NovaTech

Technical Note

Fail Well: A Comparison of 16000 I/O, Quantum I/O, and 8000 I/O Redundancy and Diagnostics

Introduction

The D/3® is a highly redundant DCS and is designed to handle subsystem failures. For this reason, the D/3 supports redundant communication with the PCMs, redundant controllers, and in many cases redundant interfaces with the I/O. At each level of the D/3, diagnostics are generated to inform the operator of failures. When these failures do occur, the D/3 is designed to mitigate the consequences, provide the operator with notification and provide system diagnostics for troubleshooting the failure.

This document discusses some recently reported I/O failures related to 16000 I/O and Quantum I/O and provides a discussion of these failure scenarios in the context of 8000 I/O. The discussion reviews the redundancy scheme for each I/O family, the failover node behavior, the power considerations, and finally the I/O failure modes. These failures would not have occurred with 8000 I/O or the situation would have been mitigated through the available diagnostics.

Discussion of I/O Failures

Recently, customers have experienced I/O failures with both 16000 I/O and Quantum I/O.

One reported situation was a PCM failover due to the failure of a Quantum drop. The PCM failover logic compares the number of healthy failover nodes between the selected and non-selected PCMs across all configured I/O. When the number of healthy nodes is higher on the non-selected PCM and the other conditions for a failover are present, the PCM will fail over. In the case of Quantum I/O, if a Quantum failover node fails e.g. due to a complete loss of power, there is a race condition based on which PCM detects this failure first. It is possible for the Quantum drop to fail on both PCMs, and this failure prompt a PCM failover based on the selected PCM detecting the failure first. With 8000 I/O, this does not happen because the selected PCM tries to reconnect 2 times via the same or alternate network paths before marking the node as failed. The non-selected PCM marks the node "FAIL"ed immediately upon the first communication failure.

In addition to the detection of failure, 8000 I/O redundancy is not tightly coupled to the communication redundancy. Unlike 16000 I/O, where loss of communication from the PIO to the mux will cause a PCM failover, or Quantum I/O, where loss of communication between the MRIOC and the drop will cause a PCM failover (both depending on the mux/drop configuration), 8000 I/O can experience the loss of the active Ethernet port on the EBIM, and the EBIM will reroute communications through the remaining healthy Ethernet port. With 8000 I/O, the communication path can be disrupted, and if the run-selected PCM is able to successfully reroute communications with the MASTER EBIM, the PCM notifies the operator of the disruption but avoids a PCM failover. In this manner, the 8000 I/O redundant communications is not coupled to the PCM redundancy as it is with 16000 and Quantum I/O.

16000 I/O does not have a configurable failsafe value for outputs. When 16000 I/O loses communication with the D/3, the 16000 I/O holds the last value. To manage this lack of configurability, a customer used Quantum I/O to de-energize 16000 I/O outputs on loss of communications. 8000 I/O provides configurable failsafe values, removing the need for this type of "work around." In addition, the 8000 I/O has several configurable failsafe timeouts, such as a protection against the PCM losing communication with the 8000 I/O drop, or the EBIM losing communication with the 8000 I/O module. The 8000 I/O provides excellent diagnostics to identify and resolve these failures.

Another failure considered was a power failure. No I/O subsystem can survive a complete loss of power. For this reason a UPS is placed ahead of the I/O. In the case of a single inline UPS, the overall reliability is limited to the UPS's reliability. The reliability of the I/O can be increased by providing a redundant UPS input to the I/O. The I/O subsystem's support of redundant power feeds simplifies this approach.

16000 I/O provides redundant power supplies for the mux. However, if the user wishes to feed these supplies from redundant feeds, this must be managed externally since there is only one power input to the redundant power supplies.

Quantum I/O provides support for redundant power supplies and redundant power feeds. Redundant power feeds work well with Quantum I/O.

8000 I/O is designed to accept redundant power feeds to the EBIMs. Redundant power is often supplied for the field power either by using a load sharing device with redundant supplies or diode ORing redundant external inputs. In addition, 8000 I/O provides diagnostic inputs to monitor power supply status, providing a system alarm when a power supply failure is detected.

A final failure was a 16000 I/O MIO board not scanning the I/O boards. In this case, all the EPNs were IBAD, but the mux did not fail and no failover was initiated. With the available diagnostics of 16000 I/O, this condition was difficult to troubleshoot. The 8000 I/O diagnostics provide system alarms for module failures and other error conditions. In addition to notifying the operator of a failure that requires operator intervention, the 8000 I/O provides carefully organized detailed information on the current 8000 I/O status making it easy to isolate the source of a problem and identify the action to resolve it.

