NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reference Document
Risks and Mitigations for Losing EMS Functions

Introduction

Energy Management System (EMS) is a system of computer-aided tools used by System Operators to monitor, control, and optimize the performance of generation and/or transmission systems. EMS, which encompasses Supervisory Control and Data Acquisition (SCADA), telecommunications and real-time reliability support tools, is vital for situational awareness and making and implementing well-informed operating decisions.

The purpose of this reference document is to identify and discuss the risk of losing EMS functions, analyze the causes of EMS events reported through the Electric Reliability Organization (ERO) Event Analysis Process (EAP), and share mitigation strategies to reduce these risks [1].

The ERO EAP is an effective tool for analyzing the reported events and identifying risks. Through the EAP, the registered entities, with the help of NERC and the regions, identify the root and contributing causes of EMS events and share this information with industry through Lessons Learned publications. Additionally, the NERC Monitoring and Situational Awareness Conference is a collaborative effort of industry and vendors. Experts gather to discuss these Lessons Learned and share best practices to minimize the frequency and duration of EMS outages. The conference takes place annually in the fall.

The following are concluded in the reference document:

- Software and telecommunications failure are major contributors to the loss of EMS functions.
- The loss of EMS functions has not directly led to the loss of generation, transmission lines, or customer load.
- Mitigating actions have been effectively applied during EMS events to manage risks within acceptable levels.
- The EAP is used to analyze, track, and trend these outages. Lessons Learned and best practices are shared with industry to improve overall EMS performance.
- The NERC Monitoring and Situational Awareness Conference provides a forum for vendor involvement to share knowledge and collaborate with industry to minimize the frequency and duration of EMS outages.

Changes to this reference document will be at the direction of the NERC Operating Committee (OC).

[1] This reference document is provided for guidance and does not reflect binding norms or mandatory requirements.

What is an Energy Management System and why is it important?

An EMS is a system of computer-aided tools used by System Operators to monitor, control, and optimize the performance of the generation and/or transmission system. EMS, which encompasses SCADA, telecommunications and real-time reliability support tools, is vital for situational awareness and making and implementing well-informed operating decisions. EMS consists of both hardware and software. The hardware part of the EMS consists of remote terminal units (RTUs) at the substations, computer servers at the data centers, the telecommunications systems both wired and wireless, plus the system control centers including all the computers used to monitor and control the BES. The software component of the EMS consists of application programs for the data acquisition, control, alarming, real-time calculations, and network analysis of power systems including state estimation, contingency analysis

The primary objective of the EMS is to provide situational awareness to the System Operators [2] and allow remote control of devices to provide secure and stable operation of the BES. The situational awareness includes but is not limited to:

- Monitor/control the frequency within the System Operator's Area
- Monitor/control the status (open or closed) of switching devices, plus real and reactive power flows on generators, BES tie-lines and transmission facilities within the System Operator's Area
- Monitor/control voltage and reactive resources
- Monitor the status of applicable EMS applications such as Real-Time Contingency Analysis (RTCA) and/or alarm management

Using this information, the System Operators make decisions that affect the reliability and resiliency of the BES. Generation can be dispatched or taken off-line to prevent overloads or improve the voltage in an area. Capacitor banks, shunt devices, synchronous condensers or other voltage-controlling tools can be utilized to maintain voltage limits. Transmission breakers and remote-controlled switches can be opened and closed as needed to address real-time and contingency conditions.

In the EMS, application programs are run in a real-time as well as an extended real-time environment to keep the power system in a secure operating state. These EMS applications include SCADA, Alarm Processing, Automatic Generation Control (AGC), Network Applications (which includes State Estimation), Power Flow, Contingency Analysis or Security Analysis (CA or SA), and Data Historians, among others. Figure 1 shows a simplified EMS configuration.

[2] Please refer to NERC Reliability Guideline " Situational Awareness for the System Operator" http://www.nerc.com/comm/OC_Reliability_Guidelines_DL/SA_for_System_Operators.pdf.

