
# TECHNICAL AND OPERATIONAL GUIDANCE (TECHOP)

# TECHOP (D-04 - Rev1 - Jan21)

# EVALUATION OF PROTECTION SYSTEMS

# JANUARY 2021

# DISCLAIMER

The information presented in this publication of the Dynamic Positioning Committee of the Marine Technology Society ('DP Committee') is made available for general information purposes without charge. The DP Committee does not warrant the accuracy, completeness, or usefulness of this information. Any reliance you place on this publication is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on this publication by you or anyone who may be informed of its contents.

# CONTENTS

# 1 INTRODUCTION

## 1.1 PREAMBLE

1.1.1 The guidance documents on DP (Design and Operations and People) were published by the MTS DP Technical Committee in 2011, 2010 and 2012, respectively. Subsequent engagement has occurred with:

- Classification Societies (DNV, ABS)
- United States Coast Guard (USCG)
- Marine Safety Forum (MSF)
- Oil Companies International Marine Forum (OCIMF)

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 and a 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 the following categories:

- General TECHOP (G)
- Design TECHOP (D)
- Operations TECHOP (O)
- People TECHOP (P)

## 1.2 TECHOP NAMING CONVENTION

1.2.1 The naming convention, TECHOP (CATEGORY (G / D / O / P) – Seq. No. – Rev.No. – MonthYear) TITLE will be used to identify TECHOPs as shown in the examples below:

Examples:

- TECHOP (D-01 - Rev1 - Jan21) Addressing $C^3EI^2$ to Eliminate Single Point Failures
- TECHOP (G-02 - Rev1 - Jan21) Power Plant Common Cause Failures
- TECHOP (O-01 - Rev1 - Jan21) DP Operations Manual

*Note: Each Category will have its own sequential number series.*

## 1.3 MTS DP GUIDANCE REVISION METHODOLOGY

1.3.1 TECHOPs 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.

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

1.3.3 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 This TECHOP provides information on:

- The use of protective functions in fault tolerant DP systems.
- The importance of separation between control, monitoring and protection.
- Classification of protective functions.

## 2.2 IMPACT

2.2.1 This TECHOP impacts the DP Vessel Design Philosophy Guidelines Part II Section 9.7.12.

# 3 CASE FOR ACTION

## 3.1 THE ROLE OF PROTECTIVE FUNCTIONS

3.1.1 The design of fault tolerant dynamic positioning system is heavily dependent on the use of protective functions to ensure that:

- Equipment fails safe from both a DP perspective and from a personnel safety perspective.
- Faulty equipment is isolated before failure effects cause malfunction of other redundant systems to which the faulty equipment may be connected.
- There are realistic limits on data used for DP control systems and power management calculations.

## 3.2 RECOMMENDED ACTION

3.2.1 DP vessel designers should carefully evaluate protective functions upon which redundancy depends to determine whether the required level of protection is actually achieved and that the protective function does not represent a single point failure.

# 4 SUGGESTED IMPLEMENTATION METHODOLOGY

## 4.1 CLASSIFICATION OF PROTECTIVE FUNCTIONS

4.1.1 This TECHOP deals primarily with a group of protective functions intended to improve the reliability of DP power plant when configured as a common power system. These protective functions are collectively known within the DP community as Advanced Generator Protection even though this term officially refers to the product of one manufacturer.

4.1.2 Advanced Generator Protection is designed to identify and isolate a range of power plant faults not addressed by traditional generator protection and which are capable of defeating the redundancy concept of diesel electric DP power systems.

4.1.3 Classification society rules for DP equipment classes 2 & 3 have always required that power systems be fully fault tolerant but certain types of failure modes affecting power plant configured as single power systems were routinely overlooked.

4.1.4 Most of the major DP electrical and control systems vendors now offer some form of advanced generator protection which may be branded with a variety of proprietary names. As AGP has become more widely known and appreciated within the DP community the number of vendors now offering similar products continues to increase. The various systems on offer have varying degrees of complexity and sophistication and effectiveness.

**4.1.5 Protection systems or extended control function: -** Some systems are marketed as supervisory or extended control functions rather than protection systems. In general, ‘control systems’ are designed to deal with errors introduced in the normal operation of a systems and ‘protection functions’ are designed to deal specifically with the effects of faults. Thus, these systems are in realty protection systems designed to prevent blackouts. Whether such systems are actually classified as ‘protection’ or ‘supervisory’ systems is not important in practical terms. What is important is that the established principles and good practice associated with the design of control and protection systems are followed to ensure the required level of protection is achieved.

