BLACKOUT RECOVERY TEST FAILED DUE TO BUS-TO-BUS SYNCHROSCOPE

Why is This Learning Is Being Issued

A blackout recovery test on an 11kV switchboard was unsuccessful due to a bus-to-bus synchroscope being left in the "on" position. The PMS was unable to automatically recover the dead bus because it appeared to be live. Although the outcome was not 'as expected' it demonstrated the value of periodic testing in finding hidden failures and configuration errors.

Target Audience for this Learning

- DP Vessel Owners and Management Teams
- DP Technical Support Function
- DP FMEA Practitioners
- Classification Societies
- Vessel Designers
- DP Assurance Teams and Charterers

What happened

A DP Class 3 MODU failed a partial blackout recovery test on one bus. This test was carried out under controlled conditions, with the two other buses still online, and thus there were no consequences from the failed recovery. The switchboard configuration error that inhibited recovery was identified and corrected, and the recovery test was successfully completed.

Why it happened

The vessel's HV switchboards are equipped with bus-to-bus synchroscopes to enable manual synchronisation and connection of the HV buses. Prior to the blackout recovery test, one of the bus-to-bus synchroscopes, between the subject bus and a neighbouring live bus, had been unintentionally left in the "on" position. This resulted in a low power voltage source being coupled to the dead bus via the synchroscope.

The coupled voltage was sufficient for the PMS logic to identify the dead bus as being live, and thus blackout recovery was not initiated. The PMS mimic showed the dead bus to be green after it was shut down for the test, but this was not noticed, and the test proceeded but failed

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.

What investigation steps were carried out

As the 11kV bus ties were open and there were no generators connected, the crew investigated other possible ways in which voltage could be coupled from one bus to the next. During this process the crew observed the switch for the synchroscope was in the 'on' position. When it was switched from 'on' to 'off', the false indication of a live bus went away on the PMS mimic.

Note: *The PMS voltage transducer was operating correctly.*

What was focused on: The investigation focused on the common points (means by which voltage could be coupled from one bus to the other) and on the criteria used by the PMS to identify blackout conditions.

Why was this focused on: There appeared to be no other way in which an otherwise dead and completely isolated bus could be energised other than through a common point between the switchboards.

- Reliable and robust blackout detection functions are critical to the efficacy of blackout recovery and help to prevent failures associated with spurious activation of blackout recovery. Power management system designs must carefully balance the need for effective dead bus identification against the impacts of unintended activation on a live bus.

- Falsely identifying a dead bus as live can result in failed blackout recovery, whereas false indication of a live bus as dead bus can result in the execution of unnecessary actions (opening of breakers, starting of generators, etc.). At best, these actions are a minor annoyance, while at worst they can result in failure effects exceeding the severity defined by the WCFDI.

What was the outcome

The investigation concluded that: The cause of the failed recovery of a healthy bus was that the voltage levels coupled through the synchroscope were sufficient to indicate the bus was already live to the PMS. The investigation therefore concluded that the switchboard transducers and PMS logic should remain unchanged, but that position of the synchroscope switches be added to engineroom checklists.

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.

Confidence level on outcomes: High

Basis of confidence: Blackout recovery was retested successfully with the synchroscope switched off. False indication of a live bus disappeared from the PMS mimic when the synchroscope was switched off.

Lessons learned

- Unexpected signal coupling may interfere with blackout detection and recovery.
- Some types of synchroscopes are capable of coupling low power voltages from a live bus to a dead bus. They should normally be off (and documented to be so in checklists).
- The effects of coupling low power signals onto the bus should be considered in the design of dead bus detection circuits. When the bus has no loads or generators connected to it, a low power signal may be able to excite the bus to the point where it indicates as live to the PMS. Care needs to be taken to ensure this does not prevent blackout recovery.
- The use of multiple signal sources in blackout detection logic can be used to increase the reliability and security of blackout detection but the choice of fail-safe condition for the blackout detection logic may favor false indication of a live bus as preferable failure effect compared to false indication of a dead bus. This choice of fail-safe means there will be failure modes in the detection circuit that can defeat blackout recovery.
- Periodic blackout recovery testing is important in ensuring the integrity of blackout recovery as a risk reduction measure. This periodic DP trials test was successful in revealing a hitherto unknown configuration error inhibiting blackout recovery.

