NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Analysis and Risk Mitigations for Loss of EMS Functions (2018–2020)

December 2021

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface iii

Executive Summary iv

- Key Findings v
- Considerations vi
  - The ERO Enterprise vi
  - The Entities vi

Introduction vii

- Background vii
- Scope and Purpose vii
- Commonly Used Terms within This Document viii

Chapter 1: Approach and Data 1

Chapter 2: Analysis and Assessment 2

- Overview Analysis 2
- Analysis of Entity Reliability Functions 4
  - Reliability Coordinators 5
  - Transmission Owners and Transmission Operators 7
  - Balancing Authorities 10
  - Generation Owners/Generation Operators 11
- Analysis of Root Causes and Contributing Causes 11
  - Event Root Causes 11
  - Contributing Causes 13

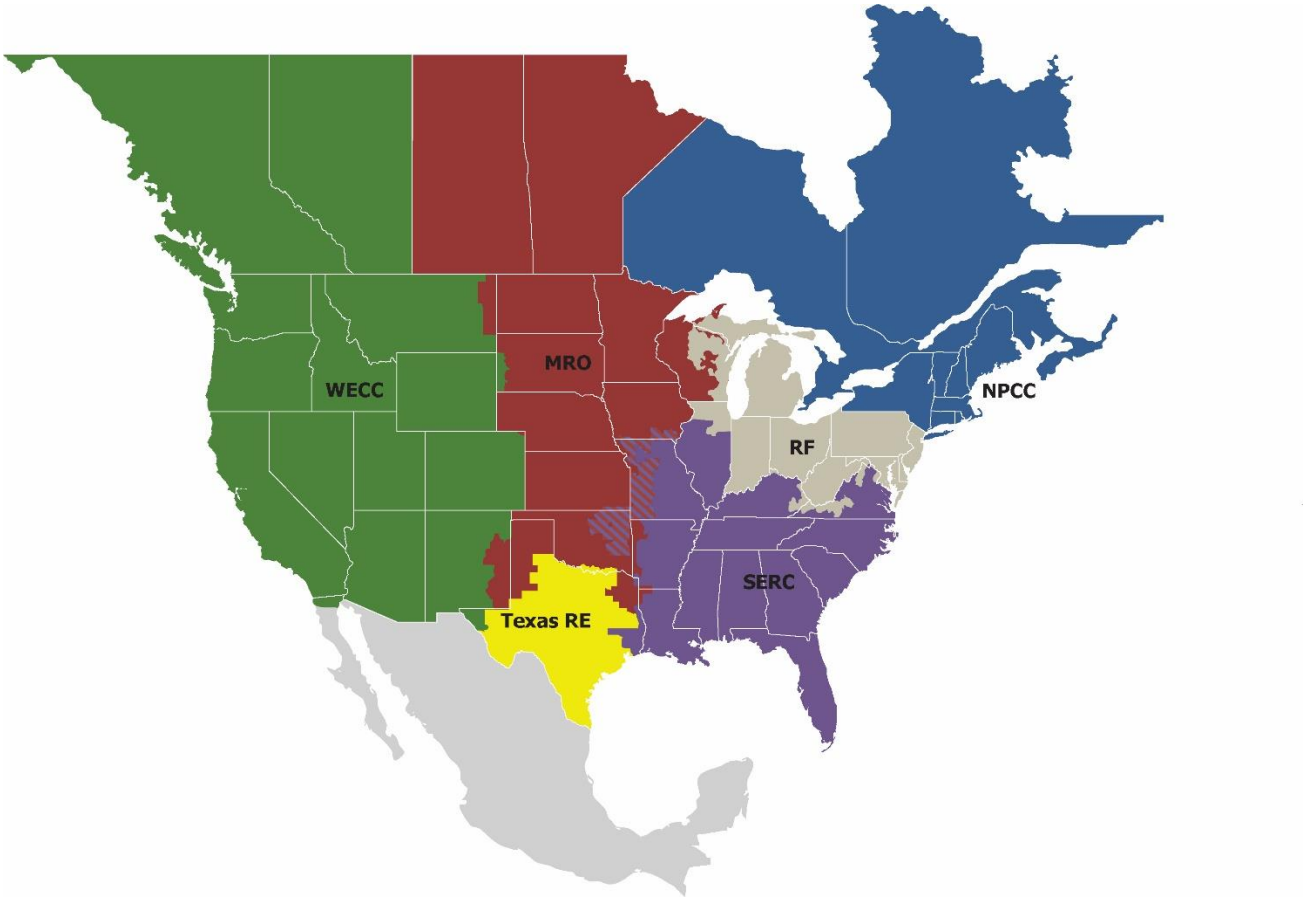
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TO)/Operators (TOP) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Loss of situational awareness is one of eleven risks identified in the *2021 ERO Reliability Risk Priorities Report*.[1] Loss or degradation of situational awareness poses BPS challenges as it affects the ability of personnel or automatic control systems to perceive and anticipate degradation of system reliability and take pre-emptive action.

An energy management system (EMS) is an automatic control system used by many entities that supports situational awareness. The primary objective of the EMS is to help system operators maintain situational awareness through automated means and enable remote control of devices to ensure secure and stable operations of the Bulk Electric System (BES).

The NERC Energy Management System Working Group (EMSWG) published the reference document *Risk and Mitigations for Losing EMS Functions* [2] in December 2017 and published a revision[3] in March 2020. The reference document contains analysis of 521 EMS events reported through the voluntary ERO Event Analysis Process (EAP) between October 2013 and April 2019. The document includes identification and a discussion of reliability and security risks due to the loss of EMS functions and presents risk mitigation strategies used by industry.

The ERO EAP is intended to promote a structured and consistent approach to performing event analyses. The events analyzed in the ERO EAP come from mandatory processes (e.g., EOP-004, OE-417) and a voluntary process that encourages entities to share their EMS events that do not meet the reporting threshold of the mandatory processes but meet the Category 1h event definition in the ERO EAP.

Of particular importance when considering the role of the EMS on the BES is the recent modification of the standard EOP-004-4, which clarified the reporting task concerning the loss of situational awareness as being the complete loss of monitoring or control capability at a staffed BES control center for 30 continuous minutes or more. The clarifying standard went into effect on April 1, 2019, in the United States and several Canadian provinces. Since that time, the standard may potentially modify entity interpretation of the need to provide visibility on partial EMS functions loss that is used for trending analysis and reported through the ERO EAP as defined by Category 1h. Therefore, the NERC EMSWG conducted an assessment and published *NERC Energy Management System Performance Special Assessment (2018–2019)*[4] as an interim activity between recurring updates to its EMS reference document by using 2018–2019 EMS events reported through the ERO EAP.

The year 2020 was the first full year that the standard EOP-004-4 was in effect. To gain a better resolution on the contribution of EMS outages to the loss of situational awareness risk and the effect of EOP-004-4, the ERO Event Analysis Program identified a need to continue the analysis by adding 2020 EMS events reported through the ERO EAP into the study period. This document includes analysis for three factors (outage duration, EMS functions, and entity reliability functions), examining associated trends, event root causes, and contributing causes identified through the ERO Cause Code Assignment Process (CCAP) for the 2018–2020 period.

[1] *2021 ERO Reliability Risk Priorities Report:*
https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf

[2] *Risk and Mitigations for Losing EMS Functions Reference Document—Version 1*:
https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Risks_and_Mitigations_for_Losing_EMS_Functions_Reference_Document_20171212.pdf

[3] *Risk and Mitigations for Losing EMS Functions Reference Document—Version 2*:
https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Risks_and_Mitigations_for_Losing_EMS_Functions_v2.pdf

[4] *NERC Energy Management System Performance Special Assessment (2018–2019)*
https://www.nerc.com/pa/rrm/ea/PapersDocumentsAssessmentsDL/EMS_Special_Assessment_March2021.pdf

Key Findings

Based on data and information collected for this document, the following key findings were identified:

- **EMSs were highly reliable from 2018–2020.**
  From 2018–2020, the loss of EMS functions did not lead to the loss of generation, transmission lines, or customer load. The number of reported EMS events declined from 88 in 2018, to 74 in 2019, and 58 in 2020. The overall median outage duration remained steady, 60 minutes in 2018 and 2019, and 62.5 minutes in 2020.

