MTS DP Subcommittee for Learnings from Incidents and Insights

LEARNINGS FROM INSIGHTS MTS DP SUBCOMMITTEE FOR LFIS LFI(n) 002/26

PERIODIC TESTING CAN BE THE ONLY BARRIER WHEN THE FAILURE MODE DISABLES THE ALARM INTENDED TO REVEAL IT

This LFI(n) highlights that an alarm may share dependencies with the equipment or condition it is intended to monitor. Where a credible failure can also disable or suppress its associated alarm, periodic functional testing may be the only effective barrier capable of revealing the concealed condition before a further failure results in loss of position.

Why this Learning Is Being Issued

A DP vessel was conducting its annual DP trials when it unexpectedly lost position. The 24 V DC power from each redundant supply passed through a DIN-rail-mounted module that also performed the associated supply monitoring and alarm function. One 24 V DC supply was already unavailable, but no alarm had been generated. When the remaining supply was interrupted during the trial, the DP control-system cabinet lost its 24 V DC power and the vessel lost position. Before the trial, the vessel had therefore been conducting DP operations with an undetected loss of power-supply redundancy.

Inspection identified that the DIN-rail-mounted module through which the 24 V DC power passed, and which also monitored the condition of the supplies, was partially displaced and not fully clipped into the DIN rail. The displaced module had interrupted the power path from one supply and, at the same time, defeated the monitoring function that should have annunciated the loss of that supply. Reseating the module restored both the intended power path and the alarm functions.

The arrangement annunciated failure or disconnection of a power supply when the module was correctly seated. However, it did not annunciate displacement of the module itself. Because the module formed part of both the 24 V DC power path and the monitoring path, its displacement could disconnect a supply while simultaneously preventing the associated alarm from revealing that disconnection. The system could therefore indicate no abnormal condition even though only one effective 24 V DC supply remained.

The annual DP trials did not create the vulnerability. They exposed a pre-existing concealed condition that had potentially been present during DP operations. The insight is therefore wider than the particular component involved: an alarm should not be assumed to be independent of every failure mode it is intended to reveal.

Central learning: The absence of an alarm is not, by itself, evidence that the monitored equipment and the complete alarm chain are healthy. Where a failure can also disable its associated alarm, periodic functional testing may be the only remaining barrier.

Target Audience for this Learning

- Charterers and their Project Teams.

MTS DP committee thanks the submitter of this 'learning from insights' on behalf of the DP community. Learnings from incidents $LFI_{(i)}$ and insights $LFI_{(n)}$ are published on the MTS DP committee website to promulgate learnings form all available sources with a view to enable proactive management of vulnerabilities and minimize potential for DP loss of position incidents.

- DP Vessel Owners & Operators / Management Teams.
- Vessel crew including Industrial Mission personnel.
- Verification and assurance providers.
- Industry bodies / regulators.

What was learned?

The Observed Condition

The DIN-rail-mounted module was not solely an alarm interface. The 24 V DC power from the redundant supplies also passed through the module. The module was sufficiently displaced to interrupt the power path from one supply while simultaneously impairing the monitoring function associated with that same path. The arrangement did not provide a separate indication that the module, its power path or its monitoring function was unavailable.

One 24 V DC supply was already ineffective, but the operator received no alarm because the same displaced module that interrupted the supply path also prevented the loss from being annunciated. The DP control-system cabinet was therefore being supported by only the remaining supply. Interruption of that remaining supply removed power from the cabinet and resulted in loss of position.

Alarm Availability Is Part of the Safety Function

An alarm function comprises more than the indication presented at the operator station. It includes the sensing point, auxiliary supply, wiring, terminals, removable modules, contacts, input channels, communications, software configuration and the final means of annunciation. A weakness anywhere in this chain may prevent the expected alarm from being generated or displayed.

The failure modes of the monitoring chain therefore require consideration in their own right. It is not sufficient to confirm only that a power-supply failure produces an alarm when the monitoring equipment is healthy.

Credible dependencies may include:

- **The alarm and the monitored equipment being supplied from a common source.**
- **A common return, fuse, terminal, connector or distribution component.**
- **A monitoring relay, interface or input module whose failure is not supervised.**
- **A removable module that can be displaced without a positive health indication.**
- **A communications pathway or software function shared by monitoring and control.**
- **An alarm contact philosophy that does not fail to the alarmed state when monitoring power is lost.**

MTS DP committee thanks the submitter of this 'learning from insights' on behalf of the DP community. Learnings from incidents $LFI_{(i)}$ and insights $LFI_{(n)}$ are published on the MTS DP committee website to promulgate learnings form all available sources with a view to enable proactive management of vulnerabilities and minimize potential for DP loss of position incidents.

Why Periodic Functional Testing Matters

Visual inspection and normal alarm status may not reveal a latent defect. Periodic testing should prove the real function from a credible point of failure through to annunciation and operator response. Testing only at a downstream alarm input or human-machine interface may prove the display while leaving the sensing and monitoring path untested.

Where practicable, testing should demonstrate that:

- **Each redundant 24 V DC supply can independently support the intended load.**
- **Failure or disconnection of either supply is correctly annunciated.**
- **Loss or impairment of the monitoring function produces a separate indication, or causes the circuit to fail to an alarmed state.**
- **The alarm remains available for the credible failure modes it is intended to reveal.**
- **The displayed status accurately represents the installed equipment condition.**
- **Removable modules, connectors and terminals are mechanically secure following maintenance and inspection.**

The test interval should be justified by the consequence of an undetected failure, the likelihood that the condition can arise between tests and the availability of other independent means of detection. Annual testing may reveal the condition, but the appropriate interval should be determined for the particular design and operating context.