Suggested actions

It is recommended that:

- Vessel owners review their bus-to-bus synchronizing arrangements for vulnerability to this type of incident.
- Vessel owners and designers review set-points and logic used by dead bus detection.
- Appropriate procedures should be put in place to confirm synchroscopes are disconnected (off) when not actively in use. Monitoring and / or alarming switch position may be a possible and practical solution in some cases.
- FMEA practitioners should consider the impact of commonality (introduced by control and monitoring devices which span the redundant DP equipment groups) on failure effects and blackout recovery.
- PMS OEMs should consider the impacts of coupled signals on their dead bus detection

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.

logic and evaluate / develop robust detection strategies.

- Redundancy in Bus VTs may provide opportunities for improved robustness in dead bus detection. Where two VTs per bus are not practical, some designs have derived a signal from other connected transformers where a simple binary indication is required for control purposes.

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.

Appendix - General Considerations in Dead Bus Detection

Several different systems rely on information about the status of the bus (Live or Dead):

- Switchgear controls synchronizing and dead bus connection of generators and switchboards.
- PMS for blackout recovery.
- Protection systems for undervoltage release.

The following discussion focuses on PMS detection for blackout recovery.

Dead bus detection in a PMS is often based on several measurements and methods:

- Voltage and frequency transducers
- 3 x Dead bus relays – (one per phase and thus three per bus section) HV and LV distribution
- CB status may be used in some designs

The logic in the PMS should triangulate multiple sources of information to increase reliability and security.

However, the choice of logic which combines this information dictates the residual vulnerability to which the power plant is exposed.

Example analysis (for information only)

Refer to Figure 1. Assume that logic '0' represents a live bus and logic '1' represents a dead bus. This convention applies to both the dead bus relay output and the PMS voltage transducer setpoint exceeded condition.".

A fail-safe condition for the detection circuit could be defined such that any fault in the detection circuit has the effect of indicating the bus is live (0). Adoption of this logic means any fault could defeat blackout recovery because the type of voting is determined by the choice of fail-safe condition.

- If multiple signals indicating dead bus (1) are OR'ed, any real or false indication that the bus is live (0) will not inhibit blackout recovery but makes it more likely that a live bus is falsely reported as dead with undesirable consequences.
- If multiple signals indicating dead bus (1) are AND'ed any real or faulty indication that the bus is live (0) will inhibit blackout recovery and make it more likely that a dead bus is

reported as live. The consequences of this are arguably less severe than that above and can be mitigated by periodic testing of blackout recovery.

Note: *The actual logic and fail-safe condition used should be confirmed before making assumptions of circuit response to failure.*

- Commonality between dead bus signal sources such as having the dead bus relay coils and the voltage transducer signals from the same VT means that loss of signal from the VT or loss of a common control power signal through the relays when the bus is live will appear as a live bus regardless of the logic as the voting inputs will either all be logic 0 or all be logic 1 for these types of faults.

- Majority voting on multiple independent sources could allow for a more robust solution that is less vulnerable to false indications of either kind (dead bus live or live bus dead). The practicalities of creating truly independent sources may favour the fail-safe approach.

- Diversity of sources could also improve robustness. For example, generator and bus tie circuit breaker status could be added to voltage, frequency and dead bus relay type detection.

- However, as the fail-safe condition is considered to be 'indicate the bus is live' regardless of its actual state then blackout recovery will be vulnerable to failures in the detection circuit. However multiple sources are of no help if the coupled voltage on the bus exceeds the point at which:

  - The transducer (and / or PMS software setpoint) indicates a live bus.

  - The blackout relays operate (by indicating logic 0).

  There is no way to distinguish this from the real condition with the information available.

Manual synchronizing of generators is understood to be a class requirement; however, the ability to manually synchronize switchboards is optional (they can be closed onto a dead bus). Therefore, removing the synchroscope may be an alternative, as could monitoring and alarming switch positions.

Note: *The example that follows is not intended to represent a suitable design; rather, it illustrates the type of analysis that can be used to gain insight into the robustness and vulnerability of a detection strategy.*

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.

For the example circuit in Figure 1 below, the truth table in Table 1 can be used to visualise the response of different types of logic to common mode failures of the bus VT's 3 pole MCB 1 to the open position and failure of the control power supply to 0V. Three types of logic are compared – AND, OR and 3oo4, the latter being a majority voting function. AND logic consistently reports the fail safe condition for any combination other than bus dead. 3oo4 logic reports conflicting conditions depending on the nature of the common mode failure but would be much more robust if provided with independent bus status measurements.

