NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

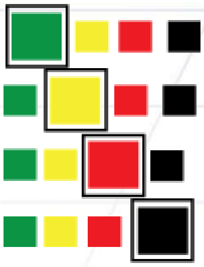
# Industry Advisory

## Preventable EMS and SCADA Events

Initial Distribution: April 10, 2012

During the period of the Event Analysis (EA) Field Trial, 28 Category 2b events have occurred where a complete loss of Supervisory Control and Data Acquisition (SCADA) or Energy Management System (EMS) lasted for more than 30 minutes. Further analysis of 24 of these events has revealed three common themes: 1) EMS Software Failure, 2) Inadequate testing of EMS Equipment and Software, and 3) Change Management[1] for EMS systems. As of the publish date of this Alert, the remaining four events are under review by EA.

Why am I receiving this? >>
About NERC Alerts >>

| **Status:** | **No Reporting is Required – For Information Only** |
|---|---|
|  | **PUBLIC**: No Restrictions<br>**PRIVATE:** Restrict to Internal Use and Necessary Consultants / Third-Party Providers<br>**SENSITIVE:** Internal Use Only (Do Not Distribute Outside Your Company)<br>**CONFIDENTIAL:** Limited Internal Distribution Decided Upon by an Officer of the Company<br>More on handling >> |
| **Instructions:** | NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.** This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved reliability standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a reliability standard. |
| **Distribution:** | **Initial Distribution:** Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Owner, Transmission Operator.<br>Who else will get this alert? >><br>What are my responsibilities? >> |

**Primary Interest Groups:**

Cyber Security – Control Systems, Cyber Security – Corporate IT, Generation Engineering, Generation Operations, Physical Security, System Operations – Transmission Engineering, System Operators, System Operators – System Protection, Transmission Planning

**Advisory:**

This Alert is intended to highlight some of the most common EMS reliability issues and identify opportunities for registered entities to reduce or avoid the complete loss of SCADA/EMS events. Listed below are examples taken from events that illustrate these issues. Also provided are some practices that industry is applying or could apply in maintaining and testing EMS systems. Employing these or similar practices can help registered entities reduce the risks of EMS interruptions. These events reinforce the need for a well-written detailed test, change management, and change control plan. Most of these events may have been avoided with proper testing using a representative EMS quality assurance (Q/A) test system, with the associated hardware configuration.

During the extent of the Event Analysis Field Trial, 28 Category 2b events (identified based on criteria in the “ERO Event Analysis Process” document) occurred, resulting in complete loss of SCADA or EMS lasting for more than 30 minutes. Further analysis of 24 of the 28 events revealed three recurring themes (some events had more than one contributing factor associated with them; therefore, the total percentage will not add up to 100%):

- 52% of the events occurred due to software failure;
- 38% of the events occurred due to inadequate testing of equipment, software, design, or installation; and
- 48% of the events occurred due to change management[1].

Analyses of the remaining four events are not complete as of the publish date of this Alert.

**Software Failure:**

As defined by NERC, software failure is *“a situation where the controlling software failed, the system froze (or hung up) or other computer-related software issues exist. It is an "occurrence" rather than a true cause, and*

[1] Based on a definition provided by Department of Energy (DOE) document DOE G 231.1-2, Change Management is defined as “problems caused by the process by which changes were controlled and implemented by management as organizational needs change to accommodate new business needs.” (See http://doe.test.doxcelerate.com/directives/current-directives/231.1-EGuide-2/view), *Occurrence Reporting Causal Analysis Guide*.

*corrective actions should involve the vendors of the software."* This definition is consistent with the method used in DOE G 231.1-2. NERC developed this causal code and its definition to fill a gap in the DOE manual, which does not address software.

**Example 1:**

An alarm was generated from a test of a new Remote Terminal Unit (RTU) on the SCADA front-end servers and was passed back to the EMS server. The alarm was corrupted and caused a program exception in the alarm process on the EMS server, resulting in the failure of the alarm process. Because the EMS system was designed to automatically restart processes that fail, each time the alarm process restarted, it attempted to process the corrupt alarm and subsequently failed. The SCADA master on the EMS server realized that the alarm process was not available and stopped processing the data from the SCADA front-end servers as well as the Inter Control Center Communication Protocol (ICCP) servers. EMS staff determined that the problem originated in the alarm process. The new RTU and its associated points created a concatenated field in the alarm process that exceeded 81 characters in length; this length exposed a coding error that was written to prevent concatenated fields from exceeding 80 characters in length. Once the backup to the alarm database was restored, the EMS was restored.