## 4.2 GOOD PRACTICE IN THE DESIGN OF CONTROL, MONITORING AND PROTECTIVE FUNCTIONS

4.2.1 The following are important elements in the design of any DP power plant:

- Control.
- Monitoring.
- Protection.

4.2.2 These elements must be as independent as possible for the following reasons:

- Failure of automatic control should not render inoperative monitoring functions which allow the operator to assess the operational condition of the power plant. Thus, failure of control functions should not prevent the operation of alarms and indication necessary to understand and evaluate the extent of the failure effect caused by the control system fault.
- Similarly, failures in control systems should not render ineffective protective functions specifically designed to deal with the effects of such control system failures. Therefore, good practice requires that control, monitoring and protection functions are as independent as possible.

4.2.3 The advent of distributed automation systems has blurred the distinction between control, monitoring and protection to some degree but classification society rules for automation and other control systems do make the distinctions and often require the necessary independence. For example, where the automation system provider supplies the engine control and monitoring functions for diesel engines and the engine safety systems it may be acceptable to collocate them with the same control cabinet but the safety system element must have independent processors, I/O and power supplies such that it will continue to protect the engines in the event that the control system fails. If the safety system fails, the operator will receive an alarm to indicate the failure and still be able to observe that the engine is functioning safely and normally until it can be shut down manually.

4.2.4 This principle of independence between control and protection should be extended to all other systems that form part of the DP redundancy concept.

4.2.5 In the case of redundant control systems protective functions may be implemented within the same software as the control functions. In such cases the necessary level of independence can be achieved by the use of cross-checking or voting functions in which one or more redundant control systems supervises the operation of the other and the faulty unit may be brought to the attention of the operator by difference alarms or by rejecting the output from the erroneous systems on the basis of median tests or other methods. Such features are difficult to implement reliably in non-redundant systems.

## 4.3 THE DISADVANTAGES OF COMBINING PROTECTION AND CONTROL

4.3.1 In some cases, non-redundant control systems contain protective functions. For example, an engine governor may have a circuit which detects a wire-break in the speed pick-up circuit and sets the governor to zero fuel. Such protective elements in control systems are valuable but it may not be prudent to rely entirely on integrated protection systems to deal with faults within a control system itself. For example, if a power management system uses the same I/O and power transducers to control load sharing and also to detect load sharing imbalance it may be possible for a faulty transducer or the I/O interface to fail in such a way that it creates a load sharing imbalance. The same fault may also render the load sharing imbalance protection ineffective.

4.3.2 The proliferation of vendors offering a form of advanced generator protection or functions intended to meet the requirements for fault tolerance in DP power plant has brought a range of products onto the market which offer significantly different levels of protection and independence between control and protection functions.

4.3.3 This range could be broadly categorised by:

- Methods of detecting the faulty generator.
- Levels of protection function redundancy.
- Independence from control systems.

4.3.4 Method of identifying the faulty generator.

- Distributed systems which make an independent assessment of a generator’s health based solely on data derived from the faulty generator.
- Systems which determine the faulty generator by comparing its performance with that of the online generators.
- System using a combination of these methods.

4.3.5 Levels of redundancy in the protection scheme.

- Systems which create extensive protection redundancy by providing functions which back-up the traditional generator protection and which open the busties if the protection function fails to disconnect the faulty generator.
- Systems which only provide those protection functions that are not provided by traditional generator protection.
- Systems which cannot identify the faulty generator but open the busties for any fault likely to destabilise the entire power system.

4.3.6 Independence from control functions.

- Hardware based systems with independent processors, power supplies and transducers.
- Hardware extensions to the power management systems using independent processors, I/O and transducers.
- Software functions within the power management system using the same hardware and transducers.

## 4.4 REVIEW OF DESIGNS AND PROPOSALS

4.4.1 Power plant designers should be aware of this difference when specifying a particular system or reviewing proposals to provide such functions and carefully determine whether the system on offer meets their requirements for protection systems on which the fault tolerance of the DP power plant depends.

4.4.2 Designers should also recognise the possibility that some providers do not have the necessary levels of competence to correctly specify appropriate protective functions to deal with the failure modes of concern.

# 5 MISCELLANEOUS

| Stakeholders | Impacted | Remarks |
|---|---|---|
| MTS DP Committee | ✓ | To track and incorporate in next rev of MTS DP Operations Guidance Document Part 2 Appendix 1.<br>Communicate to DNV, USCG, Upload in MTS website part. |
| USCG | ✓ | 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. |