- **EOP-004-4 is affecting EMS event reporting.**
  The number of state estimator/real time contingency analysis (SE/RTCA) and inter-control center protocol (ICCP) losses have declined between 2018 and 2020. Comparing to the 2018 data, the number of loss of SE/RTCA significantly declined by 25% in 2019 and 60% in 2020, respectively. There was no loss of ICCP reported in 2020. NERC Reliability Standard EOP-004-4 went into effect on April 1, 2019, in the United States and several Canadian provinces. One major modification to the standard is that the reporting is now clearly required only for complete loss of monitoring or control capability at a BES control center for 30 continuous minutes or more. Partial loss of monitoring or control is no longer considered. It appears entities are now interpreting that partial loss events (such as loss of SE/RTCA, loss of ICCP) no longer require reporting. This change in interpretation will likely reduce the data available for trending through the voluntary ERO EAP and ERO CCAP.

- **Entities minimized the operational degradation from the loss of situational awareness risk due to EMS outage.**
  The number of EMS events reported by Reliability Coordinators (RCs) remained steady from 2018–2020. United States RCs reported only three EMS events in 2019 and two in 2020. TOs/TOPs reported 81% of all EMS events reported during the same period. The median outage duration of the TO/TOP EMS events was 60 minutes in all three years. The number of EMS events reported by Balancing Authorities (BAs) was stable: 4 in 2019 and 3 in 2020. Generation Owners (GOs)/Generation Operators (GOPs) reported two EMS events in 2020. Both GO/GOP events were loss of remote terminal unit (RTU).

- **Loss of SCADA became the most prevalent EMS failure in 2020.**
  Due to a significant decline of loss of SE/RTCA events, loss of SCADA became the most prevalent EMS failure in 2020, encompassing approximately 52% of all 58 EMS events reported in 2020. It was notable that the number of loss of SCADA events increased from 24 in 2019 to 30 in 2020. There were delays in response times due to inadequate plans for an abnormal working environment that included working remotely and having to implement working split shifts at backup control centers. But over the evaluation period from 2018–2020, the loss of SE/RTCA is still the most prevalent EMS failure with 103 events or 47% of all EMS events reported from 2018–2020.

- **The Management/Organization[5] cause coding category was identified as the leading root cause.**
  Management/Organization was identified as the leading root cause in 67 of the total 203 processed EMS events. It suggests a need for the industry to focus on improving the management and organization areas within their companies to reduce the likelihood of EMS events from happening again in the future. There needs to be improved job scoping to involve all potentially impacted groups/departments and strengthen peer review of design/implementation/testing.

[5] A management/organization problem was attributed to management methods (directions, monitoring, assessment, accountability, and corrective action), inadequate resource allocation, work organization and planning, supervisory methods, and change management practices. Neither "Management" nor "Organization" is intended as a job title, solely as a function or process.

Considerations

Based on these key findings, the following considerations are offered to improve the reliability, resilience, and security of the grid:

The ERO Enterprise

- Reinforce, during all applicable/associated reliability interactions, entity development and implementation of communication and response processes between RCs, BAs, and TOPs to improve overlapping coverage of situational awareness
- Reinforce, during all applicable/associated reliability interactions, development and implementation of system recovery and restoration plans to specifically include scenarios in which the EMS and decision-support tools are unavailable (These plans must include drills and training on the procedures plus real-life practice implementing the procedures.)
- Reinforce, during all applicable/associated reliability interactions, that entities keep their on-line model up-to-date and communicate BES changes (including new substations, new facilities, and removed facilities) to neighboring entities in advance

The Entities

- It is essential to develop and practice plans/procedures for an abnormal working environment (for example, working remotely). There needs to be improved job scoping to involve all potentially impacted groups/departments and strengthen peer review of design/implementation/testing.
- It is essential to improve appropriate materials/tools that allow working shifts to monitor and control the BES from backup control centers.
- It is essential to maintain network devices on a planned schedule in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates. It is also essential that utilities build an asset management system to manage the entire life cycle of assets to identify and mitigate risks.
- It is essential to create routines for regularly testing and maintaining the backup generator, uninterruptible power supply (UPS), and associated power switches to verify and ensure that power supply redundancy has been implemented in control rooms, data centers, and substations.
- It is essential to develop dedicated and skilled in-house personnel who can troubleshoot and correct issues and provide in-house staff with real time tools and training to improve/increase knowledge transfer from the vendor.
- It is essential to perform risk assessments to determine any gaps in alarming in order to ensure that all alarms are not only functioning as intended, but that there are additional fail-safes in place to help the operators monitor the system in the most efficient manner.
- Encouraged to participate in the ERO EAP to help prevent event/issue reoccurrence and share lessons learned across industry.

Introduction

Background

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. The primary objective of the EMS is to provide situational awareness to the system operators[6] and enable remote control of devices to ensure secure and stable operation of the BES. Situational awareness includes, but is not limited to, the ability to do the following:

- Monitor frequency within the system operator's area
- Monitor the status (open or closed) of switching devices as well as real and reactive power flows on generators, BES tie-lines, and transmission facilities within the system operator's areas
- Monitor/control voltage and reactive resources
- Monitor the status of applicable EMS applications, such as RTCA and/or alarm management

Situational awareness is necessary to maintain reliability and security by anticipating events and responding appropriately when or before events occur. Without tools and data, system operators may have degraded situational awareness for making decisions that ensure reliability and security for a given condition 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 coordination or oversight can leave system operators with impaired system visibility.

The reference document *Risk and Mitigations for Losing EMS Functions* is published biennially and contains analysis and recommendations based on 521 EMS events reported through the ERO EAP between October 2013 and April 2019. Because the publication/implementation of EOP-004-4 occurred between reference document updates, the NERC EMSWG published *NERC Energy Management System Performance Special Assessment (2018–2019)* as an interim activity by using 2018–2019 EMS events reported through the ERO EAP.

The year 2020 was the first full year that the standard EOP-004-4 was in effect. The ERO Event Analysis Program identified a need to continue the analysis by adding EMS events reported through the ERO EAP in 2020 into the study period for improving resolution on the contribution of EMS outages to the loss of situational awareness and the effect from the EOP-004-4.

Scope and Purpose

This document is one of the continued efforts to explore the impact to partial loss of EMS functions reporting via the ERO EAP and to improve resolution of the contribution of these losses to a loss of situational awareness. Therefore, using EMS events reported through the ERO EAP for 2018–2020, the purpose of this document is to do the follows:

- Evaluate the effect of EOP-004-4 on EMS partial function loss reporting
- Update the EMS performance based on outage duration, EMS functions, and entity reliability functions
- Offer recommendations[7] to improve EMS reliability, security, and resiliency of the BPS

[6] NERC Reliability Guideline *Situational Awareness for the System Operator*: https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/SA_for_System_Operators.pdf

[7] It does not reflect binding norms or mandatory requirements.

Commonly Used Terms within This Document

The terms in **Table I.1** used in this document are not defined within or intended to be included in the NERC Glossary of Terms.[8] These particular definitions are identified to ensure a common industry understanding of how they are applied solely within this document.

Table I.1: Commonly Used Terms

Term	Definition
Supervisory Control and Data Acquisition	A category of software application programs for processing control and gathering data in real-time from remote locations in order to control devices and monitor conditions.
Inter-Control Center Protocol	A protocol that allows for data exchange over wide-area networks (WANs) between a utility control center and other control centers, other utilities, power pools, regional control centers, and non-utility generators. Data exchange information consists of real-time and historical power system monitoring and control data, including: measured values, scheduling data, energy accounting data, and operator messages.
Remote Terminal Unit	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 using messages from the master supervisory system to control connected devices.
Real-time Contingency Analysis	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.
State Estimator	An application used to calculate the current state of the electrical system (the voltage magnitudes and angles at every bus) by using a network model and telemetered measurements. The purpose is to provide a consistent base case of real-time system conditions for use by other network application programs, such as power flow and contingency analysis.
Automatic Generation Control	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 automatic generation control (AGC) software uses real-time data such as frequency, actual generation, tie-line load flows, and plant controller status to determine generation changes.

[8] Glossary of Terms Used in NERC Reliability Standards: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Chapter 1: Approach and Data

The ERO Event Analysis Program [9] was established to facilitate the evaluation of events on the BPS in a systematic manner for reliability improvement purposes. The program provides insight and guidance by identifying and disseminating valuable information to owners, operators, and users of the BPS who enable improved and more reliable system operations. The program includes the ERO EAP[10] and the ERO CCAP.[11] The ERO EAP involves identifying what happened during an event and is used to drive the ERO CCAP, helping to understand "why it happened." The ERO CCAP allows events to have descriptive codes, characteristics, and attributes assigned that can be used to identify and study trends.