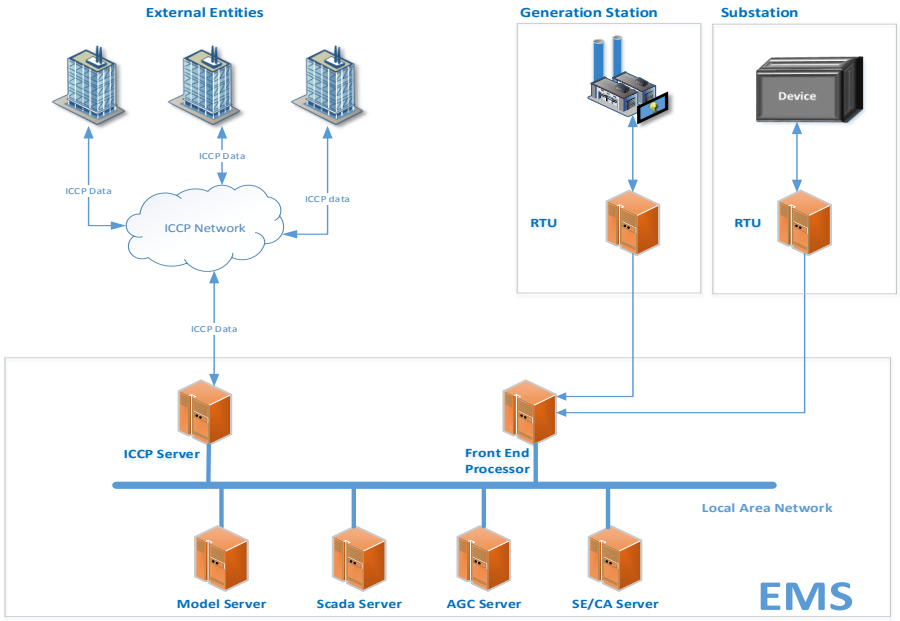

Figure 1 A simplified EMS configuration

Inter Control Center Protocol (ICCP) has been standardized under the IEC 60870-6 specifications and allows the exchange of real-time and historical power system monitoring and control data, including measured values, data quality codes, scheduling data, energy accounting data, and operator messages. Data exchange can occur over wide area networks between utility control centers, utilities, power pools, regional control centers, and non-utility generators.

Supervisory Control and Data Acquisition is a category of software application programs for process control and the gathering of data in real-time from remote locations in order to control devices and monitor conditions. SCADA sends and receives telemetered data between the RTU or ICCP link and the control center. Control signals are sent from the operator's desk at the control center back to the field to change the status of devices (e.g. open or close breakers) or adjust generation.

Remote Terminal Unit is a microprocessor-controlled electronic device that interfaces devices in the physical world to a distributed control system or SCADA system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected devices.

Front End Processor (FEP) interfaces the host computer to a number of networks, such as systems network architecture, or a number of peripheral devices, such as RTU's, terminals, disk units, printers and tape units. Data is transferred between the host computer and the front end processor using a high-speed parallel interface. The front end processor communicates with peripheral devices using slower serial interfaces, usually also through communication networks. The purpose is to off-load from the host computer the work of managing the peripheral devices, transmitting and receiving messages, packet assembly and disassembly, error detection, and error correction.

Automatic Generation Control is an application for adjusting the power output of multiple generators at different power plants in response to changes in interchange, load, generation, and frequency error. The AGC software uses real-time data such as frequency, actual generation, tie-line load flows, and plant controller status to determine generation changes.

State Estimator (SE) is an application that calculates the current state of the electrical system (the voltage magnitudes and angles at every bus) using a network model and telemetered measurements. The purpose is to provide a consistent base case for use by other network applications programs such as Power Flow and Contingency Analysis. While SCADA relies on direct telemetered values from the RTUs, the State Estimator is able to calculate and predict non-metered values to provide additional situational awareness to the System Operators.

Real-time Contingency Analysis is an application used to predict electrical system conditions after simulating specific contingencies. It relies on a base case from a State Estimator or Power Flow case.

In the EMS, voltage magnitudes and power flows over the lines are continuously monitored through SCADA, SE and RTCA to check for voltage/thermal exceedances. The EMS system is programmed with limits on the BES equipment. These limits are used with Alarm Processing to send visual and audio alarms to the System Operators when monitored quantities are approaching or exceeding the threshold of an operating limit. AGC computes a Balancing Area's Area Control Error (ACE) from interchange and frequency data. ACE determines whether a system is in balance or adjustments need to be made to generation. AGC software, while observing ACE, determines the required output for generating resources while observing energy balance and frequency control by sending set-points to generators. The scheduled tie line power flows are maintained by adjusting the real power output of the AGC controlled generators to accommodate fluctuating load demands.

The typical dependency between main EMS applications is illustrated in Figure 2.

