IMO DP guidelines nor certain DP notations.

b. Fuel cells are being considered as potential solutions to achieve GHGER objectives. Implementation on DP vessels should achieve the objectives of EBCV² and demonstrate SFT.

c. Requirements for fuel system redundancy and fault tolerance in vessels using alternative fuels have been in use on dual fuel vessels using Liquid Natural Gas (LNG) for many years and have thus not been specifically called out in this section. The above principles have been applied for dual fuel vessels using LNG.

4 ASSURANCE

4.1 Overview

4.1.1 In the context of this document 'Assurance' is the term used to describe the action of confirming that the V&V processes have been executed competently. In a traditional newbuild project and associated contracting arrangements, the assurance processes are often initiated by the DP vessel owner and/or the vessel charterer to provide confidence in the V&V work being carried out on their behalf. In EBCV^2, as described in this document, the process is formalised to indicate the nature of the responsibilities imposed upon those undertaking this role. The EBCV^2 emphasises the need to provide evidence that the entire process has been competently executed and communicated in a transparent and assurable form to assist further assurance activities which may be carried out by stakeholders through the lifecycle of the vessel.

4.2 Understanding the limitations of assurance, verification, validation, and associated tools

4.2.1 All processes have their limitations. It is critically important to understand the limitations of the V&V process for DP vessels and ensure the verification, validation and assurance processes are properly resourced with competent personnel equipped with the appropriate tools to verify the DP System comprehensively and effectively. Currently, industry guidance focuses on designing systems which may or may not be capable of being comprehensively verified by the commonly used verification tool sets. Particular challenges are associated with:

- The ever-increasing pace of technology development and deployment, and its general impact on the marine and energy industries.
- Corporate and societal commitments to address environmental challenges which is resulting in increasingly complex technical solutions being proposed.

4.2.2 It is important to recognise when challenges, limitations and/or constraints arise and to bolster the V&V processes accordingly. Tools that can assist, by supplementing live testing on the vessel, such as computer simulation of power system response to failure and MBT of protection schemes should be used to achieve comprehensive V&V objectives. It is recommended that these tools be applied regardless of classification society requirements for the DP notation being sought or alternatively, choose a class notation that requires them as it may bring other benefits. As an example, the DPSI process can augment the hardware focus of DP System FMEA in order to address vulnerabilities in software and functionality in control systems.

4.2.3 The EBCV^2 process, given its significance over the lifecycle of the vessel, should be owned by the vessel owner/VTO. They can choose to adopt and implement whatever additional requirements they considered necessary in their specifications/contractual arrangements to manage their own risk portfolio. Class has always been a minimum standard. Recent additions to notations and qualifiers provide additional choice. This unified approach to proving the SFT of DP Systems provides guidance on the methods regardless of class notation or DP equipment class. Class approval will run in parallel and class requirements will vary depending on the notation and qualifiers chosen. When the class notations that offer the highest level of station keeping integrity are selected the gaps, if any, will be smallest.

4.2.4 The system integrator, typically the shipyard, may have to assume the responsibility of the vessel owner/VTO for the EBCV^2 process when there is no clear vessel owner/VTO as a stakeholder. For example, shipyards building vessels on speculation and/or if contractually stipulated in the building specification.

4.2.5 A well-established path to failure is to design systems that are so heavily integrated and so complex that they exceed current V&V capabilities to the point where significant vulnerabilities go undetected. This risk is amplified where designers abdicate responsibility for the fault tolerance of the DP system and rely entirely on external parties to detect non-compliances. Although other Hazard Effect Management Processes (HEMP) are available, the DP community has yet to find ways to derive significant value from such HEMP processes for the purpose of proving SFT in DP Systems.

4.2.6 If highly complex and heavily integrated systems are inevitable, then the impact on the V&V process must be understood and adjustments made to the provision of V&V services well in advance of them being required. Contractual agreements alone are not effective in ensuring a positive outcome if the parties to that agreement do not understand their obligations. There may also be instances where project and operations specific contractual requirements are well specified but not cascaded down to all vendors, OEMs, designers, etc. and these deficiencies are only highlighted at a late stage of the project.

4.2.7 Progress in V&V of software dependent systems has come in the form of recommended practice on DPSI . Software related dependencies may be largely invisible to the traditional DP FMEA process.

4.2.8 Despite the recent efforts, it is still possible for designers to defeat the V&V process by creating designs which exceed the ability of the current V&V tool set and associated resources.

4.2.9 Until such time as the V&V tool set can expand to address these challenges more effectively, the solution to ensuring DP Systems is verified to be SFT is to design systems that are amenable to V&V by the available tool set. This entails:

- Minimising the number of potential fault propagation paths that need to be analysed and tested by reducing commonality, cross connections, external influences and interfaces reduces the initial and periodic V&V burden. This will also minimise the number of compensating provisions that have to be maintained and proven to be effective across a range of operating conditions in a variety of configurations.
- By introducing only those common points and cross connections that provide well defined benefits, time and resources are made available to focus on these few and are not burdened by those that provide limited benefit.

In very simple terms:

'Elimin-*ation* is the Mitig-*ation* for Propag-*ation'*.

Note: Elimination of C^3EI^2 is not the only solution but may be the best in many cases.

4.3 Getting maximum benefit from GAP analysis tools

4.3.1 The MTS DP committee developed a series of gap analysis tools for DP System FMEA and Proving Trials in the form of TECHOPs. These tools take the form of extensive checklists made more manageable by macro enabled spreadsheets with filters for equipment class and power system configuration. These gap analysis tools play an important role in the assurance part of $EBCV^2$. Remedial measures identified at the end of each critical process may include improving the analysis in those activities and not just the technical findings or concerns they generate. This process is identified by the red Closing the Gap (CTG) elements of the $EBCV^2$ flowchart. See APPENDIX A and Figure 2-1.

These gap analysis tools are capable of identifying that an FMEA is not competently executed, but they cannot be relied on to confirm absolutely, that an FMEA has been competently executed as it is based solely on a document review. Thus, a high score in an MTS gap analysis tool is a confidence builder but not absolute proof of a competently executed FMEA and/or proving trials nor do they validate SFT of the vessel on their own.

4.3.2 It is important that the gap analysis tools are used by individuals who have the requisite knowledge to use them effectively. This will typically be a competent DP FMEA provider. It is acknowledged that members of a vessel owners' technical team may also have the right skill set to use such tools.

4.3.3 In addition to the application of gap analysis tools, those charged with carrying out verification and assurance activities will provide comments on the technical content to the authors of the key deliverables to be addressed in the remediation/CTG process.

4.4 Assurance, verification, and validation as part of barrier philosophy

4.4.1 $EBCV^2$ is essentially an assurance process intended to provide an overview of other verification, validation and assurance activities. Verification, validation, and assurance are all barriers to prevent LOP and enable delivery of predictable, incident free, DP operations. In developing the $EBCV^2$ process, a conscious decision was made to link verification, validation and assurance activities in a holistic way as complementary parts of the process which ensures the SFT of DP Systems is proven in a transparent and assurable form.

4.5 Evidence based comprehensive verification and validation Statement of Assurance

4.5.1 APPENDIX C provides a template for the statement of assurance to be completed by the vessel owner or by those responsible for the EBCV^2 process on behalf of the vessel owner. APPENDIX D provides a completed example based on a fictional newbuild project.

4.5.2 The EBCV^2 statement of assurance table provides a cross reference to the key deliverables from the EBCV^2 process. The difference between a statement of assurance for vessels operating with open bus ties (isolated systems) and those configured to operate with closed bus ties (power transfer) is the number of supporting studies and the extent of the validation testing. The supporting studies are listed as subdocuments to the DP FMEA and DPSI. The validation testing – objectives, methods and results – is contained in the DP FMEA proving trials.

5 STATION KEEPING INTEGRITY & COMPENSATING PROVISIONS

5.1 Station keeping integrity through the provision of redundant systems

5.1.1 The SFT of DP Systems is based on the provision of redundant systems as described in IMO MSC.Circ.645 and MSC.1/Circ.1580. Redundancy is used to ensure the DP operation can be terminated safely if the validated worst case failure is experienced. There is no expectation that a DP vessel should be able to continue its IM after a single failure renders it non SFT. There is nothing to prevent additional 'non-critical' redundancy being included in the design if continued operations is an objective.

5.1.2 Requirements for station keeping integrity have consciously avoided references to probability and reliability. However, there is an expectation, inherent in the guidelines, that each redundant system should have sufficient reliability to reduce the probability of experiencing a second independent failure during the time that it takes to terminate the DP operation. Efforts should be made to reduce the probability of experiencing the second independent failure to the extent that it is reasonable to neglect it.

5.1.3 What cannot be neglected is the probability that one of the redundant DP equipment groups is already in a failed state at the time another failure occurs. Detecting such 'hidden failures' is the basis of the requirements for annual and periodic survey. Reasonable means should be deployed to reveal hidden failures at the moment they occur such as:

- Alarms and monitoring.
- Condition monitoring.
- Self-diagnostics.

5.1.4 Although much can be done to ease the periodic reverification burden, these measures, for example, alarms, diagnostics and real time monitoring can also fail over time. Thus, periodic verification by testing is ultimately required.

5.1.5 For DP class 3 systems, where the main requirement is separated systems and open bus ties which is a very effective barrier for the effect of hidden failures - see extract from IMO MSC.1/Circ. 1580 below. Some class societies require double independent barriers to mitigate the effect of one hidden failure. This is considered to be an essential part of satisfying the IMO requirement to demonstrate 'equivalent integrity' parasitic impedance refers to unwanted resistance, inductance, or capacitance in a circuit or component that affects its performance and is not part of its intended function.

IMO MSC.1/Circ. 1580 states in section 3.2.4 ‘For equipment class 3, the power system should be divisible into two or more systems so that, in the event of failure of one system, at least one other system will remain in operation and provide sufficient power for station keeping. The divided power system should be located in different spaces separated by A-60 class divisions. Where the power systems are located below the operational waterline, the separation should also be watertight. Bus tie breakers should be open during equipment class 3 operations unless equivalent integrity of power operation can be accepted according to paragraph 3.1.4.’

5.2 The role of compensating provisions

5.2.1 As its name suggests, a compensating provision is a function or feature provided to control the outcome (and therefore consequences) of an event. In the case of a DP System, the provision of redundant DP equipment groups is itself a compensating provision. The addition of redundant systems changes the outcome of a single failure from ‘LOP’ to ‘loss of redundancy’ enabling safe termination of DP operations.

5.2.2 In the vocabulary of the DP community, compensating provisions are variously known by synonyms such as:

- Mitigating measures.
- Protective functions.

5.2.3 Compensating provisions are applied to DP Systems in different ways to prevent the two mechanisms by which LOP can occur as the result of a single failure namely:

- Drift off.
- Drive off.

The term Force Off is often used in the discussion of LOP incidents. A Force Off occurs when the environmental forces exceed the DP capability of the vessel in the intact state. It does not occur as the result of a failure and is not discussed further in this document as it is not associated with SFT.

5.3 Drift off & drive off

5.3.1 At a fundamental level, the difference between drift off and drive off is that:

- In a drift off, the vessel will move off setpoint in a direction influenced by the environmental forces. The speed and direction of movement is determined by its residual thrust capacity and the environmental forces. Residual thrust capability may be zero in the worst case.
- In a drive off, the vessel can move off setpoint in any direction. The speed at which it moves is determined by the difference in the thrust vector it is developing and that needed to balance the environmental forces. It may be maximum thrust in the worst case.

5.4 Causes of drift off and drive off

5.4.1 Drift off occurs when there is insufficient capability to develop the required thrust vector. A performance deficit within more than one redundant equipment group is required to create a drift off in a fault tolerant DP System that is operating within its defined worst case single failure criteria. Compensating provisions are applied to common points to prevent more than one redundant DP equipment group being affected by the effects of fault propagation between redundant DP equipment groups.