Features	16000 I/O	Quantum I/O	8000 I/O
Redundant Communication	Yes	Yes	Yes
Redundant Power Feeds	No	Yes	Yes
Decoupled Redundancy	No	No	Yes
Mux/Drop/Node Diagnostics	Yes	Yes	Yes
I/O Board/Card/Module Diagnostics	No	Yes	Yes
Point Diagnostics	No	No	Yes

Figure 1 : Comparison of Features and Diagnostics 16000 I/O, Quantum I/O, 80000 I/O

16000 I/O Redundancy

16000 I/O provides redundant communication from the redundant PCM pair to the 16000 I/O mux. Each PCM communicates with the I/O via an MIO card. The mux chassis provides redundant backplane communication between the redundant MIO cards and the individual I/O boards. The 16000 I/O redundancy is coupled with the PCM redundancy in the sense that failure of an MIO card necessitates a PCM failover to resolve communications with the mux.

The PCM verifies the health of the MIO card based simply on the response of the MIO card to a command from the PIO card. From the perspective of the PCM, the response of the MIO card to a PIO command is the sum of 16000 I/O diagnostics as displayed on the system status display.

16000 I/O Power

16000 I/O supports redundant power supplies for the Mux. The Mux has a single power feed for the redundant power supplies. The field power can also be supplied in a redundant configuration. The PCM generates a system alarm in the case of a power supply failure.

16000 I/O Failover Muxes

16000 I/O failover muxes are configured in WinCOD. The PCM judges the health of the 16000 I/O node based on the MIO board's response to a command from the PIO board. The failover logic in the PCM compares the health of the run-selected PCM with the non-selected PCM based on the count of healthy failover muxes on each.

The failure of a mux presents a race condition to the PCM. Based on which PCM detects the failure first, this condition can cause a spurious PCM failover.

16000 I/O Failure Modes

Since the failover node logic is based only on the MIO responding to a command, there are several failures that can occur with 16000 I/O that will not prompt a PCM failover.

A failure at the level of the MIO card or the I/O card(s) where the MIO card is able to respond to a PIO command, but is unable to scan the actual I/O can lead to a failure that does not prompt the PCM to fail over to a potentially healthy partner. On the physical hardware the I/O cards have access LEDs that can be used as a diagnostic to verify that they are being scanned.

Figure 2 shows the diagnostic display in system status showing the health of the 16000 I/O subsystem. 16000 I/O provides limited diagnostics for the health of the subsystem- and has failure modes where the user has no diagnostic indication of a failure other than the failure of the EPNs accessing the 16000 I/O data.

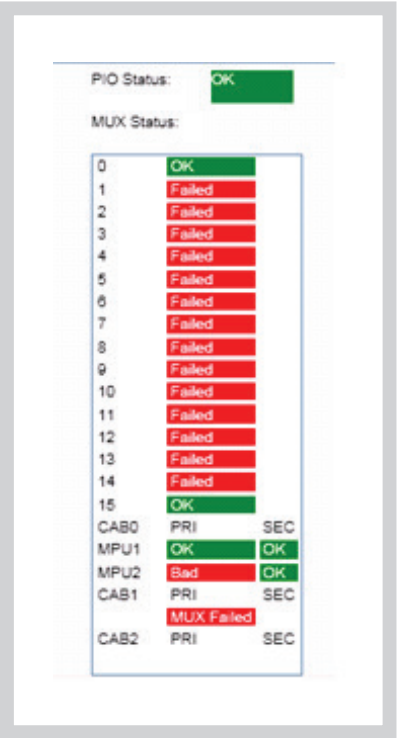

Figure 2 – 16000 I/O System Status Display

Quantum I/O Redundancy

Quantum I/O provides redundant communication from the redundant PCM pair to the Quantum I/O drop(s). Each PCM communicates via a separate CRA module in the remote drop. The Quantum I/O redundancy is coupled with the PCM redundancy in the sense that failure of a CRA module necessitates a PCM failover to resolve communications with the drop.

Quantum I/O Power

Quantum I/O supports redundant power supplies for the remote drop. These redundant power supplies can be supplied from redundant power feeds. Quantum I/O provides system alarm diagnosis of failed power supplies.

Quantum I/O Failover Nodes

Quantum I/O failover muxes are configured in WinCOD. The PCM judges the health of the Quantum I/O drop based on successfully communicating with the CRA. The failover logic in the PCM compares the health of the run-selected PCM with the non-selected PCM based on the count of healthy failover drops on each. The failure of a remote drop presents a race condition to the PCM. Based on which PCM detects the failure first, this condition can cause a spurious PCM failover.