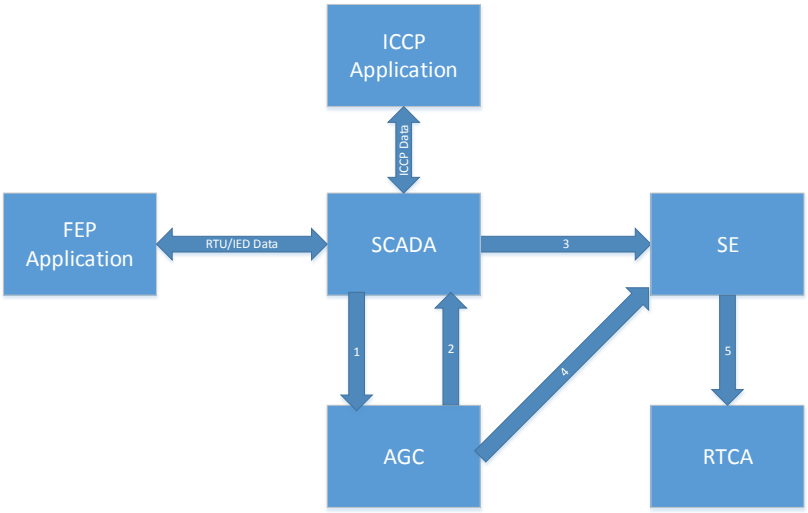

Figure 2 Typical dependency between main EMS Applications

The data flows between EMS functions shown in **Figure 2** are described below:

- ICCP Data (between ICCP Application and SCADA): real-time and historical power system monitoring and control data, including measured values, data quality codes, scheduling data, energy accounting data, generator set-point controls and operator messages
- RTU Data (between FEP Application and SCADA): data from Substation Devices and commands to Substation Devices
  - Measured Values
  - Position Indication
  - Positioning Commands
  - Alarms
- Path 1 (from SCADA to AGC): telemetered status data and analogue value data
  - Area frequency
  - Tie line MW
  - Generator unit online/offline
  - Generator unit control local or remote
  - Generator unit MW output
  - Generator unit MW set-point feedback
  - Generator unit MW limits
- Path 2 (from AGC to SCADA): new set-point controls calculated by AGC
- Path 3 (from SCADA to SE): the data typically consists of
  - Breaker statuses (open or closed)
  - Switch statuses (open or closed)
  - Transformer tap settings
  - MW flow measurements
  - MVAR flow measurements
  - Voltage magnitude measurements
  - Current magnitude measurements
  - Phase angle difference measurements
  - High-Voltage Direct Current (HVDC) operating modes
  - Tagging statuses
  - Special measurements defined by users

- Path 4 (from AGC to SE): the data typically consists of
  - Generator unit control (local or remote)
  - Generator unit MW output
  - Generator unit MW limits
- Path 5 (from SE to RTCA): A base case solution
  - System topology
  - Voltage magnitudes and angles at each bus
  - Transformer tap settings
  - Generator unit control statuses
  - Generator unit MW limits
  - HVDC operating modes
  - VAR statuses

Analysis of Loss of EMS Functions

This chapter will identify and discuss the risks of the loss of EMS functions, analyze reasons for the loss of EMS functions based on the EMS events reported by 130 NERC Compliance Registries (NCRs) between October 2013 and April 2017, and present mitigation strategies that reduce the risk when one or more EMS functions are temporarily lost or disabled.

Risks of Loss of EMS Functions

Situational awareness is necessary to maintain reliability, anticipate events and respond appropriately when or before they occur. Without the appropriate tools and data, System Operators may have degraded situational awareness for making decisions that ensure reliability for the given state of the BES. Certain essential functional capabilities must be in place with up-to-date information for staff to make informed decisions. An essential component of monitoring and situational awareness is the availability of information when needed. Unexpected outages of functions, or planned outages without appropriate coordination or oversight, can leave System Operators with impaired visibility. While failure of a decision-support tool has not directly led to the loss of generation, transmission lines, or customer load, such failures may hinder the decision-making capabilities of the System Operators during a disturbance. NERC has analyzed data and identified that short term outages of tools and monitoring systems are not uncommon, and the industry is committed to reducing the frequency and duration of these types of events.

The BES reliability risk due to EMS function failures varies depending on the function that is lost plus the duration of that outage.