Not every combination of failures in different redundancy groups leads immediately to a drift off but it is essential that failures are detected and repaired as soon as possible after they occur and before the resumption of DP operations. (Example – failure of one diesel generator in each redundant group on a vessel configured with more than two diesel generators in each redundant group). Failures in DP essential systems will have some impact on the DP System's fault tolerance either reducing post failure DP capability or removing its SFT.

5.4.2 Drive off occurs when there is adequate thrust generating capacity, but incorrect thrust magnitude and/or direction. Unlike drift off, drive off can occur because of a single failure in one redundant DP equipment group. Causes of drive off are generally associated with erroneous position solutions in the DP control system or failures in a thruster control system creating excess or misdirected (unwanted) thrust. Compensating provisions are needed to detect control system failure and taking action to mitigate it.

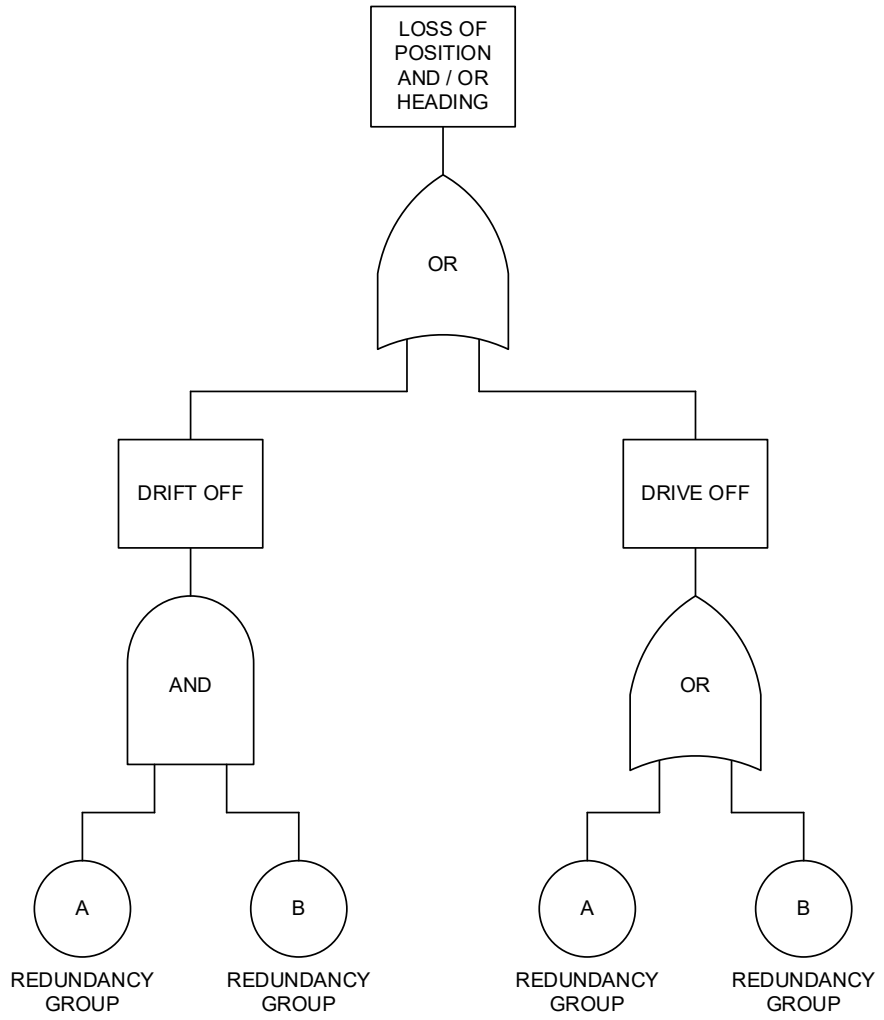

Figure 5-1 Fault Tree for Loss of Position/Heading (DP System)

5.4.3 Redundant DP System Example - two-way split. Refer to the fault tree in Figure 5-1. In the case of a DPRC with a two-way split, it takes two concurrent independent failures, or an unmitigated common cause/common mode failure, to create a drift off. That is to say both the port group (A) and the starboard group (B) must be incapable of developing the thrust required to maintain position and heading. However, it only takes a single failure, of the right kind, in one of the two redundant DP equipment groups to create a drive off. In practical terms:

- Concurrent faults in any part of the port and starboard DP power or control system equipment groups can cause a drift off. Compensating provisions include protective functions to prevent fault propagation and detection of the first fault are the mitigation.
- Some single failures in either a thruster control system or DP control system, in either the port or starboard groups, can cause a drive off. Compensating provisions, in the form of protective functions must be provided to detect the onset of these types of failures and mitigate them. This is called the 'fail-safe condition'. Compensating provisions might include:
  - Stopping a thruster that has failed to full thrust.
  - Rejecting a position reference or sensor that is corrupting the DP control system's position and/or heading solution.
  - Engaging a backup DP controller to replace one that is making erroneous calculations.

5.4.4 Mitigation of drift off and drive off:

- The compensating provision for drift off is the 'independence' of the redundant DP equipment groups.
- The compensating provision for drive off is the 'failsafe' property of the redundant DP equipment groups.

5.4.5 Independence is achieved by segregation and/or protective functions. Failsafe is achieved by protective functions.

5.5 Verification and validation of compensating provisions

5.5.1 As compensating provisions play a vital and extensive role in a DPRC's, confirming the efficacy of compensating provisions accounts for a significant part of the V&V effort.

5.5.2 The V&V processes can be described as confirming that redundant and/or independent equipment groups exist which are capable of developing the required surge, sway and yaw forces either on their own or in combination with other independent or redundant equipment groups.

5.5.3 The following terms are defined in the context of this document and have been adopted broadly across the DP community:

- **Independent,** in this context, means not subject to a common cause of failure. Defined failure criteria apply.
- A **redundant group** is capable of providing surge, sway and yaw on its own.
- An **independent group** can provide surge, sway and yaw in combination with other independent or redundant groups.

  Example – A drillship with three azimuthing thrusters forward and three aft may consist of three redundant groups, each with a forward and aft thruster, if its power system is designed as a three-way split. If it were designed as a six-way split, there would be six independent groups each with either a forward or an aft thruster.
- **Diversity in Definitions.** Organisations may define terms differently. While there is broad alignment in definitions of technical terms, some variation can be found where a particular organisation sees a need to add emphasis to an important attribute:

- The definitions by classification societies of the above terms may diverge from those used in the context of this document and broadly by the DP community
- Some organisations do not distinguish between 'Independent' and 'redundant' equipment groups for ease of communication. All groups not subject to a common cause of failure are considered to be 'redundant'. Others see benefit in making a distinction.
- Similarly, some organisations define the term 'independence' differently in so far as some consider that independence requires complete separation while others accept a degree of commonality mitigated by the operation of on-demand functions.
- Minor differences in definitions are likely to remain a feature of DP rules and guidance across the DP community and users are encouraged to become familiar with such minor variations in the same way that requirements and interpretations vary from one classification society to another.

5.5.4 Verification and validation (V&V) of compensating provisions generally means proving that they will operate effectively under all defined conditions and that the DP System is able to continue in operation without malfunction exceeding the severity of the WCFDI. The ability to continue in operations during and after the disturbance associated with clearing a fault from the power system is generally referred to as Fault Ride-Through. Although it is often applied to power systems, the term can be used more generally and applied to other systems such as control systems.

5.6 Protective functions as compensating provisions

5.6.1 DP power plant operating with closed bus ties or power transfer between redundant DP equipment groups is highly dependent on protective functions and performance attributes to mitigate the effects of faults which may propagate through the main power system coupling and any other common points.

5.6.2 The subsystems that are likely to contain protective functions would include, but are not limited to:

- Engine safety and control system.
- Detection methods and auto changeovers in dual fuel system for vessels using alternative fuels.
- Generator protection.
- Power distribution system protection at all distribution voltage levels.
- Battery management and safety systems for hybrid power/BESS.
- Power and energy management systems.
- Standalone blackout prevention systems.
- DP control systems.
- Control systems for thruster drives.
- Drilling/IM equipment control system.
- Thruster speed and azimuth closed loop control systems.

5.6.3 The accepted means of building a sufficient basis for confidence in the protection systems of power systems is an overall comprehensive protection coordination study, proven by a combination of simulation/MBT, live short circuit and ground fault testing and dynamic computer simulation of the protection scheme response.

5.6.4 The primary purpose of live short circuit testing is proving voltage dip ride through (system wide) in as realistic a manner as possible. While it will test other functions such as excitation support and over current protection it will not test this on every circuit. It is considered impractical to do so. The highest level of confidence is thus obtained using the results of a live short circuit test to validate the power system model to improve confidence in its predictions and then use the validated model to provide waveforms for use with MBT. This combination of verification measures supports the intent of providing equivalent integrity as required by IMO guidelines and Class rules.

6 DERIVING MAXIMUM VALUE FROM THIS GUIDANCE

6.1 Extracting relevant material from guidance

6.1.1 The DP community has produced a wealth of technical and operations guidance over the years, much of it derived from experience and lessons learned. Much progress has been made in promulgating new knowledge and good practice through improvements to rules and guidelines, also through DP conferences, workshops, and seminars. Organisations and individuals in the DP community are more familiar with the vocabulary of fault tolerant systems and the risks associated with fault propagation through common points. Despite these welcome developments, experience suggests there is opportunity to be more effective in ensuring that DP Systems are SFT, and verified to be so, by suitable analysis and testing.

6.1.2 The origins of this unified approach to the V&V of SFT in DP Systems lie in the realisation that the probability of a satisfactory outcome from a DP vessel newbuilding or conversion could be improved by providing a framework to support the use of the existing guidance.

6.1.3 Maximum value can be derived from the processes described in this document if they are used to understand which elements need to be extracted from technical guidance and applied directly to the vessel specification and which guidance documents need to be applied to the design information at each point in a newbuilding or major conversion DP vessel project. Such an approach can lend itself to ensuring that the design is SFT and is capable of being verified and validated by the tools currently available to the DP community. This practice allows requirements for analysis and testing to be understood and achievable by those required to comply with them.

6.2 Applicability

6.2.1 This guidance is intended to assist a diverse range of stakeholders including all of the supply chain for DP newbuildings and major conversions:

- Vessel owners and their project teams can use it to:
  - Support their use of guidance documents in the development of specifications for DP System designs that meet their expectations.
  - Understand and monitor V&V progress throughout the build and understand which stakeholders have responsibility for which activities and deliverables at each stage of basic design, detailed design and build.
- Shipyards and integrators can use it to understand the importance of deliverables, validation testing and the influence of guidance being referenced on the design.

- Verifiers, including Class and DP FMEA providers, can use it to understand the vessel owner's intentions and expectations in respect of verification, validation and validation testing.
- OEMs can use it understand their part in the V&V process.

6.3 Driving standardisation, consistency and transparency

6.3.1 One of the primary purposes of this guidance is to provide a transparent framework that shows the relationships and responsibilities between stakeholders involved in the design V&V process. Essentially - who produces what and when, and who uses it for what purpose.

6.3.2 Promoting standardisation, transparency and collaboration in the V&V process is one of the key enablers for a successful DP newbuilding or conversion. Visibility into the process allows all stakeholders to participate more effectively and more efficiently. Standardisation of processes allows all stakeholders to understand and align on expectations and obligations.

6.4 Leveraging guidance and imposing requirements contractually

6.4.1 The development of specifications for newbuildings and conversions tends to focus on listing relevant codes, standards, and industry guidance documents. This is done on the assumption that their inclusion within a contractual framework will ensure that systems are designed and built to comply with the guidance therein.

6.4.2 Experience shows that this approach is not as reliable as might be expected. This could be a result of the following:

- The vessel owner and/or key OEMs may not fully appreciate the impact of the referenced guidance on the OEM's standard/legacy offering. Adapting it to comply with guidance may be impractical by the time this incompatibility is recognised.
- Guidance documents may discuss a number of viable solutions not all of which have all the advantages of the best solution.
- The language used in guidance documents is generally not sufficiently prescriptive to rely on contractually.

