NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reference Guideline for Category 1h Events

This reference guideline 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 comprehensive 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 NERC.EventAnalysis@nerc.net.

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

Overall Information

1. Elaborate on the initiating cause, all the identified contributing causes, and the root cause, if any, for the event. Root cause analysis and, if applicable, extended conditions evaluation, should be used to provide a better understanding of the event.
2. 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
3. Elaborate on the corrective actions that have been taken so far, mitigation plans for future and follow up activities.
4. Elaborate on the consequential system changes; such as, generation changes, load changes, disturbances and equipment operations, tie line flow that are material to the event.

Cyber Information

1. What was the impact on confidentiality and integrity of information during this event? For example, did a firewall or networking device 'fail open' and allow all traffic to pass (confidentiality), or was a database or telemetry corrupted during the event (integrity)?
2. Could this event have degraded existing security controls during the event or recovery? Did your organization's information security staff review logs from the event time frame to understand any potential insights beyond the EMS and SCADA infrastructure?

Backup and failover

1. When was the multi-site failover testing last preformed?
2. When was the backup functionality last tested?

Change Management

1. Have you seen the similar but less severe events prior to this event? If so, when and how frequently did they occur? Were any corrective actions put in place to address those previous events?

2. Were the EMS systems current with the software and hardware patches? Could this problem have been prevented if the patches were applied on time?

Maintenance

1. 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?
2. How was the risk assessed properly before the change was implemented?
   a. How was the change scoped?
   b. How was testing of changes preformed before the change was implemented to the production system?
   c. Were there appropriate procedures in place for change management?
3. 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?
4. Were there any telecommunication changes on the network, such as routers, firewalls, access control lists, software/hardware maintenance, etc. that may have prevented normal data flow?

Human Performance

1. Could this have been a Human Performance related issue?
   a. Would a different person have executed the task correctly?
   b. Was it a knowledge[1], rule[2], or skill-based[3] issue?
   c. Does the entity have training programs established for training?

Vendor Support

1. What insights/solutions have the EMS vendor provided?
2. What insights/solutions have the Telecom vendor provided?

Lessons Learned

1. Were there any lessons learned or recommendations that you would like to share based on the conclusions drawn from this event?

[1] **Knowledge Base** — Behavior in response to a totally unfamiliar situation (no skill, rule, or pattern recognizable to the individual); a classic problem-solving situation that relies on personal understanding and knowledge of the system, the present state of a system, and the scientific principles and fundamental theory related to the system; an activity performed with no preprogrammed instructions or rules.
[2] **Rule Base** — Behavior based on selection of stored rules derived from one's recognition of the situation; follows IF (symptom X), THEN (situation Y) logic; an activity performed following stored rules accumulated through experience and training.
[3] **Skill Base —** Behavior associated with highly practiced actions in a familiar situation, usually executed from memory without significant conscious thought; an activity performed using stored patterns or preprogrammed instructions.