- The loss of SCADA would likely be the most impactful EMS failure. The System Operators would not have indication of the status of devices or key data points such as MW, MVAR, current, voltage, or frequency from the RTUs. Furthermore, the System Operators would not be able to

open and close breakers or switches remotely from the control center. SCADA data feeds AGC, SE/RTCA applications. Loss of quality data would compromise their functionality.

- The loss of ICCP would disrupt the information that is shared between Transmission Operators (TOP), Balancing Authorities (BA), Generator Operators (GOP), and Reliability Coordinators (RC). The RCs rely on information from its BAs and TOPs to monitor the wider area, and an ICCP outage may remove real-time updates to the affected section of the model.
- The loss of SE would involve the System Operators losing the situational awareness not directly provided by the SCADA system. While the System Operators would still have SCADA which would be control and indication of all telemetered devices, the loss of SE would eliminate other key data values that help the System Operators monitor the system, plus limit the predictive analysis that the EMS provides.
- The loss of RTCA may prevent alerting the System Operators when the next contingency presents a potential reliability issue, compromising situational awareness, increasing the complexity of performing Real Time Assessments, and reliability.

Reasons for Loss of EMS Functions

There were 318 EMS events reported between October 2013 and April 2017 through the EAP which will be further discussed in the following chapter. These include the loss of SCADA, ICCP, RTU, AGC, SE, RTCA, or a combination of these functions for 30 or more continuous minutes. Figure 3 shows the number of reported EMS events per loss of EMS functions. From Figure 3, it was found that loss of ability to monitor or control and loss of state estimator and/or RTCA are the two most common failures encompassing 75% of reported EMS events.

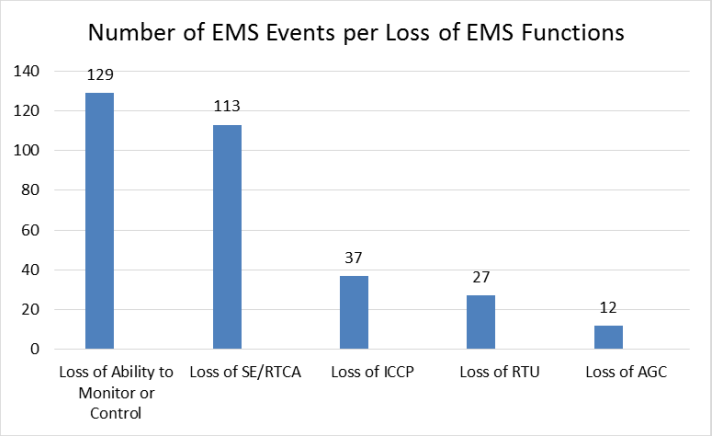

Figure 3 Number of reported EMS Events per Loss of EMS Functions

After further study, the reported EMS events can be grouped by the following attributes:

- **Software** – software defects, modeling issues, database corruption, memory issues, etc.
- **Communications** – devices issues (for example, RTU failure, FEP failure, fiber failure, network router failure,) or changes made (for example, firewall failure) or less than adequate system interactions (for example, bad telemetered data quality).

- **Facility** – loss of power to the control center or data center, fire alarm, AC failure, etc.
- **Maintenance** – system upgrades, job-scoping, change-management, risk identification and other themes such as testing in a controlled environment and implementing the change. For example, system/software configuration or settings failure, patch change, or implementation that causes EMS functions to crash.

Table 1 shows the breakdown of the attributes in each EMS function failure. Software and communications are significant contributors to loss of EMS functions.

Table 1 Contributors to Loss of EMS functions

Failure	Communications	Software	Facility	Maintenance	Total
Loss of Ability to monitor or control	28	24	49	28	129
Loss of SE/RTCA	28	77	3	5	113
Loss of ICCP	37				37
Loss of RTU	27				27
Loss of AGC	2	9		1	12
Total	**122**	**110**	**52**	**34**	**318**

Mitigations for the Risk of Loss of EMS Functions

In all of the reported events from October 2013 to April 2017, there has been no EMS event that directly led to the loss of generation, transmission lines, or customer load. The following mitigations have been effectively applied to manage the risks within acceptable levels:

- Enhanced system restoration plans, including drills and training on the procedures, plus real-life practice implementing the procedures.
- Overlapping coverage of situational awareness with RCs and neighboring TOPs and BAs – the system is being continuously monitored by additional entities outside of that immediate footprint. This is further strengthened by additional ICCP data points from generators and tie-lines that can provide visibility.
- Offline tools (studies) that can be used for analyzing contingencies plus other contingency-analysis including day-ahead studies, seasonal and standing operating guides, and System Operator training.
- Short durations – due to the continuous improvement of detective controls to identify when the EMS functions are not operating properly plus corrective controls to get them back up and running (either backing out of a change, or removing a piece of the model that is not converging). The 318 reported EMS outages from October 2013 to April 2017 were approximately 73 minutes in duration on average.
- Enhanced preventive controls including limits and bounds on external data where the SE/CA can converge around the erroneous data.

