ONTARIO POWER GENERATION

Records File Information:
FILE ELECTRONICALLY WITH
SCR

Internal Use Only

N-FORM-10134-R003*

Barrier Analysis Worksheet

Adverse Condition	Barrier(s) that should have precluded Condition	How the Barrier Failed	Why(s) the Barrier Failed
Commissioning of the 800xA software for HWMS Computers in the T1501 TRF outage identified undesirable behaviours in two areas related to alarm handling.	Comprehensive testing of the 800xA software using a test system that is fully representative of the field configuration, including the field I/O hardware. The testing of the general software functionality was the responsibility of the vendor (ABB) and the testing of the customized application was the responsibility of the project team.	Internal vendor testing and verification processes failed to discover these conditions prior to Factory Acceptance Testing. Vendor technical specialist unable to resolve the issues in a timely manner.	The 800xA software is very complex and works in a number of different configurations with various types of control equipment and I/O. In certain cases the Vendor is testing their software using simulators and emulators, as it was the case here for the Factory Acceptance Testing. The vendor is also expecting the users to discover minor issues and report them to be fixed for the benefit of all users. Obviously the conditions identified in this SCR have not been reported previously to the vendor. Anticipating this sort of situation, a vendor specialist was requested to attend the field commissioning activities. Although the specialist provided some useful insights he was not able to resolve the issues in a timely manner, and the issues are now with the vendor for resolution as part of the vendor support agreement.
		For the condition related to the initial alarm state of the D2O storage DIs following a cold start of DCU#4, the testing carried out by OPG was done without having the I/O hardware available and without considering that initially all D2O points will be in allarm (open-contact)	Unavailability of certain I/O hardware and significant costs of acquiring this hardware for the test system. A previous upgrade of the HWMS Computer Software from SR3.0 to SR6.0 was also completed without the full I/O hardware being available for testing. This reinforced the thinking that full I/O hardware may not be required for the upgrade to 800xA. The test cases did not consider the initial state when most of the D2O Storage DIs will be in an open-contact state with a large number of alarms showing in the Alarm Review display.

*Associated with N-STD-RA-0008, Incident Investigation

Barrier Analysis Worksheet

		For the condition related to the alarm hiding the test cases were not extensive enough, considering (in hindsight) that the feature behaves inconsistently.	Testers only designed test cases (and performed) only limited type testing of this functionality, rather than extensive tests for each type of point. This was considered to be adequate considering that the software package was qualified for use for Category III computer systems and was produced by a reputable vendor. This also took into consideration that the software was used extensively in the Test and Training facility without issues. This sort of decisions are made all the time to provide the best balance of costs and schedule versus the risk of breakthroughs in the field.