North American Transmission Forum

NATF Resilient Data and Voice Communications for System Operations

Version 1.0
Document ID: 1796
Approval Date: 09/24/2025

Version History

Date	Version	Notes
09/24/2025	1.0	Initial version

Review and Update Requirements

Review: every 5 years
Update: as necessary

Contents

1. Introduction

Data and voice communications are essential for maintaining the reliability of the bulk electric system. They enable real-time coordination, allowing system operators to exchange critical information about grid conditions, outages, and system stability. Effective data and voice exchange fosters collaboration and enhances situational awareness. Prompt and clear communications ensure proper decision-making during normal operations and emergencies, reducing the risk of cascading failures.

This document describes the practices that allow system operators to develop procedures to maintain data and voice communications when primary communication tools and methods are severely degraded or unavailable. The *NATF Supplemental Operating Strategies and Resiliency Practices* [1] document provides greater detail to assist NATF member utilities in preparing for extended events that affect control center functions. The subsequent sections are excerpts from that document that discuss how to incorporate resilience into data and voice communications.

2. Developing a Resilient Communications Structure

System operators use communications infrastructure to convey information in both normal and emergency conditions. Communications paths to internal and external entities, such as neighboring transmission entities and reliability entities, should be established and maintained. Methods to contact local, state, and federal agencies are also necessary during emergencies.

A variety of communication capabilities should be available and equipment diversity should be emphasized. Communication channels should be quickly verified at the start of an event and alternative forms of communication should be deployed and used as necessary.

Developing a PACE Plan for Communications Methods

It is essential to maintain communications internally and with external entities, even when normal communication channels are severely degraded, compromised, or completely unavailable. Communication plans should be developed that identify the primary, alternate, contingency, and emergency methods of communications used in the PACE plan method [2].

Developing a PACE plan involves identifying available communications methods, the redundancy of the tools used for communications, and the expected response to a communications failure. An example PACE plan is shown in “Appendix 1: PACE Plan Example.”

Elements to include in a PACE plan

2.1 Document the primary communications methods. Primary methods are the preferred and most reliable methods, such as cable or fiber internet networks, that can transmit both data and voice.

Internet-based communications can be owned by the utility as a private network and connected to neighboring utilities to strengthen communications.

2.2 Identify and document alternate communications methods. These are common methods, such as cellular networks, that while not as robust as the primary method, can transmit data and voice communications that can be secured through encryption.

Public cellular networks require power sources and can be limited in the number of users. It is possible to use private networks to improve reliability.

2.3 Identify and document contingency communications methods. These methods are typically not as fast, convenient, or reliable as primary or alternate methods. Contingency communications methods include satellite telephone networks, low earth orbit satellite internet, microwave, Government Emergency Telecommunications Service (GETS)[3], and Wireless Priority Service (WPS).

Satellites can provide data (using low earth orbit satellites) and voice communications but require line-of-sight to the sky and can be affected by weather. Microwave can transmit data and voice communications and can be deployed relatively quickly but also requires a line-of-sight.

2.4 Establish emergency communications methods, such as high frequency (HF), very high frequency (VHF), or ultra-high frequency (UHF) radio, or manually relaying messages. It may be necessary to coordinate with external entities and establish relationships with public sector entities, such as ham (amateur) radio operators, to provide communication in extreme emergency situations.

HF radio can transmit data and voice over long distances but has limited bandwidth and can be affected by weather. UHF and VHF require line-of-sight to transmit signals and can be affected by obstacles such as walls and buildings. Emergency communication methods may not be secure and have the potential for others to eavesdrop on communications. These methods should only be used when all other methods of communications are unavailable and in conjunction with additional security protocols, such as code words as discussed later in “Using Code Words for Communications.”

2.5 Develop a process to test and exercise alternate, contingency, and emergency communication methods regularly to identify and address any issues prior to an event.

2.6 Develop a process to periodically evaluate new communication tools that can be implemented as technology evolves.

3. Operating with Limited or No Communications

Following the recognition of degradation or loss of communication, a continuous and concerted effort is needed to maintain system reliability. Plan for communications of enough data and information from personnel at essential substations to personnel in the control center and between control centers to maintain situational awareness and perform Real-time assessments. This will likely look much different than the assessments completed during day-to-day operations.

