NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

Preventable SCADA/EMS Events - II

This Industry Advisory is a continuation of the Advisory issued on April 10, 2012. This and the previous Advisory center on analysis of Category 2b Events reported through the ERO Event Analysis (EA) Process, where a complete loss of Supervisory Control and Data Acquisition (SCADA) monitoring or control occurred for more than 30 minutes. Industry, through the ERO EA Process, identified an additional 74 Category 2b Events between April 10, 2012 and January 27, 2014; this advisory is based on the analysis of the remaining 74 events. Energy Management Systems (EMS), comprising SCADA and Real Time reliability tools, are vital for maintaining situational awareness and making operating decisions at both the individual and the organizational level. Typically, EMS systems are extremely reliable and redundant; however, an outage of the EMS system increases risk to the reliability of the bulk power system. While it is critical to understand the importance of this Advisory, EMS outages will continue to occur and industry has demonstrated appropriate responses to EMS outages. Through the analysis of the Category 2b Events, the ERO can now more accurately assess the residual risk to the bulk power system from EMS outages.

About NERC Alerts >>

Status:	**No Reporting is Required – For Information Only**
	**PUBLIC**: No Restrictions. Will be posted to NERC's public Alerts website, and redistribution to interested parties is encouraged.
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, Interchange Authority, Load Serving Entity, Reliability Coordinator, Reserve Sharing Group, Transmission Owner, Transmission Operator. **Who else will get this alert? >>**

Primary Interest Groups:	Energy Management Systems (EMS) Operations Support Groups, System Operations – Transmission Engineering, System Operators Control Systems, Corporate IT, Generation Engineering, Generation Operations, Physical Security

Advisory:

This advisory is intended to highlight some of the most common EMS outage themes or challenges, recommend practices to remediate those challenges and share effective interventions, and operational actions entities have taken during EMS outages to maintain situational awareness and control of the bulk power system (BPS).

Category 2b of the NERC Event Analysis (EA) Program defines an EMS outage as a complete loss of SCADA, control or monitoring functionality for 30 minutes or more. A partial outage, categorized as 1h in the revised EA program in effect from October 1, 2013, is defined as loss of monitoring or control at a control center, such that it significantly affects the entity's ability to make operating decision for 30 continuous minutes or more. Examples include, but are not limited to loss of communications from SCADA remote terminal units (RTUs), unavailability of Inter-Control Center Protocol (ICCP) links reducing BPS visibility, loss of Automatic Generation Control (AGC), unacceptable State Estimator, Contingency Analysis solutions, etc.

In the April 2012 advisory, based on the analysis of 20 events, three recurring themes were identified: Software Failure, Testing, and Change Management. These three themes remain preeminent for root causes and the contributing causes based on the analysis of 74 events. The analysis of restoration times for the outages shows 57 minutes (mean) for a complete outage and 39 minutes (mean) for a partial outage.

'Software failure', the first recurring theme, is defined in the NERC Cause Code Assignment Process (CCAP) manual as "*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 corrective actions should involve the vendors of the software"*.

Software is ubiquitous in EMS systems. Software used in the EMS systems is typically vendor supplied base product with additional enhancements, some of which are developed in-house. It spans from low level operating systems installed on the servers, critical communication equipment, to advanced applications running on the servers. There are usually a plethora of technologies and languages used in the software.

Based on analysis of all the contributing causes that can be attributed to the 74 events, 33 of the events had software failure as a contributing cause. As the definition states, software failure is just an occurrence and not a true cause. The most common reason for the failures was a bug, defect, error, or improper configuration/installation/maintenance.

Some of the other contributing causes for the EMS outages attributable to software failure are listed below:

- Incorrect arguments passed to programs
- Incorrect permission issues in active programs
- Incorrect setting of application parameters
- Unawareness of features of vendor supplied software
- Improper configuration of Software
- Coding errors in various scripts such as health check, start up, clean up, synchronization, failover etc.
- Insufficient disk space
- Inadequate memory sizing or application memory leaks
- Unreleased semaphores leading to system resource deficiencies
- Locked files
- Bugs in the communication equipment operating system software
- Improper spanning tree implementation

Testing, the second recurring theme, is vital to making sure that software meets the requirements and specifications and does not negatively affect the functioning of the system. Testing plays a key role during the design/installation phase and during the startup/pre/post modification phase to the system.

