TECHNICAL AND OPERATIONAL GUIDANCE (TECHOP)

TECHOP_GEN_01_(POWER PLANT COMMON CAUSE FAILURES)

SEPTEMBER 2012

CONTENTS

1 INTRODUCTION

1.1 PREAMBLE

1.1.1 The Guidance documents on DP (Design and Operations) were published by the MTS DP Technical Committee in 2011 and 2010, Subsequent engagement has occurred with:

- Classification Societies (DNV, ABS).
- United States Coast Guard (USCG).
- Marine Safety Forum (MSF).

1.1.2 Feedback has also been received through the comments section provided in the MTS DP Technical Committee Web Site.

1.1.3 It became apparent that a mechanism needed to be developed and implemented to address the following in a pragmatic manner.

- Feedback provided by the various stakeholders.
- Additional information and guidance that the MTS DP Technical Committee wished to provide means to facilitate revisions to the documents and communication of the same to the various stakeholders.

1.1.4 The use of Technical and Operations Guidance Notes (TECHOP) was deemed to be a suitable vehicle to address the above. These TECHOP Notes will be in two categories:

- TECHOP_ODP.
- TECHOP_GEN.

1.2 TECHOP_ODP

1.2.1 Technical guidance Notes provided to address Guidance contained within the Operations, Design or DP Personnel

1.2.2 The TECHOP will be identified by the following:

TECHOP_ODP_SNO_CATEGORY (DESIGN (D) OPERATIONS (O) DP PERSONNEL (P).

- EG 1 TECHOP_ODP_00_(O)_(HIGH LEVEL PHILOSOPHY).
- EG 2 TECHOP_ODP_02_(D)_(BLACKOUT RECOVERY).

1.3 TECHOP_GEN

1.3.1 MTS DP TECHNICAL COMMITTEE intends to publish topical white papers. These topical white papers will be identified by the following:

TECHOP_GEN_SNO_DESCRIPTION.

- EG 1 TECHOP_GEN_00 (TECHOP GUIDANCE).
- EG 2 TECHOP_GEN_02-(POWER PLANT COMMON CAUSE FAILURES)

1.3.2 TECHOP as described in 1.2 and 1,3 above will be published as relevant and appropriate. These TECHOP will be written in a manner that will facilitate them to be used as standalone documents.

1.3.3 Subsequent revisions of the MTS Guidance documents will review the published TECHOPs and incorporate as appropriate.

1.3.4 Communications with stakeholders will be established as appropriate to ensure that they are notified of intended revisions. Stakeholders will be provided with the opportunity to participate in the review process and invited to be part of the review team as appropriate.

1.4 MTS DP GUIDANCE REVISION METHODOLOGY

1.4.1 TECHOP as described above will be published as relevant and appropriate. These TECHOP will be written in a manner that will facilitate them to be used as standalone documents.

1.4.2 Subsequent revisions of the MTS Guidance documents will review the published TECHOPs and incorporate as appropriate.

1.4.3 Communications with stakeholders will be established as appropriate to ensure that they are notified of intended revisions. Stakeholders will be provided with the opportunity to participate in the review process and invited to be part of the review team as appropriate.

2 SCOPE AND IMPACT OF THIS TECHOP

2.1 SCOPE

2.1.1 TECHOP_GEN_01_(POWER PLANT COMMON CAUSE FAILURES). The subject of common cause failures affecting DP systems is an extensive one. This Techop provides some general discussion on a wide range of common cause failure modes affecting DP systems that can often be overlooked in poor quality DP FMEAs. More detailed discussion is limited to a smaller group of failure modes related to generator fuel and excitation control faults and the severe voltage dips associated with short circuit faults.

2.1.2 Many common cause / common mode failures are capable of causing effects leading to loss of position, loss of all thrusters or blackout in any power plant configuration thus operating the power plant or as two or more independent power systems (busties open) does not provide comprehensive protection again these failure modes and designers should be aware of these failure modes so that they can be properly addressed in the redundancy concept.

2.2 IMPACT ON PUBLISHED GUIDANCE

2.2.1 None

3 CASE FOR ACTION

3.1 WIDE VARIATION IN QUALITY AND SCOPE OF DP FMEAS

3.1.1 All dynamically positioned vessels of DP Equipment Classes 2 & 3 are required to be single fault tolerant in respect of defined failure criteria appropriate to the equipment class. There have been a significant number of DP incidents related to a group of common cause failure modes that affect redundant power systems in various ways.

3.1.2 This group of failure modes can be overlooked or poorly analysed in poor quality DP FMEAs. They are capable of affecting the station keeping capabilities of DP vessels operating with independent power systems (open busties) or a common power system (closed busties). It is significant that some FMEA providers find difficulty in properly evaluating these aspects of DP power system design compared to marine auxiliary systems for example. In general, a history of poor design combined with weak FMEA has allowed these failure modes to prevail.

3.2 RECOMMENDED ACTION

3.2.1 Vessel designers for power generation & distribution and other FMEA stakeholders should review the design of the vessel against the guidance in this TECHOP to determine whether the DP system is vulnerable to loss of position and heading caused by the common cause failures described below.