Based on the ERO EAP analysis, this document assesses the following factors to evaluate the contribution of EMS outage to loss of situational awareness, risk, and the effect from the EOP-004-4:

- **Outage Duration**
  Outage duration demonstrates the resilience of an EMS to recover the system or function(s). The shorter the outage duration, the stronger the resilience.
- **EMS Functions**
  SCADA is the heart of present EMS architecture. Loss or degradation of SCADA means that system operators would not have an indication of the status of devices or of critical substation data points, nor would they be able to open and close breakers, or switches, via remote operator control. Therefore, the loss of SCADA would likely be the most impactful EMS failure. The impact of the loss of other EMS functions also depends on the roles that these EMS functions play in performing an entity's reliability functions.
- **Entity Reliability Functions**
  Entities use various EMS functions based on their reliability functions. For example, AGC and SCADA are critical for BAs to monitor and control generation output and to calculate area control error. However, a TOP may use SCADA, SE, and RTCA to monitor and control the transmission network to keep the system in a reliable and secure operating condition.

This document also examines trends, event root causes, and contributing causes identified through the ERO CCAP for the 2018–2020 period. The top five contributing causes for the same period will be discussed in detail throughout this document. EMS events analyzed in this document were Category 1h[12] events reported through the ERO EAP from 2018–2020.

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 BES elements
- Loss of communications from SCADA RTUs
- Unavailability of ICCP links, which reduces BES visibility
- Loss of the ability to remotely monitor and control generating units via AGC
- Unacceptable state estimator or real-time contingency analysis solutions

[9] The ERO Event Analysis Program: https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx
[10] The ERO Event Analysis Process: https://www.nerc.com/pa/rrm/ea/ERO_EAP_Documents%20DL/ERO_EAP_v4.0_final.pdf
[11] The ERO Cause Code Assignment Process: https://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/CCAP_2020_02.pdf
[12] For the latest category definition: https://www.nerc.com/pa/rrm/ea/ERO_EAP_Documents%20DL/ERO_EAP_v4.0_final.pdf

Chapter 2: Analysis and Assessment

This section provides details regarding analysis results based on 220 EMS events reported from 2018–2020.

Overview Analysis

There were a total of 220 EMS events reported during the 2018–2020 time horizon through the ERO EAP. **Figure 2.1** shows the number of EMS events reported per year. United States entities reported 198 EMS events in these three years, encompassing approximately 90% of all EMS events reported. The number of entire EMS events reported continued to decline from 88 in 2018, to 74 in 2019, and 58 in 2020.

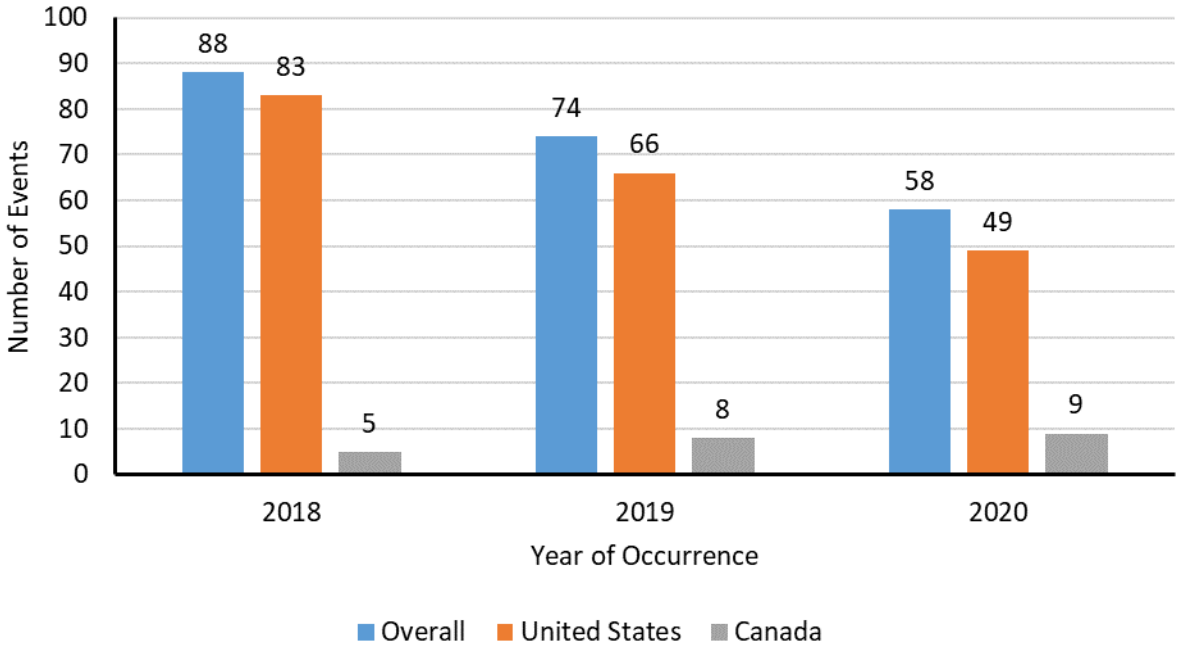


Figure 2.1: Number of Reported EMS Events (2018–2020)

These EMS events include the loss of SCADA, ICCP, RTU, AGC, SE, or RTCA for 30 or more continuous minutes. Over these three years, the loss of SE/RTCA was the most prevalent EMS failure totaling 47% or 103 events (see **Figure 2.2**). The loss of SCADA was the second leading failure in 35% or 77 events (see **Figure 2.2**) during the same period.

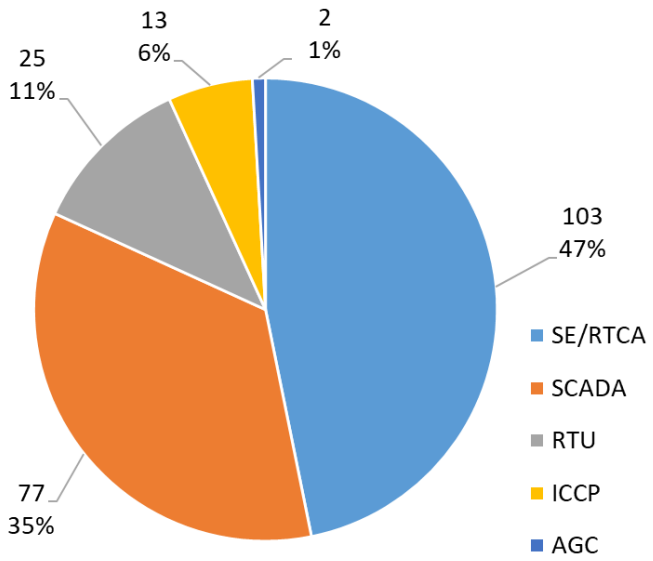


Figure 2.2: Percentage of Loss of EMS Functions (2018–2020)

Figure 2.3 shows a comparison of the reported EMS events by loss of EMS functions from 2018–2020. The number of loss of SE/RTCA and loss of ICCP events continued to decline in 2020. Only two loss of AGC events were reported during these three years. It is notable that loss of SCADA becomes the most prevalent event failure in 2020.

