NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Addendum for Category 1h Events

Disclaimer: *This NERC Event Analysis (EA) document is a working document used for analyzing events in order to identify reliability risk to the North American Bulk Power System, to ensure and continuously improve reliability.This document cannot be used for compliance monitoring or enforcement purposes.Any statements or conclusions on this document will not prejudge the outcome of an event analysis or a potential compliance review associated with the same facts or circumstances. This document makes no findings regarding compliance with reliability standards.*

This addendum is intended to be used as a checklist for issues to consider when developing an Event Report for Category 1h events. The intent is to ensure all pertinent information is provided to facilitate a comprenhensive understanding of the event and allow for detailed root cause analysis and the development of quality lessons learned. It is not intended that all items below are material to every event. Your comments are welcomed and appreciated. Please provide comments to nercea@nerc.net.

Category 1h
Loss of monitoring or control at a control center such that it significantly affects the entity's ability to make operating decisions for 30 continuous minutes or more.

Some examples that should be considered for EA reporting include but are not limited to the following:

- Loss of operator ability to remotely monitor or control Bulk Electric System (BES) elements
- Loss of communications from SCADA Remote Terminal Units (RTU)
- Unavailability of intercontrol center communications protocol (ICCP) links, which reduces BES visibility
- Loss of the ability to remotely monitor and control generating units via automatic generation control (AGC)
- Unacceptable state estimator or real time contingency analysis solutions

When completing an Event Report, the following information should be included:

1. What was the duration of the outage?
2. Elaborate on the initiating cause**,** all the identified contributing causes**,** and the root cause, if any, for the event. We suggest performing root cause analysis and, if applicable, extended conditions evaluation.
3. Which specific energy management system (EMS) applications systems were outaged that impacted your ability to make operating decisions? (AGC, Real Time Applications (SE, CA), ICCP etc.) What were the impacts?

4. Background information and description of the EMS (e.g. design, requirements or architecture of the EMS), if you feel it would allow for a better understanding of the event.
5. Were there consequential system changes; such as, generation changes, load changes, disturbances and equipment operations, tie line flow that are material to the event?
6. Were there other means available to monitor and control the system during the event and were the Reliability Coordinators (RCs) and neighbors notified?
7. Elaborate on the corrective actions that have been taken so far, mitigation plans for future and follow up activities. Were there any lessons learned or recommendations that you would like to share based on the conclusions drawn from this event?
8. Were there any human performance issues that contributed to this event? Was it a knowledge, role, or skill-based issue? Does the entity have training programs established for training?
9. Was inadequate testing of changes a contributing factor for the event? Are there adequate systems in place to test? Did the entity feel that the testing should have caught this issue before it showed up on the production system? Was post modification testing appropriately performed? Were the test plans or procedures changed post event? Please elaborate on this as we are seeing a growing trend of less than adequate testing as a root cause for a significant number of events.
10. Were there any contributing written or verbal communication issues between EMS and Operations staff that occurred leading up to or during the event? If a particular task was a contributing factor, were there written procedures for performing that task. Is it a fairly routine task?
11. Were the problems identified experienced prior to this event? If so, when and how frequently were they seen? Were any corrective actions put in place for the problem? Did the entity take appropriate actions to correct it?
12. Was there redundancy available for the servers/equipment? Did the redundant systems work as expected? If not, please elaborate on failovers not working properly. Were the failovers tested properly?
13. Is multi-site failover testing done via desktop drills or actual testing performed? Was the backup center functionality tested prior to the event? If so, how often is the backup control center functionality tested?
14. Were any design issues, with the software or hardware, identified as a cause for the event? Was there a need identified to change the design, requirements, or architecture of the EMS? Was the backup system/server architecture a contributing factor? Were those set up for failover? Please provide the rationale for the change and any lessons learned that can be shared with the industry.
15. Was the entity up to date with the software and hardware patches? Were all the patches/fixes applied that needed to be applied? Could this problem have been prevented if the patches were applied on time? If enough information is not provided in the report, please elaborate.
16. Was the EMS vendor informed about the event? Did the vendor investigate the problem? Did they have any more insight on the event? Did they play a role in the event analysis? Was the

documentation and support that they provided satisfactory for the entity? Did the vendor have the test systems that were similar to the entity system? Did they test this off-site before changes were shifted onsite?

17. Are all EMS system parameters appropriately sized? Were system limits a contributing factor?
18. Were there any indications of potential occurrence prior to this event happening? If so, were steps taken to mitigate the issues prior to the event?
19. Were there appropriate procedures in place for change management? Was the risk assessed properly before the change was implemented? Was the change scoped properly and all the necessary parties updated?
20. Were there enough system resources available to carry out the actions ? Were there any performance issues noticed on the system when the event was transpiring?
21. If the event occurred coincident to a scheduled or planned maintenance or update procedure, how often do you execute that particular maintenance or update procedure?
22. Was any new software/hardware added that may have contributed to the event? Please provide information on identified routines or components that contributed to the event.
23. Were there any telecommunication changes on the nework, such as routers, firewalls, access control lists, software/hardware maintenance, etc. that may have prevented normal SCADA data flow?
24. If the event prevented downstream application, like state estimator from solving, was a redundant system available to back up the monitoring functionality? As an example, an RTO may be the backup system.