4 SUGGESTED IMPLEMENTATION METHODOLOGY

4.1 INTRODUCTION

4.1.1 The purpose of this TECHOP is to help designers and analysts for DP Class 2 and DP Class 3 vessels to identify deficiencies in the design of the DP systems that makes it vulnerable to these types of failures.

4.2 GENERAL COMMON CAUSE FAILURES

4.2.1 Typical common cause failures affecting DP systems include:-

- Common control system power supplies accepted on the basis that generators and thrusters fail ‘as set’ on loss of power. However, failure to low voltage is not analysed or tested and causes all generators and thrusters to trip
- Common backup supplies to all generator and thruster control systems which fail to elevated voltage damaging control systems leading to loss of position.
- Failing to provide excitation support for generators causes complete system blackout when generators are unable to provide enough fault current to clear a short circuit fault
- Severe voltage dips associated with clearing short circuit faults from common power systems
- Inappropriate design of earth fault protection which is not fully selective
- Specifying inappropriate generator and power distribution system protection that is not selective and causes total blackout when the fault it is designed to act upon occurs.
- Protection relays left programmed with default settings and not those within the approved coordination study
- Protective functions in thruster drives cause the drive to trip (or loss of DP ready signal) when the propeller regenerates power to the drive.
- High levels of power system transients and harmonic distortion
- Basing all blackout protection on the assumed rated power (kW) capability of generators and failing to prove the generators are capable of rated capacity
- Inadequate load acceptance and rejection performance in generators leading to unacceptable frequency excursions and power plant malfunction.
- Failing to consider the effects of poor power factor in power plant design
- Environmental issues related to temperature and humidity levels of sensitive equipment locations. Provision of redundant HVAC and ventilation
- Oil mist detectors for engines operating spuriously in some environmental conditions
- Fuel contamination
- Combustion air contamination
- Blockage or fouling of common cooling water systems
- Common software errors in redundant systems using identical controllers and software.
- Common vessel sensor principles
- Inappropriate combinations of position reference system principles

4.3 SPECIFIC FAILURES IN DIESEL ELECTRIC POWER PLANT

4.3.1 Section 4.2 discusses the wide variety of common cause failures that can affect DP systems and may be overlooked in poor quality FMEAs. The discussion that follows considers a subset of these related to generator control systems and the reaction of consumers to power system transients. Further information on these can be found in the MTS DP Vessel Design Philosophy Guidelines – Part 2 Sections 9, 10 & 11.

4.3.2 Common cause failure mode related to generators and power distribution faults.

- Generator excitation control faults – Severe reactive power imbalance – (over / under voltage)
- Generator fuel control faults- severe active power sharing imbalance (over / under frequency)
- Broken conductors and single phasing
- Severe harmonic distortion and transient phenomena
- Severe voltage dips associated with clearing short circuit faults anywhere on the power generation level or in the lower voltage distribution system
- Overload / overcurrent due to loss of generating capacity
- inrush transients
- Under frequency caused by overload
- Over and under frequency cause by inadequate load acceptance and rejection.
- Earth faults
- Internal and external common cause failures such as fuel and combustion air contamination
- For DP Class 3 vessels the colocation of non DP related consumers can introduce a common point into the power system design even though there is no electrical connection between equipment. Fire or flood damage can cause voltage dips on independent power systems serving the common space thus each independent power systems must have sufficient voltage dip ride through to prevent the malfunction of generators, thrusters and other essential consumers.

4.3.3 Each of these failure modes is capable of causing a severe power systems malfunction including loss of all thrusters and/or blackout. Power plant malfunction is typically caused by the failure mode adversely affecting the operating point of healthy generators such that they trip on their own protective functions. Thruster drives and service transformers may also trip on their own protection.

4.4 DESIGNING A FAULT TOLERANT POWER SYSTEM

4.4.1 A common power system configuration is often adopted when carrying out less critical tasks on DP. This configuration is referred to as TAM (Task Appropriate Mode). Although the level of station keeping integrity accepted for such activities is lower than that required for CAM (Critical Activity Mode) both modes must be fully fault tolerant and analysed in the class approved DP FMEA (all modes if there are several).

4.4.2 Figure 1 provides a graphical representation of typical HV power system components and their failure modes. Power plant designers should consider these when developing a fault tolerant power system. Although many of these failure modes can be mitigated by operating the power plant as two or more independent power systems a partial blackout is now more likely to occur because of the change in the ratio of generator capacity to system load. Designers should consider the benefits of mitigating these failure modes even in open bus configuration to reduce the number of failures than can lead to total loss of redundancy. If a common power systems configuration is used (closed bustie) all failure modes should be adequately mitigated to achieve full fault tolerance.

4.4.3 Two recent developments have combined to improve confidence in the fault tolerance of common power systems for TAM:

- Live short circuit and earth fault testing.
- Advanced Generator Protection.

4.4.4 Advanced Generator Protection has become the generic name for a collection of protective functions that is designed to identify and isolate generator faults not addressed by traditional generator protection. It is also the name given to the product of one manufacturer of such integrated protection systems. See TECHOP_ODP_03_(D)_(EVALUATION OF PROTECTION SYSTEMS) for further details.