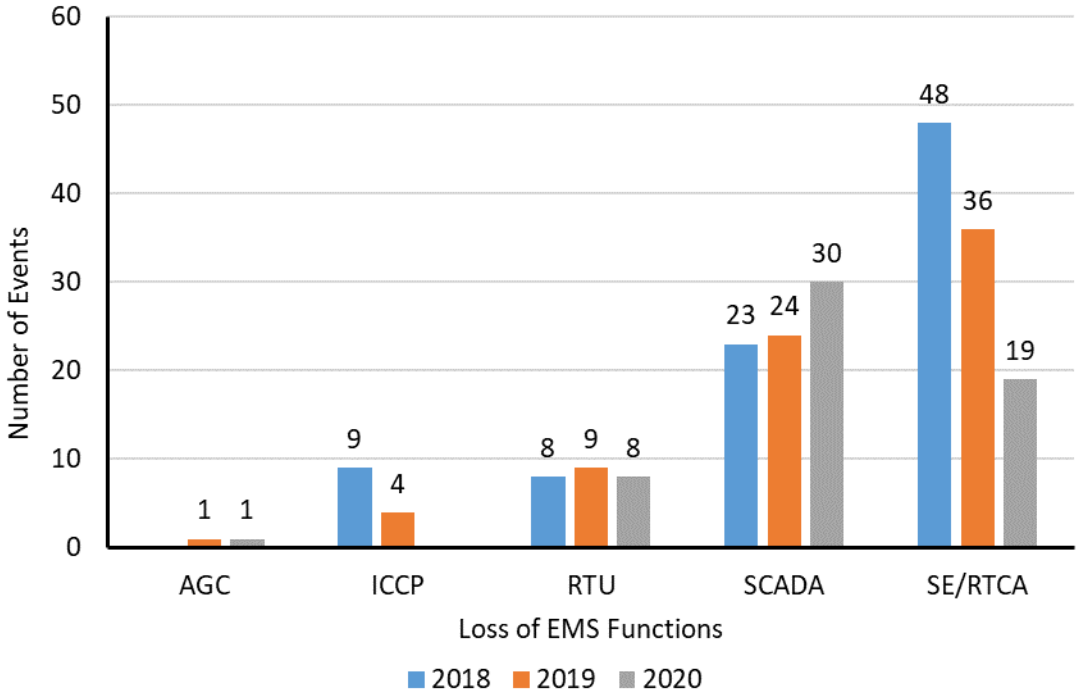


Figure 2.3: Number of Reported EMS Events by Loss of EMS Functions (2018–2020)

Outage duration indicates the resilience of an EMS to recover the system or function(s). Figure 2.4 shows the median outage durations for all EMS events reported and all individual types of EMS functions. The median outage duration for all analyzed EMS events was stable from 2018–2020 with 60 minutes in 2018 and 2019 and 62.5 minutes in 2020. Although the median outage durations for the 2020 EMS events increased, no discernable trend is identifiable.

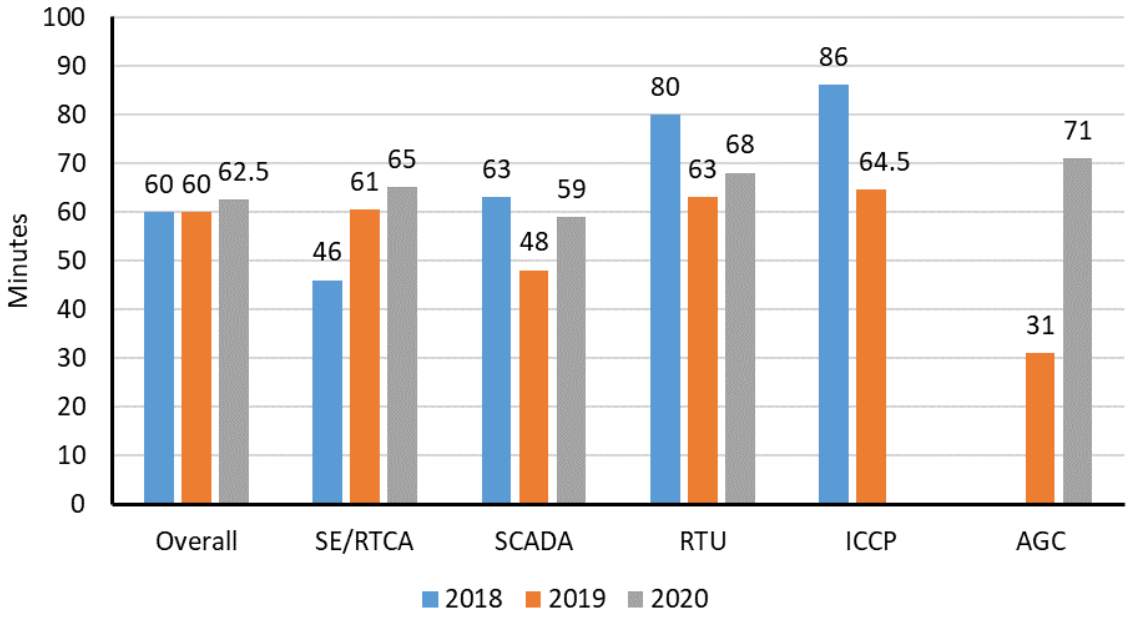


Figure 2.4: Median Outage Duration by Loss of EMS Functions (2018–2020)

Analysis of Entity Reliability Functions

Entities use various EMS capabilities to perform their reliability functions. According to the NERC compliance registry active entities list, as of June 22, 2021, there are 15 RCs, 341 TOs/TOPs, 104 BAs, and 1,162 GOs/GOPs for unique entities and reliability functions.[13] Table 2.1 shows the number of entity reliability functions[14] that reported EMS events and participated in the ERO EAP in 2018, 2019, and 2020.

Table 2.1: Entity Reliability Functions with Reported EMS Events (2018–2020)

	2018		2019		2020	
	Count	**Percentage**	**Count**	**Percentage**	**Count**	**Percentage**
RCs	8	**50%** (8/16)	3	**18.8%** (3/16)	4	**26.7%** (4/15)
TOs/TOPs	40	**11.7%** (40/341)	37	**10.9 %** (37/341)	33	**9.9%** (33/341)
BAs			3	**2.9%** (3/104)	3	**2.9%** (3/104)
GOs/GOPs					2	**0.02%** (2/1162)
Total	**48**		**43**		**42**	

Table 2.2 shows the number of loss of EMS functions reported by entity reliability functions. Notably, TOs/TOPs reported 81% of all EMS events reported in these three years. Of the 178 EMS events reported by TOs/TOPs, a large portion of EMS events (44%) included the loss of SE/RTCA.

[13] Each entity and reliability function is counted once regardless of how many regional CEA jurisdictions it may span.
[14] Based on the NERC compliance registry active entities list as of June 22, 2021

Table 2.2: Number of Loss of EMS Functions Reported by Entity Reliability Functions						
	AGC	ICCP	RTU	SCADA	SE/RTCA	Total
RCs		5		3	25	**33**
TOs/TOPs		8	22	70	78	**178**
BAs	2		1	4		**7**
GOs/GOPs			2			**2**

Reliability Coordinators

RCs are the highest level of authority responsible for the reliable operation of the BES and have a wide area view of the BES and have the operating tools, processes, procedures, and authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. Therefore, RCs will use all EMS capabilities to perform their reliability functions.

There were 33 EMS events reported by RCs over these three years. The number of EMS events reported by RCs was relatively stable, 12 events in 2018, 10 in 2019, and 11 in 2020 (see **Figure 2.5**). The number of EMS events reported by United States RCs continued to decline from 8 in 2018 to 3 in 2019 and 2 in 2020, while the number of EMS events reported by Canadian RCs increased from 4 in 2018 to 7 in 2019 and 9 in 2020. It was noted that a few Canadian entities continue to report the partial loss events because the standard EOP-004-4 is not effective in several Canadian provinces.[15]

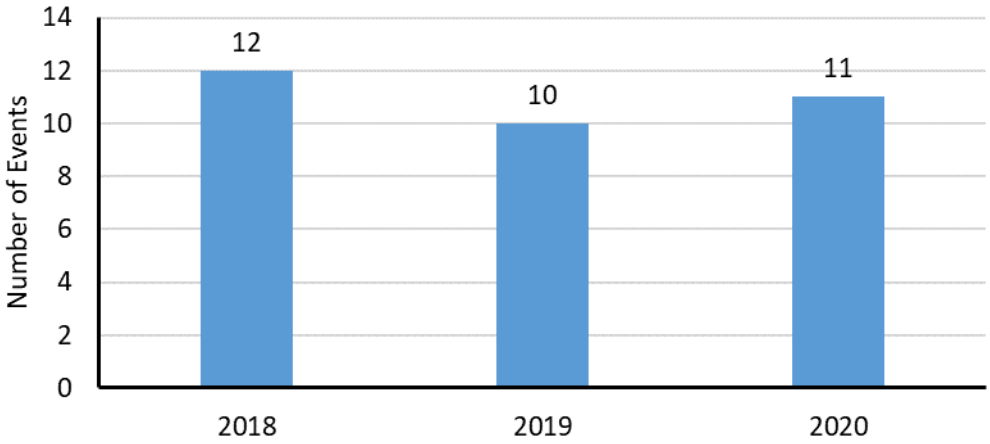


Figure 2.5: Number of EMS Events Reported by RCs (2018–2020)

Figure 2.6 shows the number of Canadian RC EMS events by loss of EMS functions from 2018–2020. The amount of loss of SE/RTCA events increased from 3 in 2018 to 7 in 2019 and 8 in 2020. The median number for Canadian RC events analyzed increased from 61 minutes in 2018 to 90 minutes in 2019 but decreased to 44 minutes in 2020. It was observed that several EMS events reported by Canadian RCs in 2019 and 2020 were due to two factors: modeling issues that led to a more prolonged troubleshooting and improper alarm configurations that caused a longer delay until system operators became aware of the issue.