6.4.3 Too often, good intentions at project initiation are compromised by insufficient attention to developing a specification that ensures the design meets expectations. It is not sufficient to simply list guidance documents. Those guidance documents have to be understood and used by those preparing the vessel specification to create design specific requirements using the appropriate contractual language.

6.4.4 Competence is an essential element in a quality V&V process. Lack of competence is often a cause of flaws being overlooked or identified too late. Care must be taken to understand the V&V burden and ensure the process is adequately resourced with competent personnel who have access to effective tools to support delivery.

7 CONCLUSIONS

7.1 Introduction

7.1.1 This publication is the output of a JDP involving representatives from IMCA, MTS, DPC, OCIMF, ABS, DNV, BV and LR. A work group was formed to develop a framework to enable the SFT of DP Systems of DP class 2 & 3 to be verified, validated and assured in a transparent, evidence based, and comprehensive manner called EBCV[2].

7.1.2 Iterative discussions at various DP community forums acknowledged the need to pivot from the established focus debating the relative merits of open and closed bus ties to the more objective approach of proving SFT in absolute terms in the configuration the vessel was operating in.

7.1.3 It was recognised that operating DP vessels in a closed bus configuration without accepting an unjustifiable amount of additional risk was possible with the implementation of currently available and evolving technology and progressive insights.

7.1.4 Addressing SFT in the context of the configurations the vessels were operated in and through the lens of EBCV^2 was acknowledged as a credible means to address obligations and societal expectations of GHGER in the DP vessel segment.

7.1.5 The subsequent sections that follow provide a summary conclusion on EBCV^2 and the influence of configuration, i.e. open and closed bus ties.

7.2 Evidence Based Comprehensive Verification and Validation

7.2.1 The main elements of EBCV^2 are a framework based on demonstration of SFT as an objective supported by tools such as RCPD, FMEA and DPSI supplemented by relevant supporting studies and informed by technical guidance on the vulnerabilities of DP Systems including C^{3}EI^2. Adherence to the principles of EBCV^2 ultimately leads to a clear and unambiguous understanding of a DPRC and its compensating provisions which provide a basis for confidence in the vessel's station keeping integrity and ensures an acceptable response to failures. The influence of system configuration on the redundancy concept and the V&V process is explained with particular focus on the attributes of performance, protection and detection upon which it relies for its SFT. Included in EBCV^2 are a:

- Process flowchart on how to combine design information with relevant guidance to undertake and inform key V&V processes. See APPENDIX A.
- Evidence distribution matrix, connecting key stakeholders in the EBCV^2 process, to the analytical and empirical evidence they must develop and review. See APPENDIX B.
- References to relevant technical guidance from all participating organisations. See APPENDIX C & **Error! Reference source not found.**.
- A list of necessary supporting engineering studies. See **Error! Reference source not found.**.
- A template for a 'Statement of DP System Assurance' which records all the documentary and other, data centric, forms of evidence which together support a conclusion of SFT in defined configurations. A worked example based on a fictional construction vessel project is provided showing the process leading up to completion of the statement of DP system assurance. See APPENDIX D.

7.3 Selecting closed bus ties as an operating configuration

7.3.1 Verification, validation, and assurance of the SFT of DP systems is an increasingly complex process. EBCV^2 is recommended for use with DP class 2 and DP class 3 vessels intending to operate in any power system configuration. Special attention has been given to the processes designed to ensure that it is possible to achieve high levels of station keeping integrity in closed bus configurations.

7.3.2 The additional complexities of DP power plant incorporating BESS, alternate fuels, power transfer between redundant DP equipment groups, for example, closed bus ties), adds further complexity and verification burden. The technical, design and construction part and the verification part must be performed effectively and comprehensively to achieve the desired outcome of incident free DP operations.

7.3.3 There is a risk that the selection of closed bus ties, as the preferred operating configuration, is made in response to pressure to address issues other than DP safety and reliability. For example, GHGER.

7.3.4 The risks are amplified if this operating configuration is selected without understanding the implications of this choice and the design, V&V burden and all complementary measures associated with Design, Operations, People and Processes. Achievement of SFT and station keeping integrity is not limited to analysis of technical systems but also includes:

- Assurance activities (initial and during operations).
- Crew training and competence.
- Operation procedures.
- MOC processes, etc.

7.3.5 In summary, the objectives of GHGER can be achieved using DP Systems based on closed bus configurations without incurring unacceptable reductions in DP station keeping integrity but only if the design and EBCV[2] process are suitably resourced and competently executed.

APPENDICES

APPENDIX A MASTER FLOWCHART

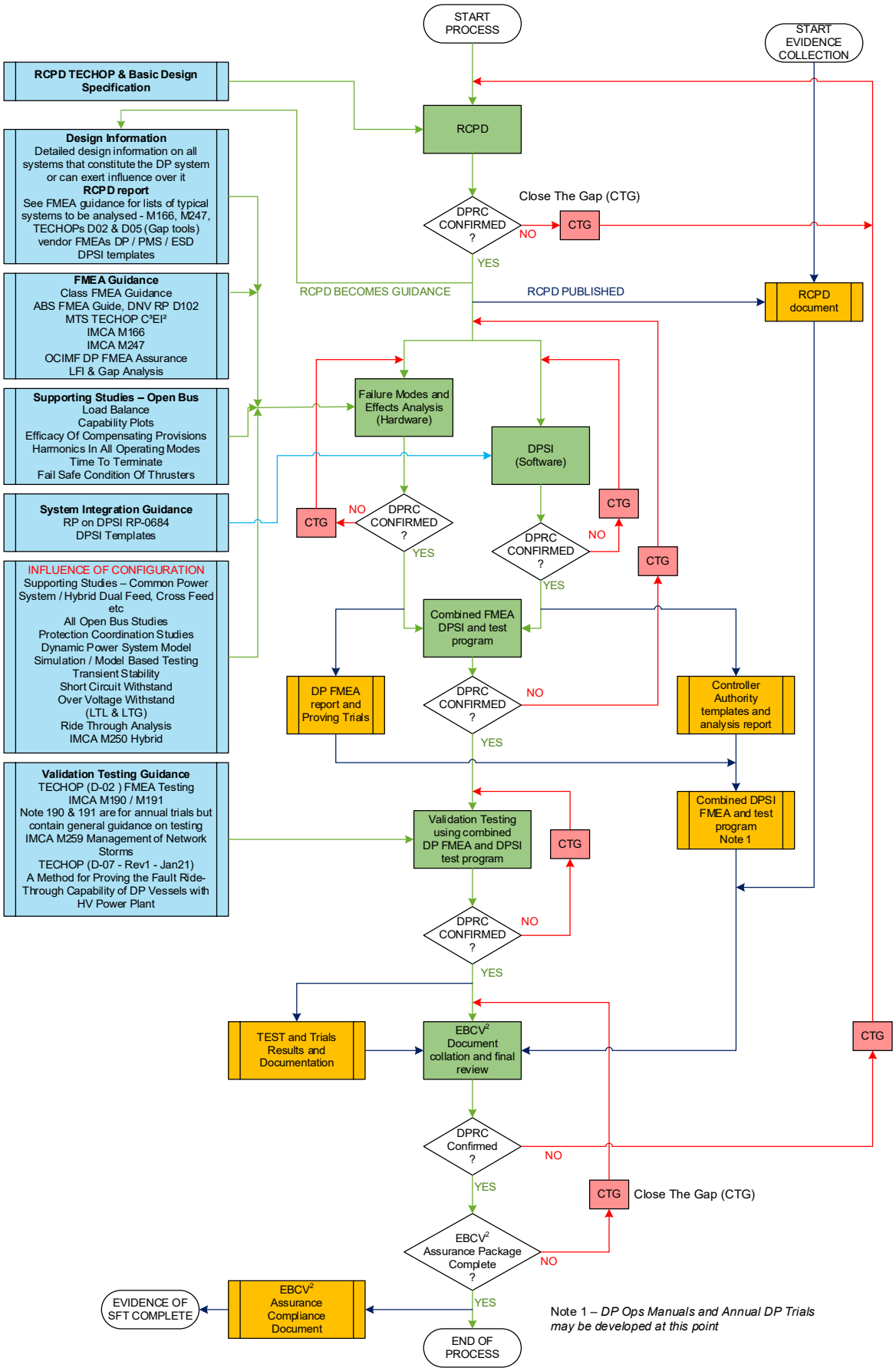

Figure A-1 - Master Evidence Based Comprehensive Verification and Validation (EBCV²)Process Flowchart

A.1 GUIDE TO FLOWCHART

A.1.1 EBCV²

A.1.1.1 EBCV² consists of several process elements. Most of these are recognisable as existing elements of any DP verification and validation process:

- RCPD.
- DP System FMEA – hardware related.
- DP System Integration (software/functionality related)*.
- DP FMEA proving trials including tests generated by supporting studies and activities such as live short circuit and ground fault testing, and MBT.
- EBCV² is the designation given to the overall verification, validation and assurance process but is also used to describe the activity of collecting all the evidence indicating that the process has been followed.

Note*: Refer to *DNV RP-0684*.

A.1.1.2 RCPD, DP System FMEA and DPSI are analytical in nature. DP FMEA proving trials is the repository for all the validation testing although some of this testing may be performed at other times and test opportunities, where appropriate.

A.1.2 FLOWCHART

A.1.2.1 There are four basic elements to the EBCV² flowchart colour coded Red, Blue Green and Yellow:

- The **Green** elements represent the processes. These processes are the familiar V&V activities such as DP system FMEA and FMEA proving trials, etc.
- The **Blue** elements are the feedstock to the processes and comprise the detailed design information and the guidance to be used in each step of the process.
- The **Yellow** elements represent the deliverable or output from each process which are collected to form the EBCV² assurance documentation package that contains the proof of the SFT of the DP System.
- The **Red** elements represent the review process and corrective actions which may be required at each stage. At the end of each process are decision points where the requirement is to confirm the DP systems' redundancy concept has not been compromised. This is determined by the findings from the process that has just been executed but also by quality checks on the process itself such as the various FMEA and proving trials gap analysis tools. EBCV² does not proceed to the next process until identified gaps have been closed.

APPENDIX B EVIDENCE BASED COMPREHENSIVE VERIFICATION AND VALIDATION (EBCV^2) MATRIX OF DELIVERABLES AND GUIDANCE REFERENCES

Evidence Based Comprehensive Verification and Validation (EBCV²)									
Assurance / V&V activity	Deliverables and Supporting Studies	Guidance Rules and Standards	Role / Usage	Class(A)	FMEA / DPSI Provider(B)	DP Assurance Providers(B) (End User Reps)	Owner / VTO Assurance / Site Teams	Designers & OEMS	Integrators Including shipyard	Notes
			Role: Developer							D
			Role: User							U
			Usage: Assurance							(A)
			Usage: Verification & Validation							(V)
			Usage: Information							(I)
			Usage: Not Used							(N)
Redundancy Concept Philosophy Document (RCPD)		RCPD TECHOP DNV RP-0591 Appendix A		U (V)	U (I)	U (A)	D(1)(V)	U (I)	U (I)	1. This could be shipyard in a spec build
DP System FMEA	DP System FMEA report (Preliminary & Final)	M166 / RP-D102 / ABS FMEA Guide / OCIMF DP FMEA Assurance(2)		U (V)	D (V A)	U (A)	U (A)	U (I)	U (I)	2. Other standards may be specified in addition to those listed
	DP Control System FMEA	M166 / RP-D102 / ABS FMEA Guide / OCIMF DP FMEA Assurance(3)		U (V)	U (V)	U (A)	U (A)	D (V)	U (I)	3. Some classification society rules require a DP System FMEA to be provided by the OEM
	PMS FMEA	M166 / RP-D102 / ABS FMEA Guide / OCIMF DP FMEA Assurance(4)		U (V)	U (V)	U (A)	U (A)	D (V)	U (I)	4. Not every project will have a dedicated PMS FMEA
	Coordination Study	IEC / MTS DP Design Philosophy Guidelines / Class rules for Electrical Installations		U (V)	U(5) (V)	U (I)	U (A)	D (V)	U (I)	5. DP FMEA provider to confirm coordination of protective function supports RC
	Model Based Testing for Power Systems(6)	MTS DP Design Philosophy Guidelines		U (V)	U (V)	U (I)	U (A)	D (V)	U (I)	6. Unlikely to be required for OPEN BUS configuration. Other sub systems (Open and Closed bus) may require MBT e.g., thruster / rudder fail safe
	Load Balance(7)	IEC / Class Rules		U (V)	U (V)	N	U (A)	D (V)	U (I)	7. Shipyard may be developer of load balance
	Time to Terminate(8)	Class Rules		U (V)	U (V)	U (I)	U (I)	D (V)	U (I)	8. Particularly for hybrid power systems with limited capacity
	Harmonics Analysis	IEC / Class Rules(9)		U (V)	U (V)	N	U (A)	D (V)	U (I)	9. Harmonics measurements are necessary to validate the analysis
	Thruster FMEA – Fail Safe Condition(10)	IMO 645 / 1580 / Class Rules		U (V)	U (V)	U (A)	U (A)	D(10)(V)	U (I)	10. May be part of a dedicated thruster control system FMEA
	Transient Stability (crash sync, load Acceptance & rejection) (11)	IEC / Class Rules		U (V)	U (V)	N	U (A)	D (V)	U (I)	11. Unlikely to be required for OPEN BUS configuration but may be required for some types of coupled power systems (example cross feeding hybrid).
	DP System FMEA Gap Analysis	MTS TECHOP		N	D(12) (A)	U (A)	U (A)	U (I)	N	12. May be commissioned from another provider.