4.4.5 Live short circuit and earth fault testing of power plants operating as a single common power system has become more prevalent. Test results confirm the value of such tests in revealing design flaws and commissioning errors that cannot be easily revealed by other means.

4.5 TESTING THE POWER SYSTEM

4.5.1 It is essential that a comprehensive test program is developed to prove the effectiveness of the mitigating measures applied to ensure fault tolerance. Tests should be carried out in a manner that realistically recreates the failure modes that the protection is designed to detect.

4.5.2 Many of these tests will require the participation of the equipment manufacturers to prepare and carry out the tests. The overall test methodology should be devised by the FMEA provider which should also review the test method provided and formally confirm they satisfy the original testing intent.

4.6 CONCLUSION

4.6.1 **General common cause failures:** There are a wide variety of common cause failures that can affect the operation of DP related systems in any power plant configuration. Designers should consider these in the preparation of redundancy concepts. Designers and other DP FMEA stakeholders should be aware that these failure modes can be overlooked in poor quality FMEAs.

4.6.2 **Specific common cause failures**: A DP power plant operated as a common power system is vulnerable to a range of failure modes not addressed by traditional protection schemes. Solutions are available from a range of manufactures and power system designers. DP FMEA practitioners should familiarise themselves with the full range of power system failure modes and ensure they are adequately mitigated by effective protection and proven by testing.

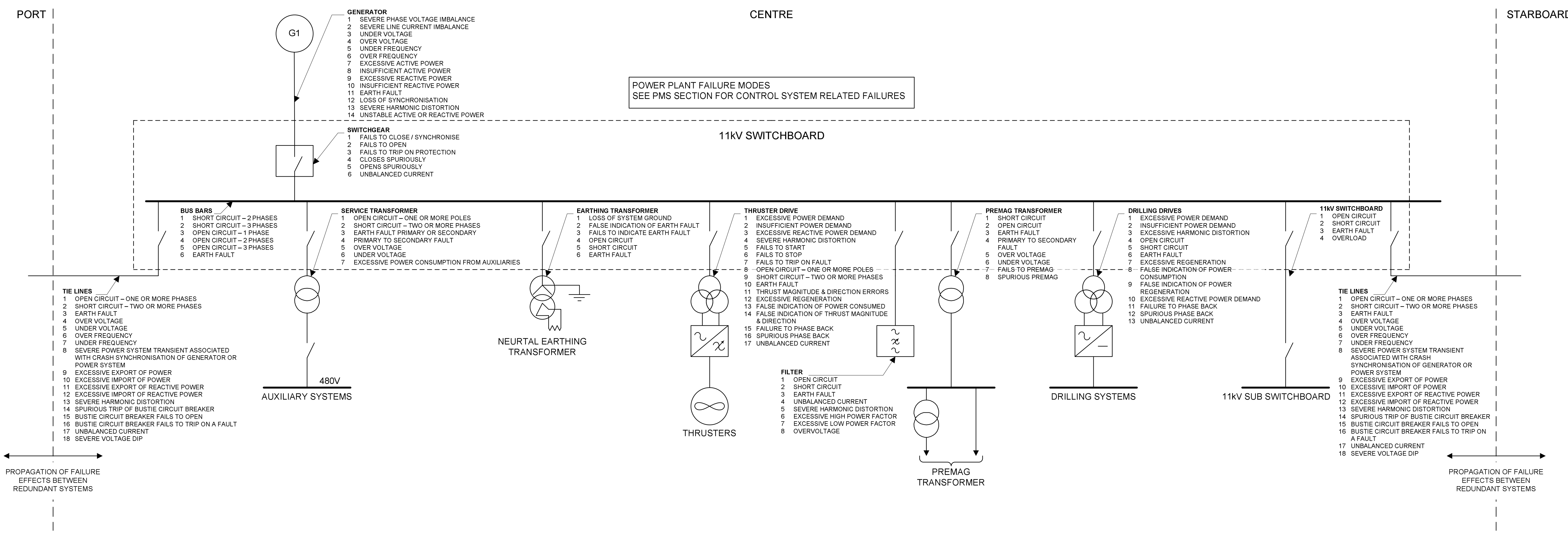

Figure 1 Typical HV power generation and distribution systems components and their failure modes

5 MISCELLANEOUS

Stakeholders	Impacted	Remarks
MTS DP Committee	X	To track and incorporate in next rev of MTS DP Operations Guidance Document Part 2 Appendix 1. Communicate to DNV, USCG, Upload in MTS website part
USCG	X	MTS to communicate- FR notice impacted when Rev is available
DNV	X	MTS to Communicate- DNV RP E 307 impacted
Equipment vendor community	✓	MTS to engage with protection suppliers
Consultant community	✓	MTS members to cascade/ promulgate
Training institutions	X	MTS members to cascade/ promulgate
Vessel Owners/Operators	✓	Establish effective means to disseminate information to Vessel Management and Vessel Operational Teams
Vessel Management/Operational teams	✓	Establish effective means to disseminate information to Vessel Operational Teams