[15] https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

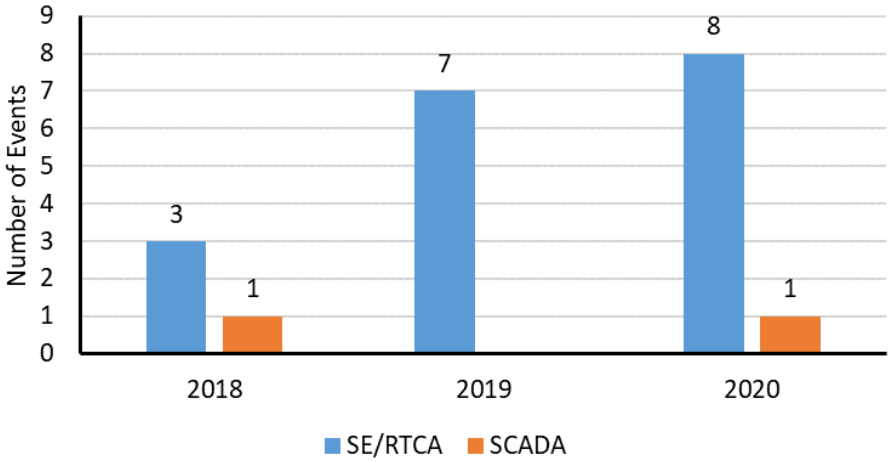


Figure 2.6: Canadian RC EMS Events by Loss of EMS Functions (2018–2020)

Figure 2.7 shows the number of United States RC EMS events by loss of EMS functions from 2018–2020. The number of both the loss of SE/RTCA and loss of ICCP decreased. The median outage duration of United States RC EMS events analyzed slightly declined from 55 minutes in 2018 to 48 minutes in 2019 but increased to 77 minutes in 2020. There was one loss of SCADA outage reported in 2020 that was due to a network hardware failure.

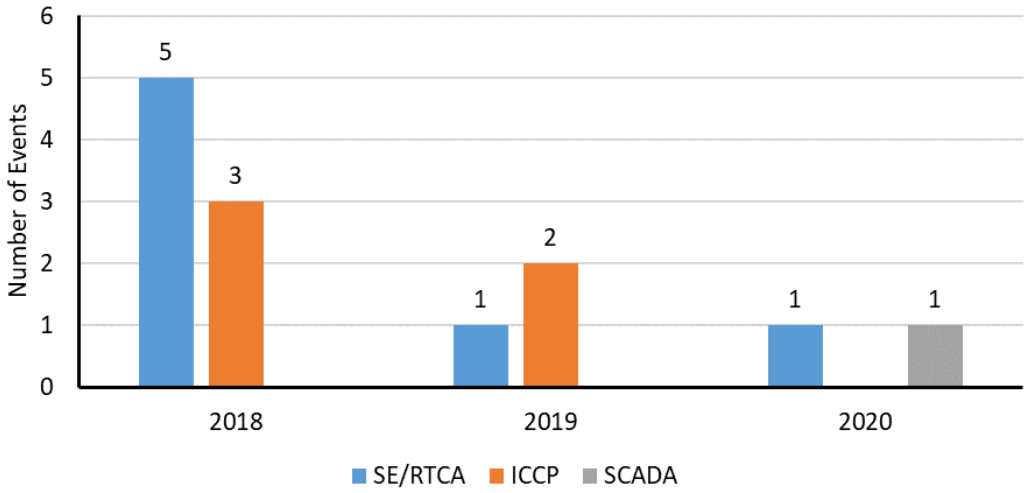


Figure 2.7: United States RC EMS Events by Loss of EMS Functions (2018–2020)

Based on the analysis of the EMS events reported by RCs, the following recommendations are made to reduce the loss of situational awareness risks due to EMS outage:

- **Maintaining models up to date**
  The models of the electrical grid are critical for EMS functions. Models should be periodically maintained but promptly updated after BES changes have been completed in the field, such as when new transmission or generation device(s) are put into service or when devices are retired; otherwise, EMS functions cannot present proper real-time changes (e.g., topology, MW output) related to these devices and sequentially yield unsolved or incorrect solutions.
- **Looking beyond geographic diversity alone for data communications redundancy**
  When contracting with multiple vendors for redundancy in data communications services, one should never assume that geographic diversity alone provides redundancy. This is because there is a point of convergence

that may exist at a common hub that becomes a single point of failure. Therefore, to ensure redundant physical circuit separation and independence of supporting equipment and power, it is recommended that the duration of the service is specified in the contract. Also, to validate independence, it is recommended that testing is performed that simulates this failure to ensure that the redundancy in place covers this scenario. More details on this topic can be found in the lessons learned titled *Telecom Provider Failure Induced Loss of ICCP from Regional Neighbors.*[16]

Transmission Owners and Transmission Operators

TOs are the entities that own and maintain transmission facilities. TOPs are the entities responsible for the reliability of "local" transmission systems and that operate or direct the operations of transmission facilities.

There were 178 EMS events reported by TOs/TOPs from 2018–2020. Over these two years, the loss of SE/RTCA was the most prevalent EMS failure in 44% or 78 events of all reported EMS events by TOs/TOPs (see **Figure 2.8**).

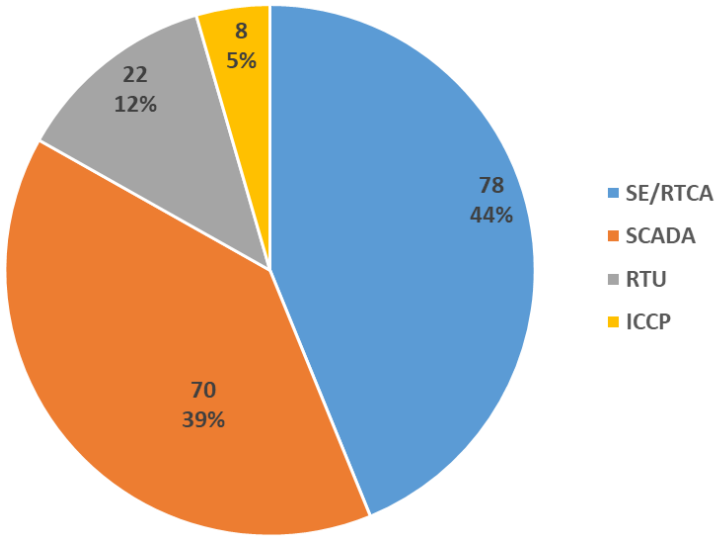


Figure 2.8: Percentage of Loss of EMS Functions Reported by TOs/TOPs (2018–2020)

Figure 2.9 shows a detailed breakdown by the loss of EMS functions reported by TOs/TOPs. The loss of SE/RTCA events continued to significantly decline from 40 in 2018, to 28 in 2019, and 10 in 2020, similar to the loss of ICCP events. Of particular note, the loss of SCADA events increased from 21 in 2019 to 27 in 2020.