A. Class may use different standards to those listed / mentioned below.

B. Independent 3rd Parties offer a range of services including DP FMEA and DP assurance work from charterers. For EBCV² these will usually be different organisations.

Evidence Based Comprehensive Verification and Validation (EBCV²)									
Assurance / V&V activity	Deliverables and Supporting Studies	Guidance Rules and Standards	Role / Usage	Class[A]	FMEA / DPSI Provider[B]	DP Assurance Providers[B] (End User Reps)	Owner / VTO Assurance / Site Teams	Designers & OEMS	Integrators Including shipyard	Notes
			Role: Developer							D
			Role: User							U
			Usage: Assurance							(A)
			Usage: Verification & Validation							(V)
			Usage: Information							(I)
			Usage: Not Used							(N)
	OCIMF DP FMEA Assurance Framework – Statement of Compliance	OCIMF DP FMEA Assurance Framework (2020)		U (*I*)	N	U (*A*)	D[13](*A*)	U (*I*)	N	13. DP FMEA provider may produce OCIMF document for VTO
DP FMEA Proving Trials	Proving trials document	MTS TECHOP IMCAM166 M103 IMCA M259 Management of Network Storms		U (*V*)	D (*V A*)	U (*A*)	U (*A*)	U [14] (*I*)	U[15] (*I*)	14. Designers and Shipyards may use the DP FMEA trials program to develop the test plans they may be required to execute.
	Proving Trials Gap Analysis	MTS TECHOP		N	D [15](*A*)	U (*A*)	U (*A*)	U (*I*)	N	15. May be commissioned from another provider.
	Short Circuit and Ground Fault Test Report[16]	TECHOP (D-07 - Rev1 - Jan21)		U (*V*)	U(*I*)	U (*A*)	U (*A*)	D (*V*)	U(*I*)	16. This may be a separate report or may be appended to the DP FMEA proving trials
Annual DP Trials	Annual DP Trials Program	IMCA M190 & M191 MTS TECHOPs		N[17]	D (*A*)	U (*A*)	U[18] (*A*)	N	N	17. Class may approve Annual Trials Program for DPDS, DNV class notations with 'A' qualifier or continuous verification regime for MODUs etc. 18. VTO may develop annual DP trials program
	Annual Trials Gap analysis	MTS TECHOP		N	D[19] (*A*)	U (*A*)	U (*A*)	U (*I*)	N	19. May be commissioned from another provider.
DP System Integration (DPSI)	RP-0684 DP System Integration	OEM Templates for controller authority[18]		U (*V*) [20]	U(*V*)[21]	N	U(*V*)	D(*V*)	U(*V*)[19]	20. Class may approve this where the RP is followed for the purposes of gaining a specific notation. 21. User will normally be DP FMEA Provider and Shipyard
C³EI²	*MTS TECHOP (D-01 - Rev1 - Jan21) 'Addressing C³EI² to Eliminate Single Point Failures', provides a wealth of knowledge on the subject of identifying, avoiding, categorising, and managing the risks introduced by common points between redundant DP equipment groups in DP Systems. The guidance is based on real life lessons learned from DP incidents and other sources. It is essential reading for those developing a Redundancy Concept for a DP vessel.*									
Class	• Class Society application of documents and various standards is applied per each Class Society's Rules and policies as deemed appropriate for each DP vessel and intended missions. • MBT is not required for all class notations therefore it must be specified by the owner in these cases. • Time to terminate is to be specified and maybe subject to comment, but as it is highly operational it is accepted for information rather than approval by some classification societies. • In this table, *V* does not necessarily imply **approval** by the class society. Class may use information for different purposes. • The proving trials document is to be used for five yearly renewal trials. It is required to be updated by class • DPSI, DNV RP-0684 is an additional service and not part of the process for the DP notations.									
DP Ops Manual / ASOG CAMO and TAM	*The DP Ops manual, A(W)SOG, CAMO and TAM do not directly from part of the verification and validation (V&V) process, but they are a direct output from it and are subject to their own assurance process which confirms their validity. They are essential elements in the process of managing station keeping risk.*									

APPENDIX C TEMPLATE FOR STATEMENT OF DP SYSTEM ASSURANCE

STATEMENT OF DP SYSTEM ASSURANCE				
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements.*	**Evidence Based Comprehensive Verification and Validation (EBCV²)**			
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG Assurance**
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**	**Project Responsible Sign Off**
Redundancy Concept Philosophy Document (RCPD)	RCPD report for DP Vessel		RCPD describes a viable, SFT DP system capable of being verified, validated and assured to class rules for the specified notations and any additional requirements.	
	CTG – Seven Pillars comparator Tool		Seven Pillars comparator indicates intention to test all performance attributes and protective functions and there are no unnecessary common points.	
DP System FMEA	DP System FMEA report		Category A concerns closed? Bs and Cs evaluated?	
	DP Control System FMEA		Conclusions compatible with overall DP System FMEA	
	PMS & VMS FMEA		Conclusions compatible with overall DP System FMEA	
	Coordination Study		Confirmed to support the DPRC	
	Computer simulation of power system and its protection		All modes of failure analysed in all configurations and protection proven to be fully selective – Supports WCFDI.	
	Load Balance		Aligns with WCFDI and PFC	
	Time to Terminate		Is appropriate for the IM	

STATEMENT OF DP SYSTEM ASSURANCE					
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements.*	**Evidence Based Comprehensive Verification and Validation (EBCV²)**				
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG Assurance**	
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**		**Project Responsible Sign Off**
	Harmonics Analysis		Meets class requirement in all configurations and post worst case failure of harmonic cancelation features		
	Thruster FMEA – Fail Safe Condition		Thrusters fail safe proven by analysis and testing		
DP System FMEA	Transient Stability (crash sync, load Acceptance & rejection)		Power plant remains stable under all failure mode in all defined configurations		
	CTG - DP System FMEA Gap Analysis		All gaps closed		
	CTG - OCIMF DP FMEA Assurance Framework – Statement of Compliance		Valid OCIMF statement of compliance		
DP FMEA Proving Trials (inc. validation testing).	Proving trials document		All Category A concerns closed and Bs and Cs evaluated		
	Model Based Testing for Power Systems		Confirms the efficacy of the protection coordination		
	Short Circuit and Ground Fault Test Report		Test method meets classification society and EBCV² requirements to proves the voltage dip ride though capability of the power plant and WCF		
	CTG - Proving Trials Gap Analysis		All gaps closed		
Annual DP Trials	Annual DP Trials Program		A proforma is available for future use in the case of new builds which proves all the elements of performance, protection, and detection		
	CTG - Annual Trials Gap analysis		All gaps closed		
DP System Integration (DPSI)	RP- 0684 DP System Integration integrated within the DP FMEA (Typically)		All category A concerns closed (as part of FMEA)		

STATEMENT OF DP SYSTEM ASSURANCE					
Note: Where required, a*cceptance criteria will include satisfying class comments in addition to any other contractually specified requirements.*	**Evidence Based Comprehensive Verification and Validation (EBCV²)**				
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG Assurance**	
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**		**Project Responsible Sign Off**
EBCV² Documentation Package Assembled Post Trials	DP FMEA with DPSI		There are no outstanding concerns at Category A		
	DP FMEA Proving Trials		There are no outstanding concerns at Category A		
	MBT Report		There are no outstanding concerns at Category A		
	Live Short Circuit and Ground Fault Report		There are no outstanding concerns at Category A - Test results prove the voltage dip ride though capability of the power plant and confirm WCFDI		
	All other supporting reports are included in the final documentation package. These may also be at higher revision levels if the validation test results have revealed a need for them to be amended.		Any concerns that could impact the single fault tolerance (SFT) and post failure DP capability of the DP System have been addressed and proven by validation testing where necessary		
	CTG - All concerns of category A from Validation testing addressed				
	CTG Documentation Package Complete				
Project Manager Sign Off	EBCV² Process and Package Completed				

APPENDIX D EXAMPLE PROCESS AND STATEMENT OF DP SYSTEM ASSURANCE (FICTIONAL)

D.1 BACKGROUND

D.1.1 This is a fictional narrative that illustrates the processes that lead eventually to completion of the EBCV[2] statement of assurance and the associated documentation package for the DP System. The vessel is being built for a contract with Enerjet, an energy company with a large oil, gas and renewables portfolio. The owners of Kondor Marine Contracting (KMC) have established a project to add a new J-lay pipelaying vessel to their fleet and are required contractually to demonstrate SFT and EBCV[2].

D.2 STAKEHOLDERS

Stakeholder	Abbreviation	Role
Kondor Marine Contracting	KMC	Owner
Enerjet PLC	EJ	End User Charterer
Central Bureau of Verification	CBV	Classification Society
Consolidated Maritime Limited	CML	Owner's DP Assurance Advisor
Omni Marine	OM	FMEA and DPSI Provider
Maritech	MT	Assurance Provider for End User Charterer
Nordic Heavy Industries	NHI	Shipyard
Scandica Marine	SM	DPCS, PMS and VMS OEM
Green-Power-Services	GPS	Power System
Torque-Master	TM	Thrusters

Table D-1 - Stakeholders

D.3 MV KONDOR-KAI

D.3.1 The new vessel, to be named Kondor-Kai, is a DP class 3 design built to the rules of the Central Bureau of Verification (CBV). To meet KVC's corporate and societal obligations to GHGER, the vessel's DPRC will include open and closed bus configurations and the use of BESS. All of the engines will be able to operate on either MDO or Methanol.

D.3.2 KMC establishes an in-house team to oversee the project and develop the specification of the vessel and its DP System with a dedicated section focusing on the pipelaying system. These specifications include basic vessel and DP System designs that will become the basis of invitations to tender from shipyards.

D.3.3 Key team members in the KMC project team are:

- Derrick Thomas Redford (*DTR*) Project Manager
- Aksel Odd Carlsen (*AOC*) Naval Architect
- Dana Gabriella Giovana (*DGG*) DP superintendent
- Andrew Neil Jones (*ANJ*) Electrical superintendent
- Bianca Larissa Perez (*BLP*) Controls and Instrumentation superintendent

D.3.4 The project team elects to use the EBCV^2 process to ensure they are able to oversee the verification, validation and assurance processes which are necessary to confirm the SFT of the DP system in a comprehensive and transparent manner. This process is complementary to the approval and classification processes being performed by CBV and a third-party assurance provider called Maritech (MT) who is providing DP assurance services to the end user charterer Enerjet.