- Backup tools and functionality including backup EMS systems, backup control centers, and other additional redundancy.
- Collaboration with vendors to build comprehensive testing procedures and/or troubleshoot the cause of the failure in order to minimize the system recovery time.
- Manning substations so that System Operators and field personnel can take action as needed (open/close breakers), verify status of devices, plus verify power flows and voltages.
- Internally defined conservative operations procedures used during EMS events (no switching, additional monitoring, manning substations, asking neighbors for assistance)
- Several layers of communications (phones, cell phones, satellite, radio, email, all-calls, RCIS) as needed.

Furthermore, FERC and NERC conducted a study – Planning Restoration Absent SCADA or EMS (PRASE)[3] – that focused on the potential impact of the loss of EMS, SCADA, or ICCP functionality on system restoration, and the manner in which such impact could be mitigated. The objective of the study was to assess entities' system restoration plan steps in the absence of EMS, SCADA, and/or ICCP data, and identify viable resources, methods or practices that would expedite system restoration despite the loss of such systems. It was concluded in the PRASE report that

- All volunteer registered entities have made significant investments in their SCADA and EMS infrastructures, including leveraging redundancies to increase availability and functionality.
- All volunteer registered entities would remain capable of executing their restoration plan without SCADA/EMS availability
- Five recommendations are provided for all entities responsible for system restoration.
  - Planning for backup communications measures
  - Planning for personnel support during system restoration absent SCADA
  - Planning backup power supplies for an extended period of time
  - Analysis tools for system restoration.
  - Incorporating loss of SCADA or EMS scenarios in system restoration training

Event Analysis Process

The ERO EAP was launched in October 2010. The ERO EAP is intended to promote a structured and consistent approach to performing event analyses in North America. Through the ERO EAP, the ERO strives to develop a culture of reliability excellence that promotes aggressive self-critical review and analysis of operations, planning, and critical infrastructure protection (CIP) processes. The ERO EAP also serves an integral function as a learning opportunity for the industry by providing insight and guidance by identifying

[3] Please refer to "FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans" https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf

and disseminating valuable information to owners, operators, and users of the bulk power system who enable improved and more reliable operation. EMS events are defined in Cat 1h[4] events.

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:

i. Loss of operator ability to remotely monitor or control BES elements

ii. Loss of communications from SCADA Remote Terminal Units (RTU)

iii. Unavailability of ICCP links, which reduces BES visibility

iv. Loss of the ability to remotely monitor and control generating units via AGC

v. Unacceptable state estimator or real time contingency analysis solutions

The process involves identifying what happened, why it happened, and what can be done to prevent reoccurrence. Identification of the sequence of events answers the "what happened" question and determination of the root cause of an event answers the "why" question. It also allows for events to have cause codes or characteristics and attributes assigned, which can then be used by the Event Analysis Subcommittee (EAS) to identify trends. Trends may identify the need to take action, such as a NERC Alert, or may support changes to Reliability Standards.

More than 160 entities reported EMS events and participated in the ERO EAP since 2010. To-date, more than 130 Lessons Learned[5] documents have been posted and shared with the industry, with more than 40 Lessons Learned specifically dealing with EMS-related issues. The ERO EAP has proven to be an effective method for analyzing EMS outages and the industry has readily participated without a NERC Reliability Standard. Focusing on the root and contributing causes helps to determine the appropriate mitigating actions, and these lessons are shared with industry. The information gathered is disseminated and shared with industry at the annual NERC Monitoring and Situational Awareness Conference, highlighted below.

NERC Monitoring and Situational Awareness Conference

As the ERO, NERC is committed to continuous learning and improvement of bulk power system reliability. Beginning in 2013, NERC has hosted an annual Monitoring and Situational Awareness Conference. The conference creates awareness of common problems observed by utilities, promotes an exchange of ideas, shares good industry practices, and brings together expertise from various utilities and vendors in a collaborative, educational atmosphere. The ERO EAP captures lessons learned and common trends for EMS outages and makes them available to industry by creating awareness and involving stakeholders in a collaborative process, many challenges can be effectively mitigated. The ultimate goal is to minimize the outages, in terms of both EMS outage duration and frequency; with the objective of maintaining the highest levels of situational awareness.