Example 1: Lesson Learned/Corrective Action:

Personnel should: know the limitations of the EMS and Intelligent Electronic Device(s) (IED) configuration parameters (along with their naming conventions, number of configurable devices, and protocol specific limitations); understand the ramifications if such limitations are exceeded; and develop offline verification methods. This information should be communicated by the vendor to the registered entity. New additions and modifications of IEDs that communicate to the EMS should be developed and tested offline using test procedures, to verify any new alarms and configuration parameters in a test environment before implementation on the production front-end or EMS. Reliability and security performance should be observed in both the testing and production environment following the install. In this case, the new RTU and its associated points were renamed to reduce the size of the concatenated fields to well under the limit of 80 characters.

**Example 2:**

To configure SCADA and Automatic Generator Control (AGC) applications for two new hydro units during commissioning tests, a Registered Entity was performing a scheduled activity to deploy a revised EMS database within its production systems. While making the change, the redundant EMS application servers failed to accept the revised configuration database. In succession of the automated system recovery, the servers also failed to accept the previous functional database. After manual efforts failed to restore the database on all servers, the EMS staff initiated vendor support, which assisted in restoring the EMS by uploading an archived database.

Example 2: Lesson Learned/Corrective Action:
In conjunction with in-house testing prior to significant configuration changes, entities should confirm EMS vendor support is available as part of the service agreements. With the assistance of the EMS vendor support, the registered entity was able to restore the EMS by uploading an archived database with recovered configuration data file directories to one of the servers. The vendor provided phone consultation and reviewed log events to support the staff. Similar support was provided for the second server, as well as synchronization tests and redundancy status. Another good practice is to have vendor support available during major or non-routine software/system updates. If possible, major software updates and significant EMS system modifications should be thoroughly tested on the vendor's factory system or representative Q/A test system. All major software updates and significant modifications should also be observed for reliability and security performance after installation.

**Testing:**
Referencing DOE G 231.1-2, Testing of Design/Installation Less Than Adequate (LTA) is defined as *"design reviews, testing, independent inspections, and acceptance were not in compliance with customer expectations and/or site requirements."* For equipment and material, inspection/testing LTA is defined as *"scheduled inspection/testing did not exist for the instrument or equipment; inspection/testing was inadequate or not performed as required; or did not include all of the essential elements."*

**Example 3:**
A registered entity successfully tested a new "group control" function with a grouping of five breakers. In the process of executing a "group control" for nearly 300 breakers, the SCADA application did not properly check that the number of controls issued exceeded the maximum possible number.

As a result, SCADA generated "CTRL ISSUED" alarms with invalid key information. The invalid key information was stored as part of the alarm record. As part of the interface with ALARM, SCADA requested a download of all unacknowledged alarms pertaining to SCADA points. During this exchange of data, ALARM reported an unacknowledged alarm on one of the invalid keys created during the "group control". An "*operating system exception"* was generated during the process of attempting to identify the record associated with the invalid key information. This exception caused the SCADA application to abort unexpectedly. After restart attempts failed, SCADA was restarted by the PROCMAN application. The unacknowledged alarms were downloaded again during the SCADA initialization process. SCADA could not restart until the offending alarm with the invalid key was located and acknowledged.

Example 3: Lesson Learned/Corrective Action:
In this example, if the changes were tested in a representative system the "exceeded maximum possible number" may have been detected. This event is also a software issue in that the value should have been "bounds checked" prior to accepting the new parameters. Therefore, before implementing new functions, the scale or magnitude of operations to be performed should be considered along with the operation itself. Testing of new functions at the scale to which they will be used offers insight to potential issues. Proper testing should be performed to show how applications may react on the EMS system, as well as to identify possible error-checking programming needs. Testing helps to determine the scale of risk associated with the change. Prior to implementation, understanding the proper bounds of any parameter is critical. Following a checklist of possible pitfalls (created during the development phase) could assist in reducing errors.

The situation was resolved via a patch from the vendor to address both the generation of invalid keys based on the maximum quantity and allowing SCADA to check for and ignore invalid key data. The patch was successfully tested on a test system and properly loaded onto the production system. The patch was posted for all customers.

Similar errors on other EMS systems related to testing were reported to cause Category 2b events. For example, dependency issues not tested prior to implementing changes to the base console log-on configuration allowed operators to log into the Primary Control Center (PCC) servers and select either the PCC or Back up Control Center (BCC) server. This log-on configuration capability created an unexpected dependency between the PCC and BCC domain servers.