Based on the analysis of all the contributing causes that can be attributed to the 74 events, 29 of the events had less than adequate testing as a contributing cause. The next few paragraphs present more specifics for these EMS outages.

There were several cases where software patches were not tested properly on the test environment prior to being placed on the production system. In some instances, the test systems were not set up similar to production systems resulting in errors on the production system. A prevalent issue in

many multi-site failovers is insufficient testing of the backup site functionality. Incomplete scope of testing, inadequate testing, and improper test procedures were also found as contributing causes for the EMS outages.

According to the NERC CCAP Manual, 'Post-maintenance/post-modification testing less than adequate (LTA)' is defined as *"The post-maintenance or post-modification testing specified was not performed or was performed incorrectly. The post-maintenance or post-modification testing was completed, but the testing requirements were less than adequate. The post-maintenance or post-modification testing was not performed in accordance with the schedule for testing."*

In many cases, the system was tested during factory acceptance; however, regression testing was not performed after additional changes were made on the system. The majority of events that fell into this category had changes tested on the primary site system only and not on the backup site system. Some examples include:

- Authentication servers were not tested after firewall rules were changed
- Substation circuits routing paths were updated, but only primary site was tested to verify connectivity
- Network device configurations were changed and only tested on the primary site

These factors became more important when the need for failover arose and the entity could not failover in a timely manner as the latent issues were discovered for the first time on the backup site systems.

'Inspection or testing less than adequate' is defined in the NERC CCAP Manual as "*Required inspection or testing was not established or performed for the equipment involved in the incident. The required inspection or testing was performed at an incorrect frequency. The acceptance criteria for the required inspection or testing were inadequately defined. All essential components were not included in the required inspection or testing*."

Some examples of EMS outages where inspection or testing was less than adequate include:

- Paper tests simulating expected behavior were conducted instead of actual real-time failover testing
- Interdependency of the domain servers was not tested when access to the backup site was given from the primary site consoles

- Passwords were changed on the system without adequate testing done to see the impact of the change on functionality of critical programs

Functional testing did not exist for the equipment or the system prior to placing them in service. Start-up testing was inadequate for the equipment or system being placed in service.

Inadequate start up testing where certain conditions are not tested at all during the site acceptance testing procedures caused some EMS outages. Some examples include:

- Disaster scenarios, fault tolerant scenarios for equipment were not tested
- Restrictions on the alarm length sizes were not discovered, as fault tolerant testing was not performed, leading to the loss of the alarm processor

Testing was not included as part of the design acceptance process. The testing did not verify the operability of the design. Design parameters did not successfully pass all testing criteria.

Some examples of less than adequate testing of design include:

- A new port scanning program was tested on the test system and without appropriate tuning it was installed on the production system, causing the EMS outage
- Vendor supplied batch file was not installed and tested on the test system, but was directly installed on the production system, causing the communications from the RTUs to stall
- Due to inherent design issues in the code, certain critical services were interrupted when system passwords were changed

Patches provided by the vendor need to be vetted and pushed to production system in safe and reliable manner. A good practice is to gather documentation from the vendor that the testing has been done at their site first, before carrying out the testing on-site.

'Change Management less than adequate' is the third recurring theme, and is defined in the NERC CCAP Manual as "P*roblems caused by the process by which changes are controlled and implemented by the management as organizational needs change to accommodate new business needs."*

Analysis of all contributing causes attributable to the 74 events revealed that over half of the events had less than adequate change management as a contributing cause. There are five distinct areas of change management to be considered.

1) Inadequate review or assessment of the risks and/or consequences associated with the change
2) Lack of system interactions consideration
3) Inadequate vendor support with changes
4) Changes not implemented in a timely manner and
5) Insufficient verification of accuracy/effectiveness of changes

Some examples for less than adequate change management include:

- Even though redundancy was set up for critical routers, power outage for one of the routers was not considered in the design and there were dependencies that were unknown until the event occurred
- The impact of a nonfunctioning alarm function was not considered in the design, as the entire EMS system failed
- Port scan software changes did not consider the tuning needed for the interaction with the real time servers
- Running multiple study applications on the real time servers did not consider the probability of insufficient system memory to support real time applications
- Lack of consideration given to system interactions when a change made to one subsystem affects another subsystem, such as Real Time Data Base Management sizing affecting front end processing
- Impact of third-party software such as Anti-Virus, Anti Spyware, Firewall, and intrusion prevention competing for resources on the systems was not considered
- Vendor did not test the batch file that was sent as a fix, and did not provide accurate instructions
- Even though entities were aware of the performance issues or outstanding issues, fixes were not timely to avoid the event
- Reduction of the database sizes, clean up or automation of cleanup of logs were not performed on a satisfactory schedule
- Some entities were aware of the changes needed to be made to their aging EMS system, but delayed implementing them resulting in an EMS outage