D.4 REDUNDANCY CONCEPT PHILOSOPHY DOCUMENT AND BASIC DESIGN

D.4.1 The KMC project team commissioned a local DP FMEA provider called Consolidated Maritime Limited (CML) to help them develop the vessel's DP System specification, a DPRC philosophy document for the vessel and provide general technical DP support to the project team.

D.4.2 With assistance from CML, the KMC project team uses established industry guidance on DP vessel design philosophy to develop a basic vessel design including the thruster layout, high-level piping and instrumentation schematics and one-line diagrams for the power and propulsion system. CML uses the guidance documents referenced in the EBCV^2 publication and MTS *TECHOP (D-11-Rev.3 - March 24)* RCPD, to evaluate the redundancy concept against the 'Seven Pillars' and present it for use in the tendering process (following final revisions to the design and specification). This document is issued as KMC-Kondor-Kai-RCPD–R001 and becomes part of the specification and ultimately the contract for the vessel. Because there are a number of novel features in the DP System of the Kondor-Kai, KMC uses the RCPD in support of an Approval In Principle (AIP) process with the classification society CBV. The findings from the AIP are incorporated into the specification. KMC proceeds to the tendering stage confident that there are no insurmountable verification challenges in the design.

D.5 DETAILED DESIGN AND CONSTRUCTION

D.5.1 The successful shipyard is Nordic Heavy Industries (NHI). They use the RCPD in their technical and commercial engagements with OEMs on the 'Makers List' and with DP FMEA providers, to ensure there are no misunderstandings about the nature of the DPRC and its defined operating configurations. The shipyard engages an FMEA provider called Omni Marine (OM) to prepare the DP System FMEA and proving trials for CBV approval and distribution to other stakeholders. This process follows the referenced guidance docs in EBCV^2 (APPENDIX B). OM is also given the job of overseeing the DPSI process. CML is given the job of overseeing the EBCV^2 process for the owner, KMC and they prepare the documentation distribution list in the form shown in APPENDIX B. To ensure that the RCPD is understood and communicated OM, the FMEA & DPSI provider works with the shipyard project team to organise a series of kick-off meetings with key OEMs as the detailed design process begins.

D.6 FAILURE MODE EFFECT ANALYSIS, PROVING TRIALS AND DP SYSTEM INTEGRATION

D.6.1 Prior to these meetings, OM begins issuing the DPSI templates for completion by the appropriate control system OEMS. Once completed OM analyses the data and incorporates their findings into the DP System FMEA. Meetings with OEMs are also used to reconfirm the commitment to using the guidance listed in the EBCV^2 guidance doc (which is listed in the specification for the vessel) with particular focus on common points and fault propagation paths as described in MTS TECHOP (D-01 - Rev1 - Jan21) Addressing C³EI² to Eliminate Single Point Failures.

D.6.2 The PMS/EMS, VMS and DP control system are all produced by the same OEM, Scandica Marine (SM). The power system OEM is Green-Power-Services (GPS), and the thrusters are provided by Torque-Master (TM).

D.6.3 Scandica Marine produces an in-house FMEA for the PMS/EMS, VMS and DPS and provides it to other stakeholders according to the distribution list. These are issued as:

- SM-Kondor Kai – PMS/EMS FMEA RA
- SM-Kondor Kai - VMS FMEA RA
- SM-Kondor Kai - DPCS FMEA RA.

D.6.4 Because the DPRC includes a configuration based on closed bus ties, the protection coordination study becomes an important input to the DP FMEA and a copy of document GPS - Kondor Kai - COORD – R01 is issued to stakeholders by the power system OEM Green-Power-Services.

D.6.5 Using the detailed design information provided by the shipyard combined with the OEM FMEAs and coordination study OM, the FMEA and DPSI provider issues preliminary DP FMEA document OM-Kondor-Kai Preliminary DP FMEA – R0 and its associated proving trials OM-Kondor-Kai Preliminary DP FMEA Proving Trials – R0. The FMEA includes the analysis associated with DPSI. The FMEA and proving trials reports are revised from ‘preliminary status’ to ‘final status’ after review, and completion of the trials program at which point both documents become R1.

D.7 COMPUTER SIMULATION AND OTHER SUPPORTING STUDIES

D.7.1 In this particular project, the power system provider GPS is also able to develop the:

- Mathematical model of the power system.
- Carry out the MBT test plan.
- Load balance.
- Harmonic distortion study.
- Transient stability study (crash sync, load acceptance & rejection).
- Live short circuit and ground fault test plan.

D.7.2 Computer simulations of the power and protection systems’ response to a comprehensive range of failure modes and loading conditions are shared with the stakeholders according to the EBCV[2] distribution table, prepared by CML, along with the other studies listed above. A preliminary MBT test program is prepared to prove the efficacy of the protection scheme and validate the computer simulation. The documents are distributed as:

- GPS- Kondor-Kai - MBT Test Plan – Rev 001.
- GPS- Kondor-Kai - Preliminary Power System Simulation – Rev 001.
- GPS- Kondor-Kai - Load Balance – Rev 001.
- GPS- Kondor-Kai - Harmonic distortion study – Rev 001.
- GPS- Kondor-Kai - Transient Stability (crash sync, load Acceptance & rejection) – Rev 001.
- GPS- Kondor-Kai - Live short circuit and ground fault test plan – Rev 001.

D.8 BATTERY ENERGY STORAGE SYSTEMS and ALTERNATIVE FUELS

D.8.1 Because both the SFT and post failure capability of DP system of the Kondor-Kai relies on stored energy in batteries, a detailed timeline from detection of reliance on battery power to safe termination of the DP operations (with adequate margins) must be developed. In this project, the domain knowledge required to establish this lies with the owner, and the pipelaying system provider. The shipyard is given the contractual responsibility of coordinating and publishing the output of a workgroup dedicated to this activity.

D.8.2 The results of this work were published by the shipyard as NHI-Kondor-Kai TIMELINE – Rev 001 and distributed according to the EBCV[2].

D.8.3 The issues associated with alternative fuels and their effects on DP System performance were analysed and documented as part of the DP System FMEA. They were further incorporated in DP ops manuals, CAMO and TAM where appropriate.

D.9 CLOSING THE GAP ON DP FAILURE MODE EFFECT ANALYSIS AND TRIALS

D.9.1 By this point in the project, the detailed design and preliminary FMEA was sufficiently complete to warrant performing the assurance processes which form the CTG process. The vessel owner, KMC commissioned their DP assurance advisors, CML to carry out a gap analyses and other checks using:

- MTS TECHOP (D-05 - Rev1 - Jan21) FMEA Gap Analysis
- MTS TECHOP (D-02 - Rev1 - Jan21) FMEA Testing
- OCIMF publication, DP FMEA Assurance Framework Risk-Based guidance (First Edition: 2020).

D.9.2 These were published by CML as:

- CML- Kondor-Kai – FMEA GAP – R001
- CML- Kondor-Kai – FMEA TRIALS GAP – R001
- CML – Kondor-Kai – OCIMF – R001.

D.9.3 The findings from the gap analyses were fed back to Omni Marine who updated their FMEA and proving trials to satisfy the requirements of the OCIMF DP FMEA assurance framework.

D.9.4 KMC had included the provision of an annual DP trials program in the contract with the shipyard and this was prepared by Omni Marine following the guidance in M190 ‘Code of practice for developing and conducting DP annual trials programmes July 2023’ and distributed to stakeholders as OM-Kondor-Kai - DP ANNUAL TRIALS – Rev 001. On receipt of this document, KMC commissioned CML to perform a gap analysis on it using TECHOP (O-02 - Rev1 - Jan21) Annual DP Trials and Gap Analysis and the findings were fed back to Omni Marine. CML published and distributed the annual DP trials gap analysis to stakeholders as CML-Kondor-Kai - ANNUAL DP TRIALS GAP – Rev 001.

D.10 EXECUTION OF TRIALS AND OTHER VALIDATION TESTING

D.10.1 By this point in the project, all parties have agreed that everything is ready for the vessel to undergo DP FMEA proving trials and associated validation testing (examples - live short circuit and ground fault testing and MBT). Any gaps in the FMEA and proving trials program have been closed. Findings from the FMEA process have been implemented and are ready for testing.

D.10.2 The sea trials/DP FMEA proving trials commence with Omni Marine onboard performing the DP FMEA proving trials for the shipyard with CML witnessing on behalf of the owner's team. Enerjet have their own resources onboard. GPS is performing the Model Based Testing and the live short circuit & ground fault testing.

D.10.3 At the end of the trials and validation testing, all findings are shared first with KMC by the shipyard. After KMC has reviewed them, they are shared with stakeholders according to the EBCV^2 distribution list by CML on behalf of the owner.

D.11 CLOSING THE GAP ON TRIALS AND VALIDATION TEST RESULTS

D.11.1 There is no formal assessment tool for this part of the process (as there is for identifying gaps in FMEAs and the proving trials program, etc.). The process is considered to be complete when any deficiencies of Category A have been addressed and proven by remedial testing if required and final versions of the reports are issued after the traditional round of comments by stakeholders.

D.11.2 In this project, Omni Marine and GPS issue the following reports (through the Shipyard) to CML who distribute them according to the EBCV^2 distribution table:

- OM-Kondor-Kai Final DP FMEA – R1.
- OM-Kondor-Kai Preliminary DP FMEA Proving Trials – R1.
- GPS-Kondor-Kai – MBT Test Plan – Rev 002.
- GPS-Kondor-Kai - Live short circuit and ground fault test results – Rev 002.

D.12 EBCV^2 DOCUMENTATION PACKAGE

D.12.1 When all concerns and comments are finally closed out in the comments round, CML packages the current revisions of all documentation generated for EBCV^2. The classification society, CBV, complete their processes to generate the various certificates, including the DP notation. CML completes the EBCV^2 checklist (see below). The KMC project team members responsible for each stage of the process sign off the documentation record and the KMC project manager signs off on the entire EBCV^2 process. CML then distributes the final documentation package to the stakeholders. At this point EBCV^2 is complete and following completion of the final protocols, the DP class 3 pipelayer Kondor Kai departs Nordic Heavy Industries shipyard for KVC's spool base for project mobilisation on its way to Enerjet's gas fields and a productive and DP incident free future.