[4] For the lastest category definition, please refer to http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx
[5] Please refer to http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

The themes of the conferences since 2013 are listed below, and the presentations are available on NERC's website[6]:

2013	Industry practices for reducing the EMS outages, alleviating risks involved when outages occur and maintaining situational awareness
2014	Sustaining EMS Reliability
2015	The tools and monitoring capabilities of both EMS/SCADA systems and third party software that gives System Operator's the real-time "bird's eye" view of system conditions
2016	EMS resiliency with an emphasis on the capacity to recover quickly from difficulties
2017	EMS Solution Quality (Modeling and Real-time Assessment)

Conclusion

This reference document describes EMS functions and components. Its primary contribution is to identify and discuss BES reliability risks due to the loss of EMS functions, analyze causes of loss of EMS functions based on EMS events reported between October 2013 and April 2017, and present mitigations used by industry to reduce the number and impact of EMS events. This reference document also highlights the work the ERO EAP does with analyzing these events and sharing this information with industry. These lessons learned and trends are also shared at the annual NERC Monitoring and Situational Awareness Conference. This conference is a collaboration with industry and vendors to minimize the duration and frequency of EMS outages and their potential reliability impacts to the BES.

The following can be concluded:

- Software and communication failures are significant contributors to the loss of EMS functions.
- The loss of EMS functions has not directly led to the loss of generation, transmission lines, or customer load. However, it is important to note that the loss of EMS functionality has contributed to cascading events because it limited system operators capability to maintain situational awareness.
- The ERO EAP is an effective process for analyzing these risks by identifying the root and contributing causes and sharing this information with industry
- "Good utility practice" mitigations have been effectively applied during EMS events to manage risks within acceptable levels.
- Enhanced system restoration plans, including drills and training on the procedures, plus real-life practice implementing the procedures.
- Overlapping coverage of situational awareness with RC's and neighboring TOPs and BAs – the system is being continuously monitored by additional entities outside of that immediate footprint. This is further strengthened by additional ICCP data points from generators and tie-lines that can provide visibility.

[6] Please refer to http://www.nerc.com/pa/rrm/Resources/Pages/Conferences-and-Workshops.aspx

- Offline tools (studies) that can be used for analyzing contingencies plus other contingency-analysis including day-ahead studies, seasonal and standing operating guides, and System Operator training.
- Short durations – due to the continuous improvement of detective controls to identify when the EMS functions are not operating properly plus corrective controls to get them back up and running (either backing out of a change, or removing a piece of the model that is not converging). The 318 reported EMS outages from October 2013 to April 2017 were approximately 73 minutes in duration on average.
- Enhanced preventive controls including limits and bounds on external data where the SE/CA can converge around the erroneous data.
- Backup tools and functionality including backup EMS systems, backup control centers, and other additional redundancy.
- Collaboration with vendors to build comprehensive testing procedures and/or troubleshoot the cause of the failure in order to minimize the system recovery time.
- Manning substations so that System Operators and field personnel can take action as needed (open/close breakers), verify status of devices, plus verify power flows and voltages.
- Internally defined conservative operations procedures used during EMS events (no switching, additional monitoring, manning substations, asking neighbors for assistance)
- Several layers of communications (phones, cell phones, satellite, radio, email, all-calls, RCIS) as needed.

Considering the average outage time (73 minutes) of the 318 events reported by 130 NCRs from October 2013 to April 2017, it was observed that the actual EMS availability was 99.99%[7] during the term. Therefore, the mitigation strategies described above have been proven to work effectively. To further enhance EMS availability, ERO will work directly with the stake-holders to maintain the EAP momentum, continue data gathering, track and trend the risk, conduct analysis, develop solutions, and share the information.

[7] Considering the average outage time (73 minutes) of the 318 reported events from October 2013 to April 2017,
Total down time (in minutes) = 318 events * 73 minutes/event = 23214 minute.

Assuming that any distinct NCRs submitting a report regarding EMS outage has an EMS system,
Total time (in minutes) =130 entities * 60 min/hr * 24hr/day * 1307 days = 244670400 minutes.

Therefore,
System Availability = (Total Time – Total Downtime)/Total Time
= (244670400 – 23214) / 244670400
= 0.9999051 ~ 99.99%