- Some entities were not made aware of vendor-identified problems or "bugs" found in other customers' systems that would be likely to impact them

Operating system and EMS vendors typically stop providing support services for older products and releases. EMS vendors do not always have the version/releases in house that an entity might require for support. Conversely, entities are reluctant to install a needed fix and purchase vendor support when system upgrades are planned for the near future.

Entities should have a plan for appropriate staffing resources during major hardware and software upgrades of EMS systems so that they will be prepared should the upgrade experience unanticipated problems. Upgrades on Primary and Backup sites should not be done simultaneously, decreasing the likelihood that a problem with an upgrade does not render both sites unavailable. Entities should also have plans to provide appropriate alternate monitoring and control capabilities at critical substations in the event that a failed upgrade causes a prolonged EMS outage.

Real-time Operational Response to an EMS Outage Positive observations from EMS outages include the remedial actions entities are taking when the event is transpiring, preventing the event from having an impact on the bulk power system. Effective actions include but are not limited to the following:

- Timely communications with neighboring system operators, generation plant operators and Reliability Coordinators.
- Communicating with various internal groups to address the problem efficiently.
- Directing plants to take local control with adjustment instructions to meet existing schedules.
- Contacting neighboring balancing authorities to check tie flows, calculating ACE manually and making generation adjustments through periodic voice communications with plants.
- Ensuring alternate monitoring of post-contingency conditions by communicating with Reliability Coordinators and neighbors.
- Assigning field personnel to staff critical substations.
- Staffing back up control centers with relief shift.
- Monitoring of critical system parameters using alternate means.
- Contacting the vendors and partnering, to identify and fix the problems.

- Designing redundant systems effectively, including addressing single point vulnerabilities.
- Making the effort to diagnose the causes (root and contributing) of events, and use this information to design and implement effective barriers to recurrence in addition to taking immediate stop gap measures.
- Performing changes on the system during appropriate times with operator approval to reduce the risk

Summary:

Software failures, testing, and change management are the three most common themes that were observed in the analysis of the aforementioned EMS outages. Entities are effectively making use of alternate means to operate the system when events transpire; however, entities and vendors need to continue to review and improve their testing practices and change management procedures to reduce the outage times and frequency. NERC will continue to analyze the events and share the findings to the industry. So far 17 lessons learned are published with nine in 2013. Click here for the lessons learned.

NERC hosted its first Monitoring and Situational Awareness conference, with the theme of 'Improving EMS Reliability' on September 18-19, 2013 in Denver, CO. The conference brought together more than 90 operations and EMS experts from more than 40 registered entities across all eight regions and Canada, as well as variety of vendors and consultants. The focus of the conference was to bring awareness of the issues and to share event response strategies. In addition, good practices in change management, managing EMS availability and robust testing methodologies were shared. Click here for presentations from the conference.

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. The event reports submitted by industry are improving and clearly demonstrate a commitment to reliability. NERC staff also developed supplemental questions for consideration for entities reviewing EMS outages. Click here for the supplemental questionnaire.

While it is important to understand the criticality of this Advisory, EMS outages continue to occur and industry has demonstrated appropriate responses. The ERO EA Process is tailored to provide a mechanism to identify, track and develop targeted remediation or intervention strategies for this and other reliability risks.

Background:	Category 2b events are defined as "Complete loss of SCADA, control or monitoring, functionality for 30 minutes or more." The NERC event analysis program has not seen category 2b events decrease in frequency or outage time. There were nine lessons learned that were published in 2013. This effort will continue until there is a reduction in the EMS outage time and frequency industry wide.
Contact:	Bulk Power System Awareness Group North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600 – North Tower Atlanta, GA 30326 (404) 446-9797 | nerc.alert@nerc.net
Alert ID:	

You have received this message because you are listed as a primary compliance contact for your organization on the 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 Bulk Power System Awareness at NERC by calling 404.446.9797 or via email at nerc.alert@nerc.net.

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