STATEMENT OF DP SYSTEM ASSURANCE				
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements*	**Evidence Based Comprehensive Verification and Validation (EBCV[2])**			
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG - Assurance**
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**	**Project Responsible**
Redundancy Concept Philosophy Document	RCPD report for DP vessel	KMC-Kondor-Kai-RCPD – R001.	RCPD describes a viable, SFT DP System capable of being verified, validated and assured to class rules for the specified notations and any additional requirements.	AOC
	CTG – Seven Pillars Comparator	KMC-Kondor-Kai-RCPD – R001.	Seven Pillars comparator indicates intention to test all performance attributes and protective functions and no unnecessary common points	AOC
DP System FMEA	DP System FMEA report	OM-Kondor-Kai Preliminary DP FMEA – R0	Category A concerns closed? B's and Cs evaluated	DGG
	DP Control System FMEA	SM-DPCS FMEA RA	Conclusions compatible with overall DP System FMEA	DGG
	PMS & VMS FMEA	SM-PMS FMEA RA SM-VMS FMEA RA	Conclusions compatible with overall DP System FMEA	DGG
	Coordination Study	GPS-Kondor Kai - COORD – R01	Confirmed to support the DPRC	ANJ

STATEMENT OF DP SYSTEM ASSURANCE				
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements*	**Evidence Based Comprehensive Verification and Validation (EBCV[2])**			
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG - Assurance**
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**	**Project Responsible**
DP System FMEA	Computer simulation of power system and its protection	GPS- Kondor-Kai – MBT Test Plan – Rev 001 GPS – Kondor – Kai – Preliminary Power System Simulation – Rev 001	All modes of failure analysed in all configurations and protection proven to be fully selective – Supports WCFDI.	ANJ
	Load Balance	GPS- Kondor-Kai – Load balance – Rev 001	Aligns with WCFDI and PFC	ANJ
	Time to Terminate	NHI-Kondor-Kai TIMELINE – Rev 001	Is appropriate for the IM	BLP
	Harmonics Analysis	GPS- Kondor-Kai - Harmonic distortion study – Rev 001	Meets class requirement in all configurations and post worst case failure of harmonic cancelation features	ANJ
	Thruster FMEA – Fail Safe Condition	OM-Kondor-Kai Preliminary DP FMEA – R0	Thrusters fail safe proven by analysis and testing	DGG
	Transient Stability (crash sync, load Acceptance & rejection)	Transient Stability (crash sync, load Acceptance & rejection) – Rev 001	Power plant remains stable under all failure mode in all defined configurations	ANJ
	DP System FMEA Gap Analysis	CML- Kondor-Kai – GAP – R001	All gaps closed	DGG

STATEMENT OF DP SYSTEM ASSURANCE				
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements*	**Evidence Based Comprehensive Verification and Validation (EBCV^2)**			
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG - Assurance**
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**	**Project Responsible**
DP System FMEA	OCIMF DP FMEA Assurance Framework – Statement of Compliance	CML – Kondor-Kai – OCIMF – R001	Valid OCIMF statement of compliance	DGG
DP FMEA Proving Trials (inc. validation testing)	Proving trials document	OM-Kondor-Kai Preliminary DP FMEA Proving Trials – R0	All Category A concerns closed and Bs and Cs evaluated	DGG
	Model Based Testing for Power Systems	GPS- Kondor-Kai – MBT Test Plan – Rev 001	Confirms the efficacy of the protection coordination	ANJ
	Short Circuit and Ground Fault Test Report	GPS - Kondor-Kai - Live short circuit and ground fault test plan – Rev 001	Test method meets classification society and EBCV^2 requirements to proves the voltage dip ride though capability of the power plant and WCF	ANJ
	Proving Trials Gap Analysis	CML- Kondor-Kai – FMEA TRIALS GAP – R001	All gaps closed	DGG
Annual DP Trials	Annual DP Trials Program	OM-Kondor-Kai - DP ANNUAL TRIALS – Rev 001	A proforma is available for future use in the case of new builds which proves all the elements of performance, protection, and detection	DGG
	Annual Trials Gap Analysis	CML-Kondor-Kai - ANNUAL DP TRIALS GAP – Rev 001	All gaps closed	DGG

STATEMENT OF DP SYSTEM ASSURANCE				
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements*	**Evidence Based Comprehensive Verification and Validation (EBCV²)**			
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG - Assurance**
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**	**Project Responsible**
DP System Integration (DPSI)	RP- 0684 DP System Integration integrated within the DP FMEA (Typically)	OM-Kondor-Kai Preliminary DP FMEA – R0	All category A concerns closed (as part of FMEA)	DGG
EBCV² Documentation Package Assembled Post Trials	DP FMEA with DPSI	OM-Kondor-Kai Final DP FMEA – R1	There are no outstanding concerns at Category A	DGG
	DP FMEA Proving Trials	OM-Kondor-Kai Preliminary DP FMEA Proving Trials – R1	There are no outstanding concerns at Category A	DGG
	MBT Report	GPS- Kondor-Kai – MBT Test Plan – Rev 002	There are no outstanding concerns at Category A	ANJ
	Live Short Circuit and Ground Fault Report	GPS - Kondor-Kai - Live short circuit and ground fault test results – Rev 002	There are no outstanding concerns at Category A - Test results prove the voltage dip ride though capability of the power plant and WCF	ANJ

STATEMENT OF DP SYSTEM ASSURANCE					
Note: Where required, *acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements*		**Evidence Based Comprehensive Verification and Validation (EBCV²)**			
Colour Key	**All Concepts/Configurations**	**Closed Bus/Power Transfer**	**Hybrid Power**	**CTG - Assurance**	
Key Deliverable	**Substantiating & Supporting Documentation**	**Doc No. & Rev**	**Acceptance Criteria**		**Project Responsible**
EBCV² Documentation Package Assembled Post Trials	All other supporting reports are included in the final documentation package. These may also be at higher revision levels if the validation test results have revealed a need for them to be amended.	GPS-Kondor Kai - COORD – R01	Any concerns that could impact the single fault tolerance (SFT)and post failure DP capability of the DP System have been addressed and proven by validation testing where necessary		ANJ
		GPS- Kondor-Kai – MBT Test Plan – Rev 001 GPS – Kondor – Kai – Preliminary Power System Simulation – Rev 001			ANJ
		GPS- Kondor-Kai – Load balance – Rev 001			ANJ
		NHI-Kondor-Kai TIMELINE – Rev 001			BLP
		GPS- Kondor-Kai - Harmonic distortion study – Rev 001			ANJ

<table>
<tr><th colspan="5">STATEMENT OF DP SYSTEM ASSURANCE</th></tr>
<tr><td colspan="2">Note: Where required, acceptance criteria will include satisfying class comments in addition to any other contractually specified requirements</td><td colspan="3">Evidence Based Comprehensive Verification and Validation (EBCV²)</td></tr>
<tr><td>Colour Key</td><td>All Concepts/Configurations</td><td>Closed Bus/Power Transfer</td><td>Hybrid Power</td><td>CTG - Assurance</td></tr>
<tr><td>Key Deliverable</td><td>Substantiating & Supporting Documentation</td><td>Doc No. & Rev</td><td colspan="2">Acceptance Criteria</td><td>Project Responsible</td></tr>
<tr><td rowspan="2">EBCV² Documentation Package Assembled Post Trials</td><td>CTG - All concerns of category A from Validation testing addressed</td><td rowspan="2">There are no tools for formal assessment of this stage. Demonstration of adherence to the guidance is based on resubmission of the documentation, with relevant concerns cleared, accompanied by substantiating documentation.</td><td colspan="2" rowspan="2">Any concerns that could impact the single fault tolerance (SFT) and post failure DP capability of the DP System have been addressed and proven by validation testing where necessary</td><td>DGG</td></tr>
<tr><td>CTG Documentation Package Complete</td><td>DGG</td></tr>
<tr><td>Project Manager Sign Off</td><td>EBCV² Process and Package Completed</td><td colspan="3">DTR on behalf of KMC</td></tr>
</table>

Table D-1 - Example Statement of DP System Assurance

APPENDIX E VERIFICATION OF POWER SYSTEMS OPERATING WITH CLOSED BUS TIES WITH OWNERS' REQUIREMENTS FOR LOW IMPACT FAILURE EFFECT CONCEPT

E.1 INTRODUCTION

E.1.1 Background to technical verification

E.1.1.1 IMO MSC/Circ. 645 and MSC.1/Circ. 1580 both require that DP Class 3 power systems operating in configurations based on closed bus ties (common power system) have equivalent integrity to a power plant configured with open bus ties (isolated power systems).

E.1.1.2 There was no formal way of demonstrating equivalent integrity until the major classification societies developed DP notations and qualifiers specifically for this purpose. The Unified Approach to Verification, Validation and Assurance of Single Fault Tolerance (SFT) in DP vessels provides a roadmap that allows a vessel owner to demonstrate that a common power system has equivalent integrity to a DPRC based on isolated power systems.

E.1.1.3 This appendix provides additional detail on what such a process would entail. It also makes reference to compliance with the requirements of the LIFE concept which is described in the MTS DP Design Philosophy Document. This concept is used as an example of 'Vessel Owners' requirements which are additional to Class requirements and therefore must be verified independently.

Note: This example is intended as guidance and uses appropriate language and terminology. Those intending to convert this for use in contracts and specifications should consider whether this language is suitable for their needs and consider converting terms such as 'should' to 'shall' for example.

E.1.2 Verification criteria

E.1.2.1 Verification and validation (V&V) criteria are based on a combination of the following activities:

- Design compliance with spec derived from MTS DP design philosophy guidelines (LIFE concept).
- Analysis.
- Survey and testing.

E.1.2.2 The power plant will then be surveyed and tested at DP FMEA proving trials to confirm redundancy and failure response is correctly predicted by the FMEA.

E.1.2.3 The test results should also be used to confirm:

- validly of a computer model of the power plant.
- The computer model, so validated, will then be used to examine redundancy and failure response (of all power plant failure modes) in all intended operating configurations of thrusters, generators, switchboard configurations and load levels.
- The final step in the V&V process is the preparation of annual and periodic trials (proforma) designed to ensure that the integrity of the power plant is maintained throughout its operational life.
- The annual process is an essential element in detecting hidden failures that could defeat the DPRC.
- The periodic process involves reverifying and revalidation the DPRC by applying lessons learned, new knowledge and new methods to the verification of the original rules.

E.1.3 Applicable guidelines

E.1.3.1 Applicable guidelines would typically include:

- Those required by the owner in the vessel spec./contract with the shipyard.
- Those required by the classification society.
- Those required by the Unified Approach to the Verification, Validation and Assurance of the Single Fault Tolerance (SFT) of DP vessels.

There may be considerable overlaps in these lists.

E.1.4 Acceptance criteria

E.1.4.1 Design criteria The DP System design should comply with:

- Examples (ABS EHS-E, DNV DYNPOS (AUTRO – CBT & CBS))
- LIFE Concept

E.1.5 Failure criteria

E.1.5.1 The DP vessel should have a SFT design based on the provision of redundant DP equipment groups capable of maintaining position and heading on any bearing by developing surge, sway and yaw forces either together or in defined combinations.

- For Class DP notation there are no limitations in the definition of a single fault for class failure criteria.
- Class failure criteria include hidden failures and the effects of fire and flooding.
- For LIFE Concept, the definition of a single fault aligns with the class definition but excludes the effects of fire and flooding and faults acting directly on the bus bars of the HV switchboards.

E.1.6 Worst Case Failure and Redundancy Design Intents

E.1.6.1 The DP vessel is to have a defined redundancy design intent (RDI) and associated WCFDI for its appliable class notation and the LIFE Concept.

- **WCFDI CLASS** – No single failure as defined for classification society DP notation will have a greater effect on the vessel's ability to maintain position than the loss of one redundant DP equipment group.
- **WCFDI LIFE** – No single failure as defined by the LIFE concept will have a greater effect on the vessel's ability to maintain position than the loss of one thruster and/or one generator.

A class approved DP System FMEA for the relevant power system configurations will validate the RDI and prove that no defined single failure has effects of a severity exceeding those defined by the worst-case failure design intent(s).

1. The validated RDI shall be used, along with other information on power and thrust capability, to define a post WCF DP capability.
2. No defined single failure, shall lead to any of the following:
    a. A LOP or heading when the vessel is operated at or below the limits of its post failure DP capability.
    b. Failure effects exceeding the severity of the worst case failure design intent(s).
    c. The malfunction of equipment in more than the number of redundant groups identified in the DP System FMEA as being affected by a single failure.

E.1.7 Statement of assurance

E.1.7.1 All deliverables presented in support of this technical verification should include a statement of assurance indicating whether in the opinion of the authors the results presented within those reports supports the conclusion that the DP System satisfies the acceptance criteria listed in this appendix.

E.2 ANALYSIS

E.2.1 Power plant simulation & proof of fault ride-through capability

E.2.1.1 Reference can be made to the following documents for further information:

- MTS TECHOP (D-07 - Rev1 - Jan21) Proving Fault Ride -Through Capability of DP Vessels.

E.2.1.2 A time-domain computer simulation based on established electrical engineering principles and using proven commercially available software and methods will be created to demonstrate the ability of the vessel to maintain position and heading following a full range of fault conditions including all those power system failure modes listed in the DP System FMEA.