Quantum I/O Failure Modes

Since the failover node logic is based on the ability to communicate with the CRA, Quantum failover node logic assumes communication is the primary failure mode. The physical hardware has an “Active” indicator that can be used to diagnose communication between the PCM and the individual modules in the drop.

A failure of the CRA to properly communicate with the I/O modules in the drop will not prompt a failover and will provide little diagnostic information of the failure.

Figure 3 shows the detail display of Quantum I/O status. Quantum I/O provides diagnostic information down to the specific module health. This detailed diagnostic information makes it easy to diagnose a failure all the way down to the slot.

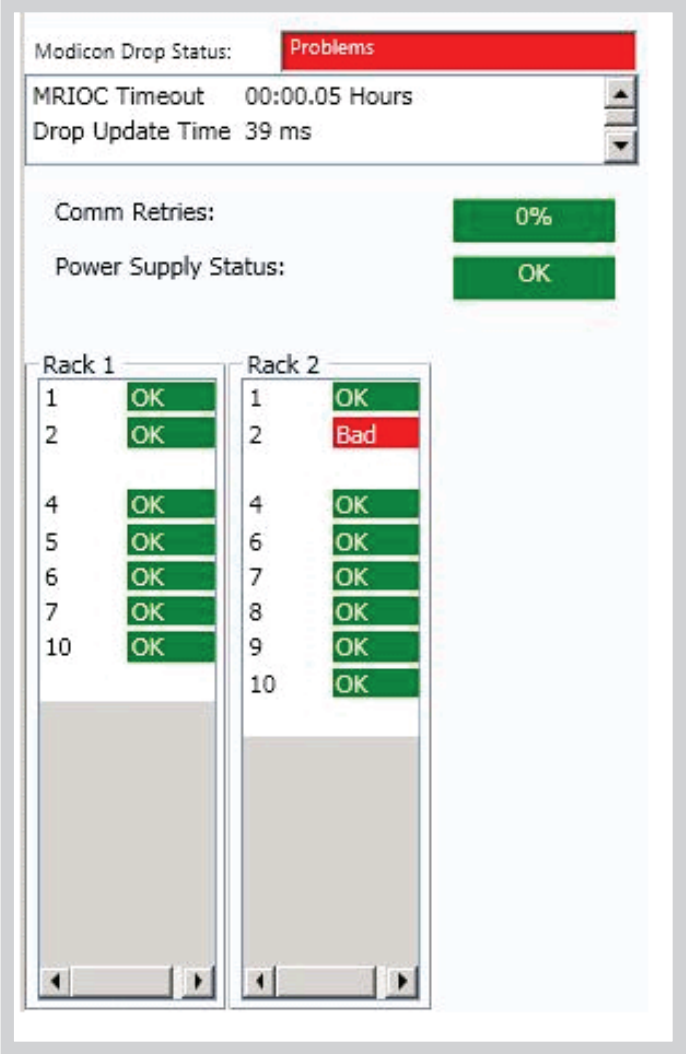

Figure 3 – Quantum I/O System Status Details Display

8000 I/O Redundancy

8000 I/O provides redundant communication via the redundant EBIMs and the redundant Ethernet interfaces on those EBIMs. The EBIMs use an FTE (Fault Tolerant Ethernet) protocol to manage their Ethernet interfaces. Communication between a PCM and 8000 I/O can experience various failures without requiring a PCM failover to recover. The 8000 I/O redundant communication is not coupled with the PCM redundancy. The 8000 I/O monitors the Ethernet network health and generates a system alarm if it detects a failure.

Because the communication redundancy is decoupled from the PCM redundancy, it is possible to upgrade firmware on the individual EBIMs on a running system without generating a PCM failover.

The 8000 I/O provides the PCM with node, modules, and channel diagnostics. The PCM generates system alarms based on network, node, and module failures.

In addition to the failure mode diagnostics, the tight integration of 8000 I/O in the D/3 eases troubleshooting and configuration.

8000 I/O Power Supplies

8000 I/O supports redundant power supplies for the EBIM and I/O as well as redundant field power. 8000 I/O is designed for installation with redundant power feeds.