Create a staffing plan to provide support for system operators and field operations. Additional staff may be necessary, especially if degraded communications persist for a long time. For example, manual calculation of the system limits necessary for the continued reliable operation of the electric system, through load flow analysis, can be a labor-intensive process.

Alternate Data Communications Method for System Data

In an emergency, it is important to have established alternative methods for entities to send and receive data of the type that, under normal operating conditions, is exchanged via ICCP. Examples of emergency conditions include extended unplanned ICCP link outages, extended planned network outages, and cyber-attacks. The

following practices describe an alternate method for a sender, such as a Transmission Operator (TOP), and a receiver, such as a Reliability Coordinator (RC), to exchange this type of data.

3.1 Create an alternate data exchange system that can transfer limited data upon loss of ICCP. Appendix 2 shows an example of an alternate data exchange system. Appendix 3 shows an automated alternate data exchange workflow.

3.2 Document the alternate system and provide a procedure to all entities that will exchange data.

3.3 Specify the conditions under which the communication method will be used, notification requirements, and when to return to the normal data source. For example, if an unplanned ICCP link outage occurs, after 30 minutes the RC calls the TOP to initiate the alternate communications method.

3.4 Establish a pre-defined, simple file format (e.g., CSV file) to transmit the required data points.

3.5 Define the file naming convention and the information to be transmitted, including:

- ICCP Object ID
- Value
- Quality (ensure all applicable quality attributes are included)
- Timestamp
- Measurement description or identifier

Use UTC time to avoid confusion when data is exchanged between entities in different time zones.

3.6 Write a data pull script to create a snapshot of the relevant data points to be sent via the alternate data exchange method.

3.7 Use a secure file transfer protocol (SFTP) application when sending data via the alternate communications method.

This may require entities to establish an account if the SFTP application uses the infrastructure of an external service provider.

3.8 Use an encrypted transport path for the SFTP exchange with public/private encryption keys. Rotate encryption keys periodically (e.g., every 90 days).

3.9 Establish SFTP network segmentation that consists of the following:

- The SFTP server resides in a separate security zone from the EMS server
- The server is on a separate firewall from the EMS server firewall
- Only the required ports are opened from the source to the destination

3.10 Ensure the SFTP host has installed and updated anti-malware solutions whenever possible and that all files are scanned at the source and destination.

3.11 Define a low periodicity requirement (e.g., every five minutes) for the sender to upload the data file into the SFTP application.

3.12 Upload the received file of data points into the EMS every 5-30 minutes.

3.13 Establish a method to verify received data against the ICCP database and last-known-good value from the normal ICCP connection before being propagated to the EMS.

3.14 Collect and analyze logs, whenever possible, from the applications/servers deployed in the environment.

3.15 Generate a log message and conduct troubleshooting between sender and receiver if incoming data inconsistencies or errors are identified.

3.16 Monitor the data processing to ensure the data is properly delivered to the ICCP database. For example, verify the file is formatted and named correctly and that the timestamp is recent (within 30 minutes).

3.17 Continuously capture communications data so that the alternate ICCP communications method can be activated quickly in an emergent condition.

> A process can be created to periodically delete stored files to not use excessive storage space.

3.18 Establish a procedure to ensure that when changes are made to the primary data measurements or IDs, the alternate data measurements or IDs are updated accordingly.

> An entity's changes may occur automatically/dynamically and performing manual data checks may not be necessary.

3.19 Periodically train and test personnel on enabling the alternate ICCP communications method and validating the data. For example, conduct annual refresher training and test personnel during normal maintenance activities.

Operating with Limited or No Voice Communications Tools

It is essential to maintain communications, both internally and with external entities, even when normal voice communications are severely degraded, compromised, or completely unavailable.

3.20 Establish procedures that take effect in the event of severely degraded or total loss of reliable voice communications.

3.20.1 Describe how coordination is maintained between entities that are required by NERC Reliability Standard COM-001 [4] to have Interpersonal Communications capability.

3.20.2 Identify how the total loss of reliable voice communications impacts other emergency procedures, such as manual load shedding, transmission loading relief, blackstart, etc.

3.20.3 Describe when and how the company incident command structure (ICS) and external agencies, such as local and federal emergency management agencies, are involved in the communications process.

3.21 Identify the criteria that trigger the use of the procedures.

3.22 Verify equipment status and capability and implement the PACE plan to use the best available method.

3.23 Initiate repairs to any degraded or unavailable communications method even if a better method is available and in use.