E.2.1.3 Fault conditions to be simulated will include, but are not limited, to the following:

- Combinations of bolted short circuit faults between phases and to earth.
- Combinations of arcing faults between phases and to earth.
- Unbalanced faults caused by broken conductors, faulty circuit breaker poles open or closed, or single phasing of motors.
- Fault with DC components, leading to transformer or generator saturation for example.
- Intermittent, recurrent faults including breakdown across circuit breaker poles when open.
- Generator fuel control system failures to insufficient, excess fuel and hunting.
- Generator excitation faults:
  - Insufficient excitation
  - Excess excitation
  - Hunting
- Severe mechanical failure in an online generator leading to loss of synchronisation.
- Inadvertent connection of a stopped generator.
- Crash synchronisation of an incoming generator.
- Crash synchronisation of two power supplies.
- The effects of simultaneous and sequential short circuits occurring on power supplies from redundant power systems feeding equipment subject to the effects of fire or flooding in a single compartment for HV and LV distribution.
- The effects of fire and flooding on control power and signals crossing the A60/WT boundary between redundant DP equipment groups.
- Failure of a thruster or large consumer to full power/thrust.
- Faults, for example – short circuit and earth fault, at a dual fed consumer on the LV distribution such as a crane.
- Maximum load acceptance and rejection from generators because of a single failure.

- The study will be validated by testing.
- The generator fault current decrement curve measured during testing should be compared to that used in the mathematical model and adjustments to predictions made if necessary.

E.2.1.4 It is expected that all power system failure modes and their associated protective functions will be accurately modelled including those in the generator and switchboard protection, engine safety system, thruster drives, IM equipment drives, DP control system, energy storage facilities and PMS where applicable.

E.2.1.5 Where functions are duplicated, such as in switchboard protection relays and dedicated generator protection, PLCs, both protective functions will be modelled.

E.2.1.6 It is intended that the studies cover the full range of operating conditions and power plant configurations. If, however, it is impractical for reasons of computing time to model every conceivable variation of failure, operating condition and failure mode, it is acceptable that the worst case scenarios (number of generators, thrusters and loading) are modelled for each failure mode provided sufficient studies and justification are provided to conclude that these are in fact the worst cases.

E.2.2 Harmonics analysis

E.2.2.1 Harmonics analysis should confirm that levels of Total Harmonic Distortion is below the level at which it represents a potential common mode failure. Typically, the single largest harmonic contribution should be less than 5% and 3% of the fundamental respectively in the following conditions:

- Worst case intact power plant condition.
- Worst case increases in harmonics due to a failure in the power plant.
- Worst case failure of harmonic cancellation features.

E.2.2.2 The study should confirm there are no resonance points which could be excited to cause a severe overvoltage condition.

E.2.3 Load balance

E.2.3.1 A comprehensive load balance calculation should be carried out demonstrating the active and reactive power supplied by the generators and the power available for thrust under the full range of intended operating configurations.

E.2.4 Load acceptance and rejection

E.2.4.1 A study should confirm that the worst case load acceptance and rejection caused by a failure anywhere in the power plant will not cause an unacceptable rise or fall in system frequency and voltage leading to undesired operation of protective functions.

- It is accepted that load shedding functions, for example thruster/drilling phase back, may operate to achieve this.

E.2.4.2 The results of the study should be confirmed by testing.

E.2.5 Protection coordination study

E.2.5.1 An overall protection coordination study should be produced demonstrating effective coordination between all protective functions located in various subsystems which may influence the failure response of the DP Systems. The studies will cover all intended system configurations including status of bus tie circuit breakers, open or closed, and number of thrusters and generators connected across the full range of anticipated system loadings. The subsystems would include but are not limited to:

- Engine safety and control system.
- Generator protection.
- Power distribution system protection at all distribution voltage levels.
- Power/energy management system.
- Battery management systems.
- DP control systems.
- Control system for thruster drives.
- Drilling control system.
- Thruster speed and azimuth closed loop control systems.

E.2.5.2 The study will be presented in a graphical format with supporting explanatory narrative which concludes upon the efficacy of the protection system, including primary and backup protection, across the full range of operating conditions.

E.3 FAILURE MODES AND EFFECTS ANALYSES

E.3.1 Specification

E.3.1.1 A failure modes and effects analysis and accompanying DP FMEA proving trials should be carried out meeting the requirements of the following:

- DNV RP D-102, FMEA of Redundant Systems – (2012 or later)
- OCIMF DP FMEA Assurance Framework – Risk-based Guidance 2020
- IMCA M166, Code of Practice on Failure Modes and Effects Analysis, (2024 or later)

E.3.2 DP System Integration

E.3.2.1 Unacceptable modes of failure associated with dependencies and controller authority with control system functionality should be addressed by application of DNV RP 0684 ‘DP System Integration’.

E.3.3 Model Based Testing

E.3.3.1 Model based or simulation-based testing should be performed on all protective functions in the power system upon which the redundancy concept relies for its single fault tolerance (SFT). All power plant failure modes from the FMEA should be modelled and protective functions tested not just those listed in the protection coordination study. The efficacy of the protection coordination study should be proven by a combination of live testing and MBT.

E.3.4 MTS DP FMEA and proving trials gap analyses

E.3.4.1 A gap analysis of the DP System FMEA and proving trials can be carried out following the guidance in the MTS TECHOPs listed below.

- TECHOP (D-05 - Rev1 - Jan21) FMEA Gap Analysis.
- TECHOP (D-02 - Rev1 - Jan21) FMEA Testing.

E.3.5 Equipment Manufacturer/Supplier’s Failure Mode Effect Analyses

E.3.5.1 Equipment vendors should provide failure modes and effects analysis of the following systems:

- ESD.
- F&G.
- PMS.
- VMS.
- Thruster control systems.

E.3.5.2 The FMEAs should be carried out in compliance with a recognised industry standard such as IEC 60812 or DNV RP D102, where there is a significant element of redundancy in the design.

E.4 SURVEY AND TESTING

E.4.1 Initial Survey and DP Failure Mode Effect Analysis Proving Trials

E.4.1.1 DP FMEA proving trials should be prepared following the guidance in:

- MTS TECHOP (D-02 - Rev1 - Jan21) FMEA Testing.
- MTS TECHOP (D-01 - Rev1 - Jan21) Addressing C³EI² to Eliminate Single Point Failures.
- DNV RU-SHIP Pt.6 Ch.3. Navigation, manoeuvring and position keeping.

E.4.1.2 The fault tolerance of DP Systems based on redundancy depends upon elements of:

- Performance.
- Protection.
- Detection.

E.4.1.3 Each test will attempt to prove the presence of one or more of the elements above with the expectation that such elements in the DP System will be tested.

E.4.1.4 Each test will include a cross-reference to the section of the FMEA which describes the elements of performance, protection and detection upon which fault tolerance depends.

E.4.1.5 Each test should be justified on the basis of the need to prove these elements, and the justification for doing so included in the 'Purpose' section of each test sheet.

E.4.2 Gap Analysis of DP Failure Mode Effect Analysis Proving Trials

E.4.2.1 The DP FMEA proving trials should be subjected to a gap analysis using the gap analysis tool in MTS TECHOP (D-02 - Rev1 - Jan21) FMEA Testing. Any gaps so identified should be closed.

E.4.3 Verification of performance

E.4.3.1 The following power plant performance tests will be carried out:

- All generators in one redundant group simultaneously to 100 % power in groups of two, (one engine room) for long enough for cooling system temperatures to stabilise.
- Thrusters to 100 % for long enough for cooling water temperatures to stabilise.

E.4.4 Verification of software revisions and protection settings

E.4.4.1 After commissioning and prior to commencement of the DP FMEA proving trials, a survey will be made to record the following software revision levels:

- DP control system.
- Engine control and safety system.
- Power/Vessel/Energy/Battery management systems.
- Generator Protection, (Fuel control and excitation control fault protection).
- Engine governors.
- Thruster variable speed drives.
- Automatic voltage regulators.
- Thruster control system.

E.4.4.2 After commissioning and prior to commencement of the DP FMEA proving trials, a survey will be made to record the following protection settings from the protection devices:

- DP control system related to power management.
- Power management system.
- Main switchboard relay protection settings, generators feeders and tie-lines.
- Engine control and safety systems.
- Automatic voltage regulator.
- Drilling/IM power system, interface to DP power systems.
- Thruster variable speed drives.
- Thruster control systems.

E.4.4.3 The protection settings, so recorded, should be compared with a record of the approved settings and referenced from the DP System FMEA.

E.4.5 Fault ride-through testing for short circuit and earth faults

E.4.5.1 Fault ride-through testing of short circuit and earth faults will be carried out on the main HV switchboards.

E.4.5.2 Reference can be made to the following document for guidance on how this type of testing can be performed:

- MTS TECHOP (D-07 - Rev1 - Jan21) A Method for Proving the Fault Ride-Through Capability of DP Vessels with HV Power Plant. The results from this testing program will be used to validate the results of the modelling work carried out. In particular, the results will be used to demonstrate that the mathematical model can accurately predict:
  - The fault current at all points in the power system.
  - The bus voltage recovery following the fault.
  - The current surge following recovery.
  - The correct operations of the protective functions.
  - The correct response of the drilling drives.

E.4.6 Fault ride-through testing for other faults

E.4.6.1 Realistic failure simulations will be carried out to demonstrate the effects of the following faults and the correct operation of protective functions. Where redundant protective functions are required, the primary and backup protection will be demonstrated:

- Generators fuel control system failure to insufficient and excess fuel and hunting.
- Generators excitation system failure to insufficient and excess excitation and hunting.
- Overload leading to phase back of drilling equipment.
- Overload leading to phase back of thrusters.
- Current imbalance associated with a negative phase sequence fault.
- Load acceptance and rejection due to single failures.

E.4.6.2 When testing the response of the power plant to overload, the effectiveness of the phase back system is to be tested by creating a significant step overload. For example, by tripping generators at high load from a power skew condition where one generator will be at high load and the others at low load or in reverse power.

E.4.6.3 Failure modes of control system signals should include, at least, the following:

- Fixed offset too high and too low.
- Slow drift.
- Step change.
- Out of range.

E.4.6.4 When testing the phase back of drilling systems, means will be provided to create a drilling load of sufficient magnitude to test drilling load shedding functions reliably.

E.4.7 Bus tie protection

E.4.7.1 Tests will be carried out to verify the correct operations of the following protection which opens the bus ties:

- Over and under voltage.
- Over and under frequency.
- Negative phase sequence.

E.4.7.2 In the case of earth fault and short circuit protection functions not tested by the fault-ride through test, short circuit and earth fault then the correct operation of these functions shall be proven by secondary injection methods.

E.4.8 Interlocks and configuration checks

E.4.8.1 Interlocks are used to prevent maloperation which could defeat redundancy or cause an unfavourable outcome.

- Interlocks shall be tested by non-destructive means.
- Automatic functions used to confirm the DP system is correctly configured should be tested.

E.4.9 Blackout recovery and ESD 0 recovery

E.4.9.1 Tests of the automatic blackout recovery system will be carried out on full auto DP with the vessel configured for CAM with closed bus ties and all thrusters online. Effective operation of the blackout recovery system will be demonstrated and repeated on each main bus individually when the plant is configured with open bus ties. Blackout will be initiated by a realistic fault condition and not by stopping the last connected generator.

E.4.9.2 Test to demonstrate effective recovery from activation of an all-vessel shutdown condition, ESD 0, will be initiated with the vessel operating on full auto DP with the power plant configured for CAM with closed bus ties, all generators and all thrusters online.

E.4.9.3 Tests of automatic blackout recovery should be conducted separately from tests intended to prove recovery from an all-vessel shutdown.

E.4.9.4 Means should be available to ensure safety in the event of a prolonged recovery, for example, anchors or tugs, as appropriate.

E.4.10 Inspection and thermos-graphic survey

E.4.10.1 A visual inspection of the HV switchboards will be performed after commissioning and testing to verify all test materials have been removed and the switchboards returned to operational condition.

E.4.10.2 Where possible, a thermos-graphic survey of the bus bars and connection points will be performed after commissioning to confirm the integrity of the switchboards.

- Inspections described in MTS TECHOP (D-07 - Rev1 - Jan21) section 8.10 should be carried out.