[16] Lessons learned *Telecom Provider Failure Induced Loss of ICCP from Regional Neighbors*: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190503_Loss_of_ICCP_from_Regional_Neighbors.pdf

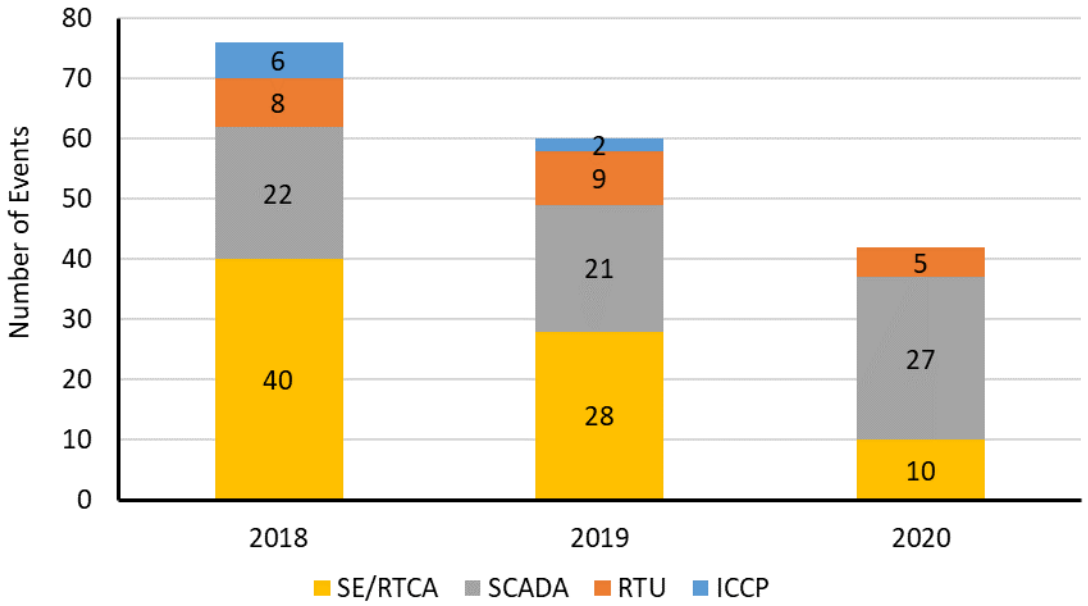


Figure 2.9: Breakdown of Loss of EMS Functions Reported by TOs/TOPs (2018–2020)

There are two reasons for the declining direction of loss of SE/RTCA and loss of ICCP:

- Partial loss events are no longer required as part of EOP-004-4 reporting. NERC standard EOP-004-4 was modified to only require the complete loss of monitoring or control capability at a BES control center for 30 continuous minutes or more. The modified NERC Reliability Standard went into effect on April 1, 2019, in the United States and several Canadian provinces. However, some entities still report partial EMS loss.
- The industry has made significant efforts to enhance EMS reliability and resilience. For example, many entities implemented a 24x7 onsite team that works along with system operators and provides dedicated support to SE and RTCA. This action has significantly reduced the outage duration, resulting in many SE/RTCA issues not being reportable.

Figure 2.10 shows the median outage durations for all TO/TOP EMS events and all individual types of EMS functions. The median outage duration for all TO/TOP EMS events was stable, 60 minutes in all three years. The median outage duration for the loss of SCADA reported by TO/TOPs decreased from 71.5 minutes in 2018 to 46 minutes in 2019 but increased to 58 minutes in 2020. The median outage duration for the loss of SE/RTCA increased from 46 minutes in 2018, to 56.5 minutes in 2019, and to 73 minutes in 2020.

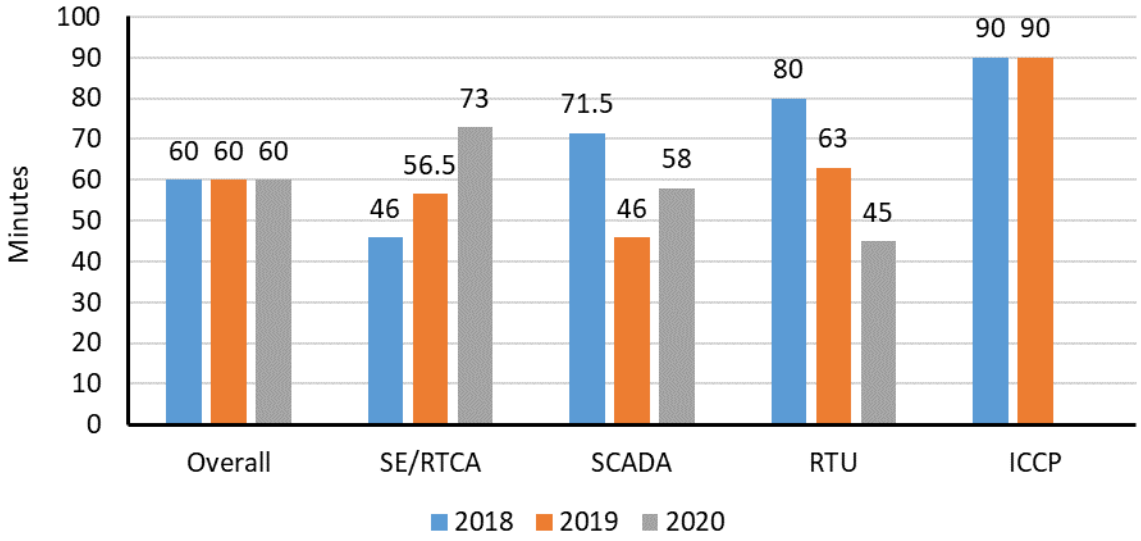


Figure 2.10: Median Outage Duration by Loss of EMS Functions—TOs/TOPs (2018–2020)

The following observations and recommendations were made during analysis of the EMS events reported by TOs/TOPs:

- **External Modeling**
  Many entities have expanded their EMS models to monitor the impact of events and outages outside of their footprint. This has increased potential exposure to bad data points, inaccurate topology modeling, and communication issues that may cause EMS events. Entities should communicate BES changes (including new substations, new facilities, and removed facilities) to neighboring entities in advance. This will enable neighboring entities to update their external EMS models in a timely manner and ensure that the data received through ICCP links is accurately matched to the appropriate data points in the model.[17]

- **Network Communications Configuration**
  EMS-related communications networks are moving from point-to-point serial communication infrastructures to packet-based networks. The main advantage of a packet-based network is to transmit data from one node to another node while avoiding a communications system failure caused by the breakdown of a single (or few) intermediate link(s). Consequently, the correct configuration is critical to ensure the communications network functions as designed. Reporting included four complete loss events due to networking packet broadcast storms caused by improper network configurations. This led to the following recommendations:

  - Establish standardized settings for network devices
  - Complete physical separation between SCADA operations networks and business networks, voice over internet protocol (VoIP), and external facing networks is preferred over virtual local area network (VLAN) to avoid network traffic congestion and security issues[18]

- **Alarming**
  Alarming has not initiated any EMS events. However, an improper configuration can degrade the system operator's situational awareness. A risk assessment should be performed to determine any gaps in alarming.

[17] Lessons learned *External Model Data Causing State Estimator to Not Converge*: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20180602_External_Model_Data_Causing_State_Estimator_to_Not_Converge.pdf

[18] Lessons learned *Networking Packet Broadcast Storms*: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20181001_Networking_Packet_Broadcast_Storms.pdf

Alarming regarding quantity, visualization, and even sound effects widely vary. It is essential for the entity to not only determine what alarms are needed but also to assess what can cause them to fail or otherwise go unnoticed.[19]

- **Power Supply**
  Stable and secure power supplies are critical to control rooms, data centers, and substations. Sixteen EMS events were due to loss of power supply. Although the redundant power supply was installed at the control rooms, data centers, and substations, it is essential that routines be established for monthly testing and maintenance of the backup generator, UPS, and associated power switches. More recommendations can be found in the lessons learned titled *Loss of Monitoring or Control Capability due to Power Supply Failure*[20] and *Loss of SCADA Operating and Monitoring Ability*.[21]

- **Dealing with Abnormal Working Environment**
  In 2020, entities implemented work-from-home policies for non-essential employee. Lots of tasks (like maintenance, software/database deployment, etc.) that normally were conducted onsite had to be executed in a remote fashion. Job scoping needs improvement to involve all potentially impacted groups and departments and strengthen peer review of design, implementation, and testing.

  Many entities also implemented working split shifts both at the primary control center and backup control center in order to practice social distancing. It is recommended to improve appropriate materials/tools, which allow working shifts to monitor and control the BES from backup control centers.

Balancing Authorities

BAs are the responsible entities that integrate resource plans ahead of time, maintain load-interchange-generation balance within a BA area, and support Interconnection frequency in real time. Consequently, AGC and SCADA are two essential EMS components for BAs to support their functions.

There were seven EMS events reported by BAs from 2018–2020 (see **Figure 2.11**). There were two loss of AGC events reported in 2019 and 2020. Both loss of AGC events were caused by software bugs introduced during regular AGC software updates. NERC recognizes AGC as a critical function for a BA and has published a lesson learned titled *Loss of Automatic Generation Control during Routine Update* [22] to emphasize that a completed software testing process is critical to guarantee that products meet intended requirements.