Using Code Words for Communications

It may be necessary to verify the identity of communicating parties or to disseminate information, such as generator tripping, loss of a tie-line, energy emergency, etc., through insecure or compromised communications methods. Code words are words or phrases with meaning only to specific individuals or parties. Code words are used to verify identity or provide additional security.

3.24 Code words should be common words or phrases using the English language that do not require complex spelling. See Appendix 4 for an example code word list.

> Use phrases or sentences to increase security and reduce the likelihood of the code being guessed.

3.25 Identify criteria that trigger the use of code words and the process to ensure all parties involved understand when they are in use. Use of code words can be triggered when there is uncertainty, when communications are unreliable or compromised, or any reason deemed necessary to verify a party's identity.

3.26 Establish code words to verify the identity of a communicating party.

3.26.1 The communicating party is asked to provide the code word prior to communication proceeding. If the individual cannot provide the proper word or phrase, communication ends.

3.26.2 To prevent the code word from being guessed, hints are not used.

3.27 Establish code words to communicate information or Operating Instructions in the event of severely degraded or total loss of reliable communications.

3.27.1 Review critical tasks and procedures that need to be completed under these conditions; identify how information about these tasks can be communicated using code words.

3.27.2 It may be necessary to modify critical tasks and procedures to fully use code words. For example, complex tasks can be broken down into smaller statements that link to the code words.

> Code words can be used to configure the system in pre-studied and conservative operating postures that are designed to address foreseeable operating situations and minimize the likelihood of system instability, overloading neighboring systems, burdening the interconnection, etc.

3.28 Identify how the code words are delivered to the receiving party. Since code words can only be understood by the sender and receiver, any delivery method can be used.

3.28.1 When normal secure communications are unreliable or unavailable, transmit messages using code words through unsecure methods such as microwave, VHF, UHF, amateur (ham) radio, etc.

3.28.2 When there is no communications tool available, hand deliver the message using non-essential employees or third parties such as local emergency management and government entities (i.e., FEMA, National Guard, etc.).

3.29 Develop multiple code word lists to provide resilience and protect the confidentiality of the system in the event the list is compromised.

- Only use a code word list for one event, whether to confirm identity or relay information
- Store lists in multiple locations
- Use code words to identify each list and to verify each party is using the same list

3.30 Develop a process to replace code words periodically. This could be accomplished manually or through automatic methods similar to how authenticator applications use one-time passcodes.

3.31 Conduct training and drills on the use of code words.

3.32 Periodically review and update procedures and operating postures that use code words to ensure continued relevance to foreseeable operating scenarios.

4. Conclusion

Adequate communications methods are critical for operating the bulk electric system under normal and emergency operations. Redundancy ensures that system operators can maintain effective communications even if primary channels fail due to technical issues, cyberattacks, or natural disasters. Backup systems, such as secondary data networks, satellite communications, or alternative voice channels allow operators to continue exchanging essential information without interruption. This layered approach minimizes downtime, facilitates quick recovery, and helps prevent cascading failures that could jeopardize grid reliability.

5. References

[1] North American Transmission Forum, "NATF Practice - NATF Supplemental Operating Strategies and Resiliency Practices.pdf," [Online]. Available: https://portal.natf.net/document-viewer?id={95742448-a3f2-6307-be03-ff00005e4fde}.

[2] National Council of Statewide Interoperability Coordinators, "Leveraging the PACE Plan into the Emergency Communications Ecosystem," 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-10/2024_NCSWICPTE_Leveraging_PACE_Plan_Emergency_Comms_Ecosystems.pdf.

[3] Cybersecurity & Infrastructure Security Agency, "Government Emergency Telecommunications Service (GETS)," [Online]. Available: https://www.cisa.gov/resources-tools/services/government-emergency-telecommunications-service-gets.

[4] North American Electric Reliability Corporation, "COM-001-3: Communications," [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/COM-001-3.pdf.

Appendix 1: PACE Plan Example

The communications methods available are placed into tiered categories of primary, alternate, contingency, and emergency. The primary methods are used under normal operations and the other methods are only used when the primary is unavailable or degraded. There should be redundancy built into each level to increase resilience. Below is an example of a PACE plan listing the communications method for each level.