E.4.11 Annual Survey

E.4.11.1 Annual trials program - An annual DP trials program will be created based on the principles described in the following documents.

- MTS TECHOP (G-03 - Rev1 - Jan21) Continuous Trials for DP MODUs.
- IMCA M191 Guidelines for Annual DP Trials for DP MODUS.
- IMCA M190 Guidance for Developing and Conducting Annual DP Trials Programmes for DP Vessels.
- IMCA M225 Example Redundancy Concept and Annual DP Trials for a DP Class 3 Construction Vessel.

E.4.11.2 Trials will typically be subdivided into groups of tests that can be carried out:

- As part of planned maintenance.
- Between wells.

E.4.11.3 All protective functions, performance attributes and detection facilities upon which redundancy depends when operating in CAM shall be tested annually.

E.4.11.4 Protective functions which are only relied upon in TAM may be scheduled over a longer period, class and other regulatory requirements notwithstanding.

- This period should typically not exceed two years.
- Gap analysis of annual DP trials

E.4.11.5 The annual DP trials will be subjected to a gap analysis using the gap analysis tool in MTS TECHOP (O-02 - Rev1 - Jan21), Annual DP Trials and Gap Analysis. Any gaps identified should be closed.

E.5 PERIODIC SURVEY (5-YEARLY)

E.5.1 Continuous trials

E.5.1.1 It is expected that a well-prepared annual DP trials program will obviate the need for a dedicated periodic test program to be developed from first principles. However, it is expected that the periodic test will have the same focus as the initial survey and DP FMEA proving trials. It is expected that this opportunity will be used to apply new methods and lessons learned. Some exploratory testing may be added. It is associated with new knowledge, new methods and lessons learned. This is not to be taken as a requirement to repeat the original DP FMEA proving trial.

E.5.2 Fault ride-through testing and class survey requirements

E.5.2.1 Class requirements as part of the five-yearly survey will form part of the periodic survey including fault ride-through testing by a method acceptable to class.

E.6 DELIVERABLES

E.6.1 Summary

E.6.1.1 This section summarises the survey, testing, analysis and other reports which form the deliverables upon which this technical verification will be performed.

- Report on mathematical modelling of the power systems described in MTS TECHOP (D-07 - Rev1 - Jan21), section 8.2 ‘Presentation of Results’.
- Harmonics analysis.
- Load balance.
- Load acceptance and rejection study – may form part of item 1.
- Failure modes and effects analysis of the DP System.

- System Manufacturers' FMEAs
- Gap analysis of the DP System FMEA.
- DP FMEA proving trials report – Completed.
- Gap analysis of the DP FMEA proving trials.
- Record of software and protection setting verification.
- Test results from fault ride-through testing for short circuit and earth fault – may be incorporated with item 1.
- Test result from fault ride-through testing of other faults – may be incorporated with item 1.
- Post fault ride-through inspection test report.
- Annual DP trials program – pro forma.
- Periodic survey program – pro forma.

APPENDIX F APPLICATION OF EVIDENCE BASED COMPREHENSIVE VERIFICATION AND VALIDATION TO VESSELS IN SERVICE

F.1 WHEN TO CONSIDER APPLYING EVIDENCE BASED COMPREHENSIVE VERIFICATION AND VALIDATION TO A DP VESSEL IN SERVICE

F.1.1 EBCV^2 is primarily intended for use with newbuilds. However, there were frequent requests from participants at MTS workshops and other forums for advice on its application to DP vessels in service. This section explains some of the challenges associated with carrying out the processes within EBCV^2 on a vessel in service or undergoing a limited upgrade for which no extended out of service period is planned.

F.1.2 Vessel owners may elect to use all or part of the EBCV² process:

- To bring the verification, validations and assurance processes for an older DP vessel up to modern standards.
- When a significant change is made to the vessel's operating configuration, such as the adoption of a closed bus mode for the power plant.

F.1.3 EBCV^2 is a collaborative process involving several stakeholders as identified in the table of roles and responsibilities in APPENDIX B EBCV^2 Matrix of Deliverables and Guidance References. This collaboration is more easily accomplished when all OEMs and other stakeholders are committed to a newbuild program and contractual agreements are in place through the shipyard to satisfy the referenced rules, guidelines and recommended practices. On a vessel in service, the coordinated participation of these stakeholders would need to be arranged by the vessel technical owner.

F.1.4 The technical activities that make up the EBCV^2 process are:

- RCPD – Informed by C^{3}EI^2.
- FMEA.
- DPSI.
- Supporting Studies.
- Validation testing.
- CTG assurance tools used to confirm the efficacy of the V&V process.

F.2 REDUNDANCY CONCEPT PHILOSOPHY DOCUMENT

F.2.1 The redundancy concept of the DP System should be well described in the FMEA; however, considerable progress has been made in the past decade in understanding the impacts associated with common points, cross connections, external interfaces and influences. Applying new knowledge and methods to the analysis of the DP system may reveal many opportunities to improve station keeping integrity without undue burden.

F.2.2 The Seven Pillars comparator tool, provided in the RCPD TECHOP, can help to understand the degree to which the DP System could be compromised by common points and also help identify the changes that could be implemented to reduce it and the mitigating measure and validation testing required (if it must be retained).

F.2.3 Integrating elements of the RCPD into an introductory section to the DP System FMEA may be a reasonable alternative when modernisation of the FMEA and minimal but necessary remedial work is the primary objective. A separate document may be warranted if a more extensive upgrade or conversion is planned and there is a need to communicate a new redundancy concept to OEMs, integrators and other stakeholders.

F.3 FAILURE MODES AND EFFECTS ANALYSIS

F.3.1 FMEA – Updating an FMEA on a vessel in service is a well-established process. Updates to FMEAs are carried out as needed to address changes and not later than every five years.

- Where an FMEA is done to address changes to the DP System, it is usually straightforward to get the required information from the OEMs involved, as they will have engineering teams involved in the upgrade process.
- Updating an FMEA to bring the analysis in line with modern practice for FMEAs can be more challenging as it may require the VTO to request information on systems where there is no current OEM involvement. The VTO may have to rely on their relationship with the OEM through service agreements or establish new arrangements for this purpose. Equipment obsolescence can cause additional complications.
- The desk top analysis needs of a DP FMEA provider are generally limited to requesting schematics and answers to technical queries. Greater challenges may be experienced when it comes to organising OEM support for testing associated with new analysis and compensating provisions.

F.4 SUPPORTING STUDIES FOR DP FAILURE MODE AND EFFECT ANALYSES

F.4.1 If any of the required supporting studies are missing, it will generally be necessary for the VTO to commission those from a suitably qualified resource. Many power system OEMs can offer standard studies for protection coordination, harmonics, load balance and so on.

F.4.2 Mathematical modelling of a closed bus power plant is likely to present the most significant challenge such as gathering data on the electrical characteristics of power system components, including but not limited to, generators, transformers, motors, engines, automatic voltage regulators and governors, etc. Experienced modelling service providers are typically able to overcome this using their experience and database of similar equipment which have characteristics close enough to serve the intended purpose. Models exist for standard IEC and ANSI protection functions. Bespoke protection such as Advanced/Additional Power System Protection (ASPS) may require OEM support.

F.5 TESTING

F.5.1 Carrying out tests to validate the conclusions of supporting studies and FMEAs requires vessel out of service time. The risk of equipment damage from properly prepared tests is low but not zero and this should be borne in mind when selecting an appropriate time in the vessel's operational program to carry out such tests. Arrange to have OEM support and critical spare parts available onboard.

F.5.2 Fault Ride-Through, live short circuit and ground fault, testing is one aspect of the EBCV[2] process that needs the most effort and pre-execution planning on a vessel in service. Such activities may become more common as the drive to improve GHG emissions encourages the adoption of closed bus, common power system configurations. The VTO may elect to engage a suitably qualified engineering resource to assess the design of the power plant and its protection system to determine whether they are suitable for such configurations and what remedial work is required to bring the power plant and its protection scheme up to a suitable standard. It may also be possible to provide an assessment of the suitability of the power plant to undergo the stresses of fault ride-through testing.

F.5.3 The DP notations of the relevant classification society will dictate the minimum test requirement. EBCV^2 for newbuilds encourages the use of live short circuit and ground fault testing, where practical, even if it is not required by class. This test method has proven to be highly effective in revealing shortcomings in fault ride-through capability. In the case of EBCV^2, applied to vessels in service, the power plant may not have been designed with live short circuit and ground fault testing in mind even though it is approved for operation in closed bus configurations. In theory, such a power plant should be capable of withstanding the effects of a short circuit fault, but the lack of validation testing will undoubtedly introduce a degree of uncertainty about the suitability of the power plant to undergo such testing. It is acknowledged that full adherence to all parts of EBCV^2 may not be practical on vessels in service. The decision to omit live short circuit testing or adopt alternative test methods to prove the fault ride-through capability of closed bus power systems may influence external assurance processes when considering if the vessel is suitable for closed bus CAM. Even with such limitations it is possible to benefit from implementing the EBCV^2 process if only for the rigor and oversight it introduces into the V&V process.

F.6 MODEL BASED TESTING

F.6.1 Model based testing can in theory be applied to any system. It is similar in concept to HIL Testing where control system was tested using a DP vessel model or a power plant model. In the context of EBCV^2, use of MBT is limited to proving the efficacy of the power systems protection scheme to support a conclusion of SFT in closed bus power systems. In particular, it is used to supplement live testing and traditional test methods to extend the range of test condition and scenarios without using the DP systems power plant as a test set. It may make use of the same power plant model developed for other purposes.

F.6.2 Model Based Testing requires considerable preparation time and initial engineering effort. Once established it can be used in Annual DP trials and Periodic Revalidation with much reduce effort. The complexity of the test harness to the main switchboards depends on the type of overcurrent and generator protection being used. Power systems using load sharing in uncompensated droop with time graded, rather than differential or direction protection, is much simpler to test.

F.7 DP SYSTEM INTEGRATION (RP-0684)

F.7.1 DPSI arguably requires more commitment from control system OEMs than is required by the traditional DP FMEA process. Completing the information exchange templates which allow the DP FMEA provider to understand and assess the influence of the various controller authorities will involve the OEM in some effort for which they will likely expect compensation. It may also require the availability of engineers/programmers familiar with any vessel specific software functionality.

F.8 ASSURANCE ACTIVITIES

F.8.1 The CTG process for EBCV^2 may in fact be the starting point when applying it to vessels in service. Several gap analysis tools are available to assess the scope and depth of the analysis in key DP documentation. The results from tools such as the MTS DP FMEA gap analysis tool or the heat map generators OCIMF DP FMEA Assurance may prove insight into the scope and depth of the remedial work required to both the analysis and the DP Systems itself.

F.9 SUMMARY

F.9.1 The benefits and burden of applying EBCV^2 to a DP vessel in service will vary depending on:

- The needs of the VTO.
- The state of the original V&V documentation.
- The extent of any upgrades or remedial work.
- The anticipated power plant configuration (open or closed bus ties).
- The nature of the redundancy concept (well segregated or heavily integrated).

F.9.2 Table F-1 provides a summary of the activity, anticipated burden and application of the various elements of EBCV^2 to a DP vessel in service.

Table F-1 Evidence Based Comprehensive Verification and Validation - Activity Burden & Application to DP Vessels in Service

Activity		Burden	Application	Remarks
RCPD – Informed by C^{3}EI^2		Low	All	An introductory section in the DP FMEA may be preferred unless the intention is to communicate a new concept to OEMs.
FMEA		Low	All	Established process typically Low burden but Medium if original FMEA is of poor quality.
DPSI		Medium	All	OEM commitment required.
Supporting Studies	Mathematical modelling	Medium	Closed bus	To be commissioned by VTO.
	Other	Low	All	No particular challenges.
Validation testing	SC & GF	Medium	Closed bus	Evaluation and preparation required.
	Other	Low	All	No particular challenges.
	MBT	High	Closed Bus	Potentially long lead time.
CTG		Low	All	Gap analyses are a reasonable starting point for a vessel in service.