[19] Lessons learned *Enhanced Alarming Can Help Detect State Estimator and Real-Time Contingency Analysis Issues*: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190502_Enhanced_Alarming_helps_detect_SE_RTCA_issues.pdf

[20] Lessons learned *Loss of Monitoring or Control Capability due to Power Supply Failure*: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190801_Loss_of_Monitoring_Control_due_to_Power_Supply_Failure.pdf

[21] Lessons learned *Loss of SCADA Operating and Monitoring Ability:* https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20170503_Loss_of_SCADA_Operating_and_Monitoring_Ability.pdf

[22] Lessons learned *Loss of Automatic Generation Control During Routine Update*: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20200403_Loss_of_AGC_During_Routine_Update.pdf

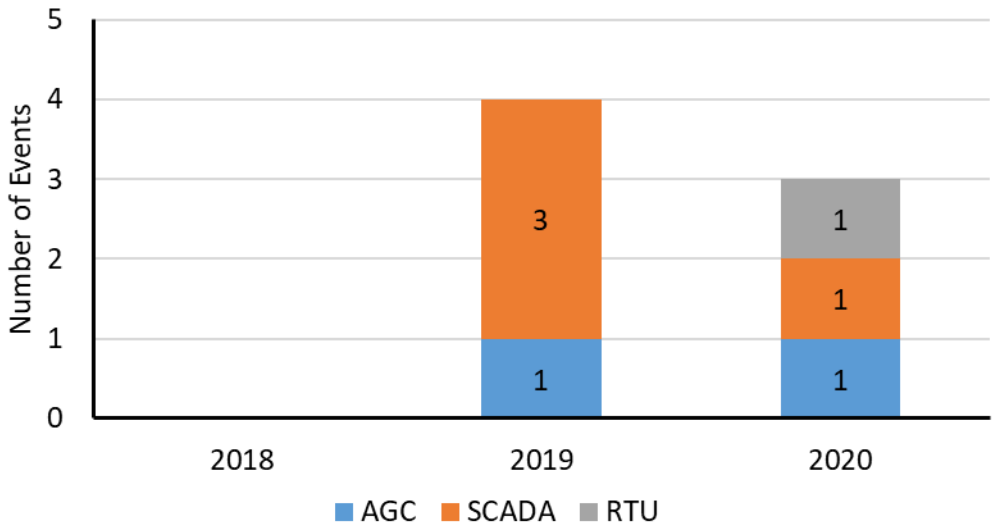


Figure 2.11: Number of EMS Events by Loss of EMS Functions—BAs (2018–2020)

All three loss of SCADA events reported in 2019 were related to firewall issues. Two events were caused by firewall hardware failure, and another one was due to an improper firewall configuration. To prevent recurrence of the events, entities should maintain network devices on a scheduled basis in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates.

The loss of SCADA event reported in 2020 was due to a hardware damage caused by a lighting strike. The loss of RTU event in 2020 was caused by the exhaustion of UPS.

Generation Owners/Generation Operators

GOs own and maintain generating facilities. GOPs operate generating facilities and perform the functions of supplying energy and Interconnected Operations Services.

There were two EMS events reported by GOs/GOPs in 2020. Both were loss of RTU events caused by network device failures. It was essential to maintain network devices on a scheduled basis in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates.

Analysis of Root Causes and Contributing Causes

This section will discuss the event root causes and contributing causes identified through the ERO CCAP for the years 2018 and 2020. Of the 220 EMS events reported from 2018–2020, 203 EMS events were processed through the ERO CCAP because the processing of 2020 EMS events is ongoing.

Event Root Causes

A root cause is the fundamental reason for the occurrence of a problem or event. Analysts identify the root cause of an event in order to prevent it from happening again in the future; if it were not for the root cause, an event would not take place. It is important to determine roots causes so that corrective actions can be implemented to avoid a repeat of the event.

Of the 203 EMS events processed, 68 events did not yield a root cause, resulting in dependence on the contributing causes for insights into the associated events. The top three common reasons for the less-than-optimal root cause yield include the following:

- **Vendor Cited as Involved in Event**
  Some EMS events were due to defects in software, firmware, or hardware provided by vendors. This is beyond the entity's control/direction. The entity does not know why it is wrong, but a patch, fix, or upgrade provided by the vendor resolves the issue. To prevent this type of event, entities may consider the following:
  - Maintaining network devices on a planned schedule in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates
  - Periodically reviewing system parameters and settings with the vendor's help (There are different flags and weighting levels that may need to be adjusted as models are expanded or system conditions change.)
  - Continuing to develop dedicated in-house expertise and/or acquire third party services onsite (More skilled in-house personnel who can troubleshoot and correct these issues can lead to shorter EMS outage durations, including additional knowledge transfer from the vendor to the in-house staff.)
- **Report Stops at Failure or Error Mode**
  For some EMS events, the entity knows what happened but does not understand why it happened due to a lack of information. For example, consider that a SE failed to converge for more than 30 minutes due to bad data from a select RTU. After testing and inspection of the RTU, no defects were found. Because the root cause was not identified, the same problem could occur in the future. The entity should install enhanced detective controls to discover the issue and recover quickly.
- **Other NERC-Registered Entity Cited as Involved in Event**
  This type of event usually is data related. For example, a neighboring entity sends data that indicates a unit generates 3,000 MVar reactive power, which is unreasonable for the type of unit. This data causes the entity's SE failure. To prevent this type of event, entities may consider the following:
  - Entities should implement or enhance a tool or feature that prevents, detects, and corrects the data error before it is used in EMS functions, especially in SE. As an example of the unreasonable 3,000 MVar reactive power, a bad data detector would be implemented in the SE module. Firstly, the detector identifies the bad data based on the predefined unit MVar limit and labels it for the system operator's awareness. Secondly, the detector excludes the bad data from the SE computation. Finally, it replaces the bad data with the last-good value, a unit MVar limit, or a value calculated from good surrounding measurements.
  - Entities should communicate with the RC and neighboring entities about the data error to understand why the data error was sent and how they resolved it.

Management/Organization was identified as the leading root cause in 49% (see **Figure 2.12**) of the 135 identified root cause events. Some topics considered in Management/Organization causes are management/supervisory methods, resource management, work organization and planning, and change management efforts. Some examples of these causes are as follows:

- Management/Organization had the correct identification of a cause for a previous event but failed to implement a good corrective action plan prior to another similar event occurring.
- Management/Organization did not identify a special circumstance that needed to be addressed during work, and failed to recognize that a second system might be impacted by work currently being performed. For example, an entity updated its external model based on the Common Information Model from its RC. However, the project scope failed to identify a special circumstance that the Common Information Model was exported from the RC's market system. Many parameters related to the voltage control were neither correct nor up-to-date in the market system. As a result, the entity's SE failed to converge at the external area due to low voltage.

- Management/Organization did not include all potential affected departments or work groups in task. For example, an entity scheduled maintenance to update network infrastructure. The network team coordinated on a bridge call and connected from home to company systems via VPN. SCADA system visibility/connectivity was interrupted due to a corrupted address resolution protocol table during the maintenance. However, the team did not realize the issue because they lost their remote connection due to a brief service interruption. This resulted in delays in restoration. The incident could have been prevented if real-time operation personnel were invited on the bridge call and would notice the team immediately when the SCADA system visibility/connectivity issue first arose.

Design/Engineering was the second leading cause in 27% (see **Figure 2.12**) of the 135 identified root cause events. Cause considerations include design input, design output, documentation, installation, verification, and operability of design and/or environment issues. Some examples of these causes are a shortfall in the scoping of the design failing to realize that an alarm system was not configured to account for stale SCADA data or obsolete SE/RTCA solutions.