**Change management[1]:**
**Example 4:**
Prior to experiencing an unexpected system shutdown, an error occurred with a written switching order for building switchgear to cut power to the "B" building load (two separate loads power the entire building – "A" and "B"). Included in the "B" load were all of the EMS workstations (both primary and secondary consoles) which the Energy Control Center (ECC) operators used to communicate with the EMS servers. Within an hour of the initial event, the Registered Entity experienced a second unexpected system

shutdown of both the primary and backup EMS servers within seconds of each other. The data center power distribution unit (PDU) "B" had tripped offline due to the earlier problem with the switchgear outage. Corporate IT (the primary user of the data center) told the facilities group there was no rush to return it to service because all systems had both an "A" and "B" feed. In actuality, the EMS servers did not have dual feeds. This left the EMS servers with only the single feed from the "A" PDU. While no definitive outage was reported after the initial switching order event, there appears to have been a sufficient size voltage fluctuation that caused the EMS servers to restart. This fluctuation may have occurred during the switching operations to restore the power feeds back to their normal settings.

Example 4: Lesson Learned/Corrective Action:

Entities should verify that redundant systems are in place. Review all power configurations, including uninterruptible power supply (UPS) loading capacity, to ensure that redundant systems are actually fed from isolated power feeds. Also, verify current draw on all individual circuits will not exceed their rating when one or more power feeds are interrupted. Consider all risks that could occur during each maintenance operation.

**Example 5:**

A registered entity experienced a partial loss of its EMS functionality. The outage was caused by an internal power failure in the primary mainframe of the EMS system. The power failure also interfered with the automated fail-over to the backup mainframe and resulted in a loss of monitoring and control capability for much of the transmission system. The EMS system was initially put in service in 1991, and the hardware and software for this EMS system is no longer supported by its vendor or other third parties. The sole source of support for the system consists of the entity's staff of system and application analysts and technicians. The entity had expected to retire the system many years ago. The earliest efforts to replace the system began in 2000. However, it was nine years before a new solution and a vendor was selected to proceed with the replacement. Although, management was aware of the EMS system's life expectancy, a decision was made to prolong the use of the system which did not adequately associate the risks or consequences of this decision.

Example 5: Lesson Learned/Corrective Action:

Despite best efforts to maintain a system, if the systems are kept for periods beyond their life cycle, reliability of the system can be affected. Hardware and software systems operating well past the end of life cycle are more prone to failure. Consideration should be given to update the system as soon as the vendor notifies the entity that support will no longer be provided by its original vendor or other third parties. However, it is also understood there are many reasons that may not permit immediate replacement when notification of end-of-life occurs; therefore, it is essential a detailed plan exists to address any issue that may arise due to the failure of the unsupported system(s).

**Summary**:
The five examples above provide a starting point to review and evaluate current EMS/SCADA software, testing and change management practices. One of the challenges of reviewing all of the EMS/SCADA events has been the capacity to gather detailed information. Loss of logs has prevented the ability for some entities to produce detailed reports or conduct thorough analyses. Creating a redundancy of recording logs may present an opportunity to conduct more detailed analysis when events occur in the bulk power system (BPS).

Lastly, due to the high number of EMS/SCADA events, the potential for a high alarm rate could create conditions for alarms to be disabled or silenced. Regardless of the nuisance, the purpose of audible alarms is to draw attention to an unusual situation with the potential of preventing further problems.

NERC estimates that the risk to BPS reliability from these events is **MEDIUM** due to the wide range of near misses and actual events that continue to occur on the BPS.

**Background:**

Category 2b events are defined as "Complete loss of SCADA, control or monitoring, functionality for 30 minutes or more." Despite the awareness within the industry from the three (3) lessons learned published by NERC in 2010, an opportunity for improvement exists in the reduction of EMS-SCADA events through greater examination in the three focus areas outlined within this alert.

**Contact:**

Earl Shockley
Director of Reliability Risk Management
(404) 446-2570
earl.shockley@nerc.net

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
(609) 452-1422
esisac@nerc.com

**Alert ID:** A-2012-04-10-01

*You have received this message because you are listed as a primary compliance contact for your organization on North American Electric Reliability Corporation's compliance registry. If you believe that you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact Trion King at NERC by calling (404) 446-9654 or emailing Trion directly at: trion.king@nerc.net.*

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560 www.nerc.com