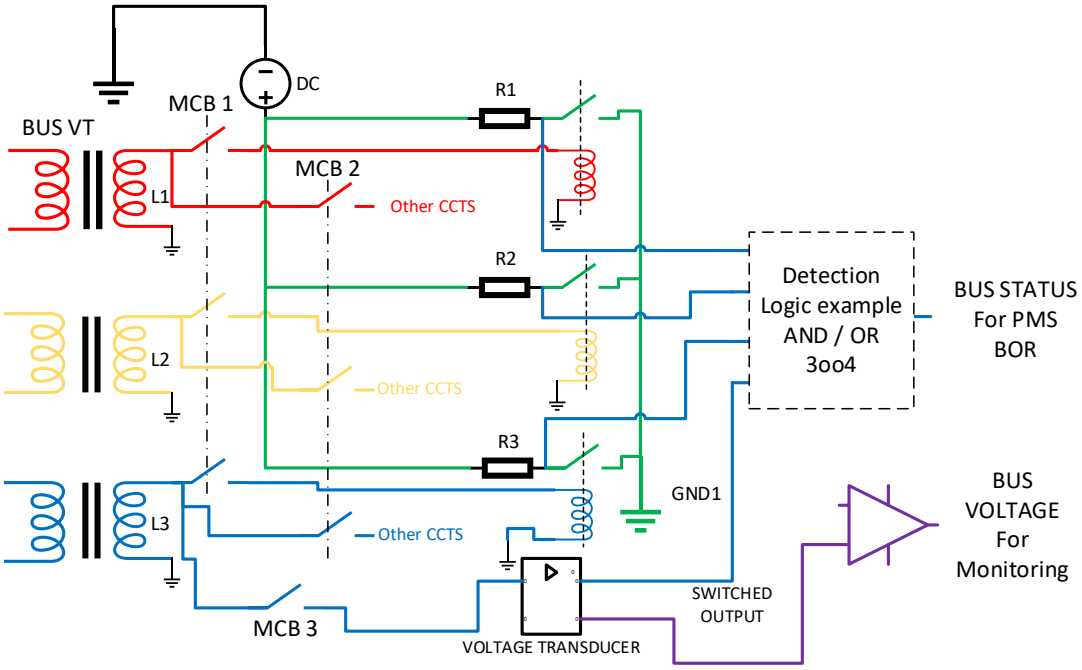

Figure 1 Example Dead Bus Detection Circuit (not to be used for design)

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.

Table 1 – Truth Table

Equivalent to failure of control power supply to 0V

0 = Live			1 = Dead	Bus Status		
Input to Logic				Output from Logic		
Phase A	Phase B	Phase C	Voltage Transducer	AND	OR	3oo4
0	0	0	0	0	0	0
0	0	0	1	0	1	0
0	0	1	0	0	1	0
0	0	1	1	0	1	0
0	1	0	0	0	1	0
0	1	0	1	0	1	0
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	1	0
1	0	0	1	0	1	0
1	0	1	0	0	1	0
1	0	1	1	0	1	1
1	1	0	0	0	1	0
1	1	0	1	0	1	1
1	1	1	0	0	1	1
1	1	1	1	1	1	1

Equivalent to common mode failure of VT – 3 pole MCB trips

Although much can be done to improve the reliability of the PMS's blackout detection process it is difficult to achieve a design that is fail-safe for every possible fault condition. Effort may be better focused on ensuring the primary barrier provided by the single fault tolerance of the DP systems is robust and well defended rather than expending more effort on blackout recovery which is intended to reduce the consequences of an unpredictable situation. This is strategy is best visualised in the familiar Bow Tie model.

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.

Other Considerations

Blackout detection and recovery systems can also be vulnerable to false indication of blackout associated with voltage dips and other transient conditions. In designs where all circuit breakers on a switchboard are opened by the PMS on blackout detection, such transient conditions can turn a false blackout into a real one.

It is thus important that the set-points and time delays are defined such that they reliably detect real dead-bus conditions but do not react to normal operation, including transient conditions associated with the starting of large equipment or clearance of faults.

The case in this LFI has focused attention on the need to consider the coupling of low power voltage signals onto the dead bus.

Detection systems should be tuned such that they are not influenced by transient conditions.

Unwanted coupled signals are best eliminated during blackout recovery as it may be challenging to design a detection circuit that can cope with this type of phenomena. On this vessel, the coupling was via the synchroscope, however, other means of coupling may be possible.

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.