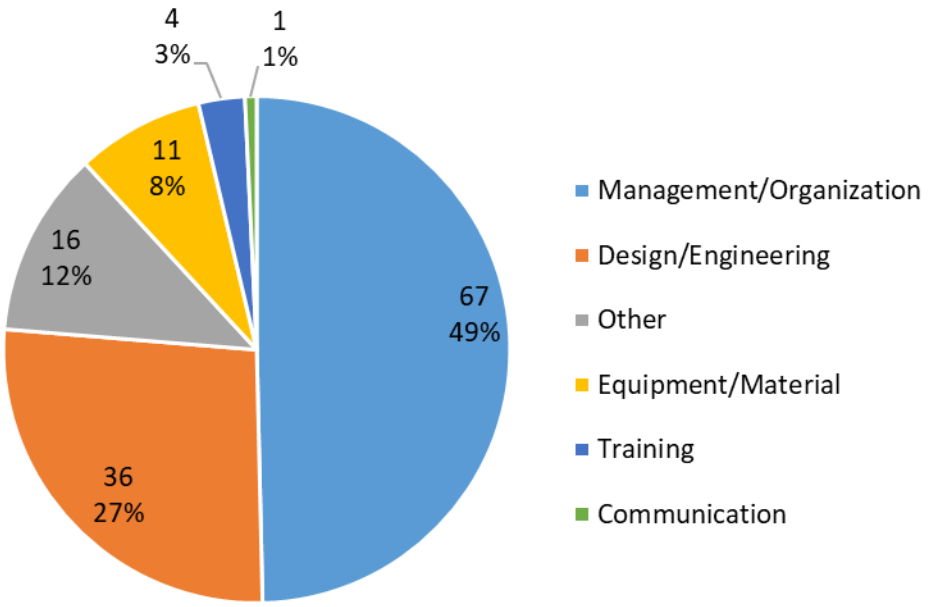


Figure 2.12: 2018–2020 Identified EMS Event Root Causes (Processed to date)

Contributing Causes

A contributing cause is not a single factor that drives an event. Tracking and trending of contributing causes may identify the need to take action. **Figure 2.13** shows a trend of identified contributing causes for all processed EMS events from 2018–2020.

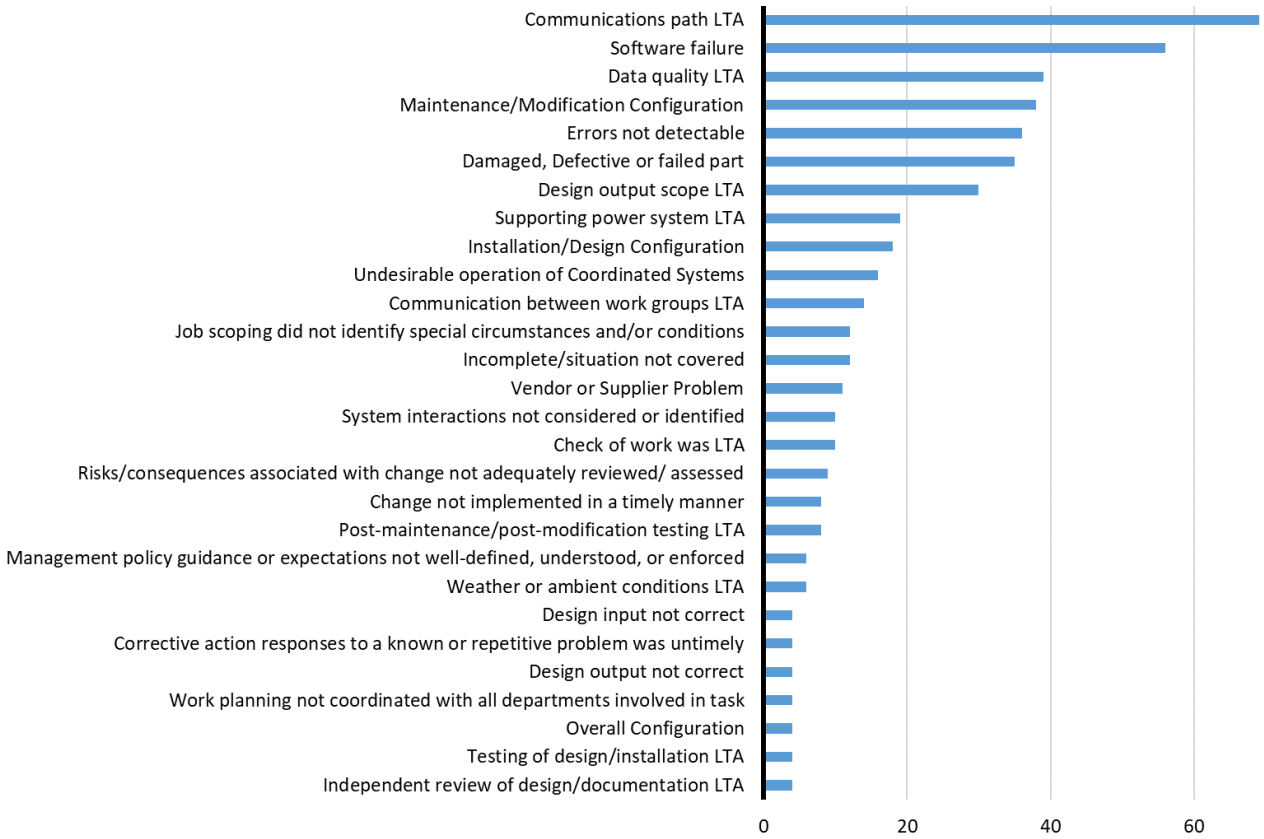


Figure 2.13: Identified Contributing Causes for EMS Events (2018–2020)

The top five detailed contributing causes are listed below:

- **Communications Path Less than Adequate[23]**
  "Communications path less than adequate" was identified as the leading contributing cause (a total of 69 times). This cause indicates that data exchange was degraded between substations and control rooms or between the entity and its RC/neighboring entities. Internal network configuration error and hardware failure at the telecom company are two major contributors to this cause. An example is a spanning-tree protocol implementation in a network switch, causing a loop that generated an exceptionally high volume of traffic. The result was to shut down the communication network supporting the EMS. Another example is that the entity lost RTU data from major substations as the telecom company's staff cut the fiber between the substations and the data center. Entities should maintain network devices on a schedule in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates. Entities must also consider redesigning communications systems such that the most critical BES substations communicate simultaneously over entirely separate physical paths (and possibly separate vendors) to both control centers, eliminating the need for telecom company communication structure.

- **Software Failure**
  This was the second-leading contributing cause of failures resulting in EMS events, occurring 56 times as a contributing cause. A bug either in a vendor application or in an in-house implementation caused the software failure. A completed software testing process is always recommended to guarantee that the software meets its requirements. Systems and software assurance requires a process model for formal

[23] For the purposes of the CCAP, the phrase "Less than Adequate," or "LTA," does not imply any negligence or fault for the entity; it is solely intended to say that the situation to which the LTA is assigned was not sufficient to prevent the undesired situation from occurring.

testing based upon the software development framework that the software was created within. The scope of the test should provide an assurance case for operation of the software under test for both known and unknown operating conditions, with the inclusion of a data integrity check of the module. In general, the process is considered to have four components:

- **Test Scope**: Define the test environment requirements and setup, features/functions that need to be tested, documentation to refer and produce as output, approval workflows, etc.
- **Test Design**: Design the test cases that are necessary to validate the system/functions/features being built compared to its design requirements. Typically, regression testing and incremental testing are necessary
- **Test Execution**: Execute tests in many different ways
- **Test Closure**: Consider the exit criteria for signaling completion of the test cycle and readiness for release

- **Data Quality LTA**
  This was identified as a contributing cause 39 times. Bad data from the external area was a major contributor to this cause. The entity was encouraged to implement or enhance a tool or feature that can prevent, detect, and correct the data error before the data error is used in EMS functions, especially in SE. Communications between the entity and its RC/neighboring entities are critical to detect, block, and correct these less-quality data.

- **Maintenance/Modification Configuration**
  This was identified as a contributing cause 38 times. Besides the network configuration error mentioned in above sections, the error in settings/parameters for SE/RTCA are a major concern. These SE/RTCA settings and parameters are often uniquely programmed for the entity to meet the individual needs based upon the entity's configuration, topology, contingencies, and external model. When the entity expanded or modified its model, the settings/parameters needed to be tuned or calibrated based upon subsequent topology changes. Periodic reviews of SE/RTCA settings and parameters with the vendor's help may be necessary to ensure that the SE/RTCA continues to converge and produce a quality solution. The frequency of these reviews will vary, but consideration to reviewing the settings and parameters following model changes, generation retirements, software upgrades, and any other significant changes made to the EMS system or the model is necessary.

- **Error not Detectable**
  This was identified as a contributing cause 36 times. Lack of alarming is a major contributor to this cause. Maintaining situational awareness of the bulk power system is a critical task for an operator. While the technology does a great job of alerting the operators, not knowing that the system has been compromised introduces risk as the operator makes decisions based on stale data or a contingency analysis that has not been updated. Ensure that all alarms are not only functioning as intended but that there are additional fail-safes in-place to help operators monitor the system.