FMEA and Assurance Implications

The DP FMEA should consider both failure of the monitored function and failure of the means used to detect and annunciate that failure. A statement that a failure is alarmed should be supported by an understanding of how the alarm is generated and whether the initiating failure can also remove or suppress the alarm.

FMEA proving trials and other assurance activities should identify the point at which the failure is introduced. A test performed too far downstream may not validate the complete alarm chain or reveal common dependencies. Where intrusive testing is impracticable, the limitation and the alternative basis of confidence should be documented.

The learning is applicable beyond 24 V DC supplies. Similar concealed-failure mechanisms may exist in thruster control, power management, network monitoring, cooling, ventilation, uninterruptible power supplies, battery chargers, remote I/O and other supporting systems on which DP capability depends.

Mechanical Security Is a Functional Requirement

For rail-mounted and plug-in components, correct seating and retention are part of the functional integrity of the system. Installation, maintenance and inspection practices should confirm that modules are fully engaged, retaining clips are secure, terminals are correctly tightened and any positive indication of engagement is visible and understood.

MTS DP committee thanks the submitter of this ‘learning from insights’ on behalf of the DP community. Learnings from incidents $LFI_{(i)}$ and insights $LFI_{(n)}$ are published on the MTS DP committee website to promulgate learnings form all available sources with a view to enable proactive management of vulnerabilities and minimize potential for DP loss of position incidents.

If a component can become partially disengaged while appearing generally in place, inspection criteria should address that specific vulnerability. Where practical, design improvements should provide positive retention, monitoring of module health, fail-safe alarm contacts or other means of revealing loss of the monitoring function.

Suggested Action

It is suggested that vessel owners, operators and DP assurance stakeholders evaluate this learning for applicability to their vessels and systems. Actions should be proportionate to the design and consequence, and may include:

- **Reviewing DP control-system DC supplies and associated alarm chains for common dependencies and concealed-failure modes.**
- **Confirming that failure of the monitoring function is itself annunciated or otherwise detectable.**
- **Functionally testing each redundant supply from a credible point of failure, rather than solely stimulating a downstream alarm input.**
- **Verifying that each supply can independently support the connected load without loss of essential DP control functions.**
- **Inspecting the seating and retention of DIN-rail-mounted, plug-in and removable modules, including after maintenance.**
- **Reviewing DP FMEAs, proving trials and planned maintenance tasks to ensure that alarm-path failures and latent failures are addressed.**
- **Justifying test intervals with regard to the consequence and potential exposure time associated with an undetected failure.**
- **Applying suitable operational controls where confidence in power-supply redundancy or alarm availability cannot be established.**

Do not rely entirely on alarms being independent of the failure modes they are intended to reveal. Test the protected function, the redundancy and the complete means of detection.

Conclusions

The absence of an alarm did not demonstrate that the DP control-system power supplies and their monitoring arrangement were healthy. One 24 V DC supply was already unavailable. Because the displaced module formed part of both the supply power path and the monitoring path, the same condition that interrupted the supply also defeated the alarm intended to reveal the interruption. The concealed loss of redundancy was only exposed when the remaining supply was interrupted and the cabinet lost power.

Periodic functional testing exposed the vulnerability. This demonstrates why alarm availability must be treated as part of the function being assured, and why the failure modes of the monitoring path require explicit consideration in design reviews, DP FMEAs, proving trials and planned maintenance.

Where a credible failure can disable both the monitored function and the alarm intended to reveal it, periodic testing may be the only barrier preventing a latent loss of redundancy from remaining

MTS DP committee thanks the submitter of this 'learning from insights' on behalf of the DP community. Learnings from incidents $LFI_{(i)}$ and insights $LFI_{(n)}$ are published on the MTS DP committee website to promulgate learnings form all available sources with a view to enable proactive management of vulnerabilities and minimize potential for DP loss of position incidents.

undetected until a further failure causes loss of position.

APPENDIX - Concealed Alarm Failure Review Prompts

The following prompts may assist reviews of alarms associated with essential DP functions:

- **Can the initiating failure remove power from, disconnect or otherwise disable its own alarm path?**
- **Does loss of the monitoring relay, input module, communications path or auxiliary supply produce a separate alarm?**
- **Is the alarm philosophy fail-safe for loss of monitoring power or an open circuit?**
- **Does the functional test begin at a credible point of failure and prove the complete chain to the operator indication?**
- **Can each redundant supply or channel support the required function independently?**
- **Are plug-in and DIN-rail-mounted components positively retained and included in inspection criteria?**
- **Is the periodic test interval justified for the consequence and potential exposure time of a concealed failure?**
- **Are identified limitations reflected in the DP FMEA, proving trials, planned maintenance and operational guidance?**

MTS DP committee thanks the submitter of this 'learning from insights' on behalf of the DP community. Learnings from incidents $LFI_{(i)}$ and insights $LFI_{(n)}$ are published on the MTS DP committee website to promulgate learnings form all available sources with a view to enable proactive management of vulnerabilities and minimize potential for DP loss of position incidents.