8000 I/O Failover Nodes

8000 I/O supports online configuration of failover nodes in the Ethernet I/O configuration tool. Unlike 16000 I/O and Quantum I/O, 8000 I/O failover nodes are not configured in WinCOD. 8000 I/O failover nodes can be added to a running system in the Ethernet I/O configuration tool. All the failover node configuration for 8000 I/O is done in the Ethernet I/O configuration tool. This configuration can be done either off-line or online. Unlike 16000 I/O or Quantum I/O, 8000 I/O does not require a PCM reload to modify the failover node configuration. 8000 I/O failover nodes serve the purpose of validating which PCM has healthier communication with the I/O drops. Unlike 16000 I/O and Quantum I/O, when the run-selected PCM loses communication with an 8000 I/O node, the selected PCM tries to reconnect before triggering a failover. This attempt to reconnect is designed to prevent spurious failovers based on the failure of failover nodes on both the selected and non-selected PCMs.

8000 I/O Failure Modes

The PCM marks an 8000 I/O node as failed based on loss of communication. Loss of communication with an 8000 I/O node is in general due to a loss of networking or the failure of the EBIM. The network topology provides redundant communication paths. The 8000 I/O EBIMs monitor the health of the Ethernet network, and if the PCM detects a failure, it generates a system alarm. The redundant EBIM presents EBIM health diagnostics to the PCM and if an EBIM fails or changes mastership, the PCM generates a system alarm.

Figure 4 shows the 8000 I/O system status node diagnostic display. The diagnostics in the 8000 I/O extend to all areas of the I/O subsystem. The EBIMs monitor the network health and adjust communications accordingly. The PCM monitors conditions in the 8000 I/O and generates system alarms based on networking failures, module failures, and EBIM interface failures. All these diagnostics provide the customer with the information needed to troubleshoot failure conditions quickly and accurately.

Figure 5 shows the 8000 I/O module level diagnostics display. 8000 I/O diagnostics allow the operator to see from the PCM level all the way down to the analog value the EPN is reading on an 8000 I/O module.

Figure 4 – 8000 I/O System Status Node Status Display

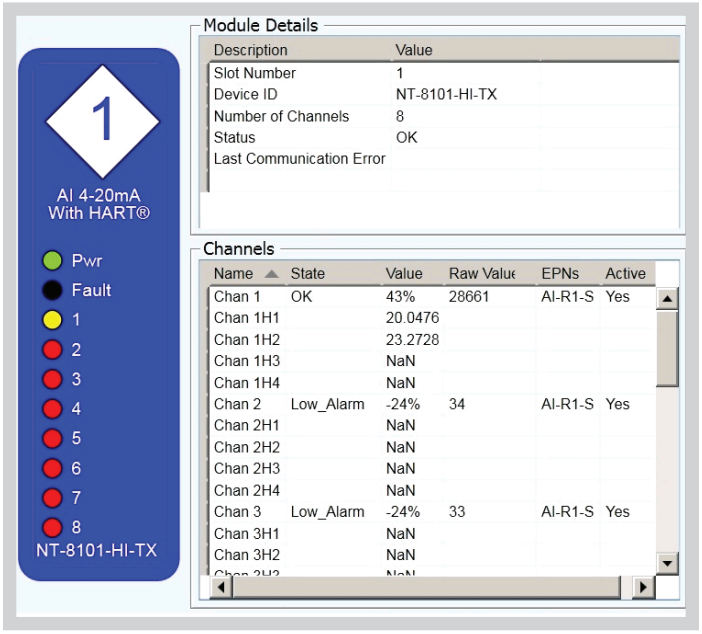

Figure 5 - 8000 I/O System Status Module Detail Display

Conclusion

For the three failures identified in this paper, the 8000 I/O subsystem would have provided the customer with much better outcomes.

In the first instance where a failover node failed on both PCMs, unlike 16000 I/O and Quantum I/O where a race condition exists to identify the node failure first, the 8000 I/O is designed to identify the node failure on the non-selected PCM first in order to avoid a spurious failover. In addition to 8000 I/O's better failover behavior, 8000 I/O supports failsafe configuration and failsafe timeouts that eliminate the need for a "work around" for communications failures.

In the second instance where the I/O suffered a power outage and UPS failure, 8000 I/O is designed for installation that mitigates this type of failure.

In the third instance a latent failure in the 16000 I/O subsystem resulted in diminished operation of the I/O subsystem without notifying the operator of the condition or providing diagnostic data that could be used to troubleshoot the condition. 8000 I/O provides the operator with notification of failures that threaten or degrade the operation of the I/O subsystem. Aside from these system alarms, 8000 I/O provides clear diagnostic information to make the resolution of any failure condition quick and accurate.

novatechweb.com