Level	Communications Method	Redundancy	Failure Response
PRIMARY	• Automatic ring down circuits (ARDs) • Voice over IP (VoIP)	• Provide multiple servers for voice communication systems	• Initiate procedures to make repairs • Enable Alternate methods
ALTERNATE	• Land lines to the public switched telephone network (PSTN) • Cellular telephone network	• Provide multiple lines for PSTN access • Use multiple cellular communication providers	• Initiate procedures to make repairs • Notify ICS and external entities as per procedure • Enable Contingency methods
CONTINGENCY	• Satellite telephone network • Government Emergency Telecommunications Service (GETS) • Wireless Priority Service (WPS) • Microwave	• Provide portable units	• Initiate procedures to make repairs • Notify ICS and external entities as per procedure • Enable Emergency methods

EMERGENCY	• Radio systems
	  ○ HF
	  ○ VHF
	  ○ UHF
	• Manual communications using code words
	  ○ Ham (amateur) radio
	  ○ Non-essential employee or third party
		• Provide portable units
		• Maintain a secondary list of code words in the event of compromise
			• Initiate procedures to make repairs
			• Notify ICS and external entities as per procedure
			• Enact manual communications procedures

The use of code words is not restricted to the emergency level and can be used at any level when there is uncertainty of the identity of a communicating party, or when communications methods are unsecure or unreliable.

Appendix 2: Alternate Data Exchange System

Figure 1 is an example of using an alternate data exchange system to transmit data normally communicated by ICCP links. The alternate data exchange system can be used when the ICCP communications link or links fail. This can be applied for TO/TOP to RC, RC to TO/TOP, or TO/TOP to TO/TOP scenarios.

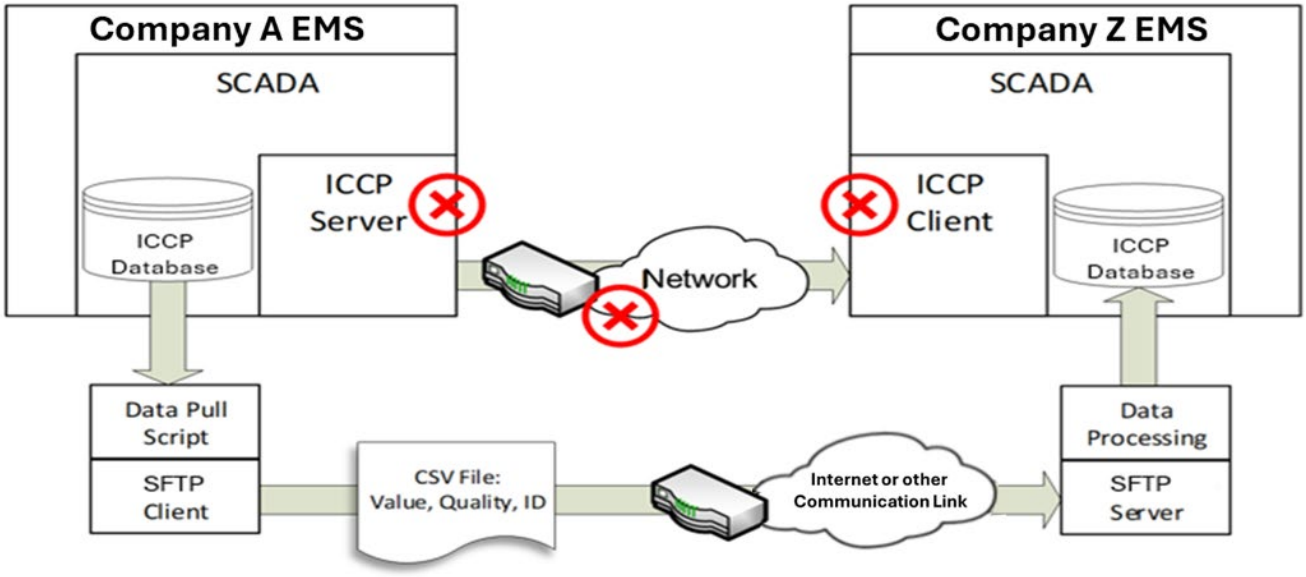

Figure 1. Alternate Data Exchange System

Appendix 3: Alternate Data Flow

Figure 3 is an example of an automated workflow where a file is created from the sending EMS, uploaded via SFTP, and processed by the receiving EMS. This can be applied for TO/TOP to RC, RC to TO/TOP, or TO/TOP to TO/TOP scenarios.

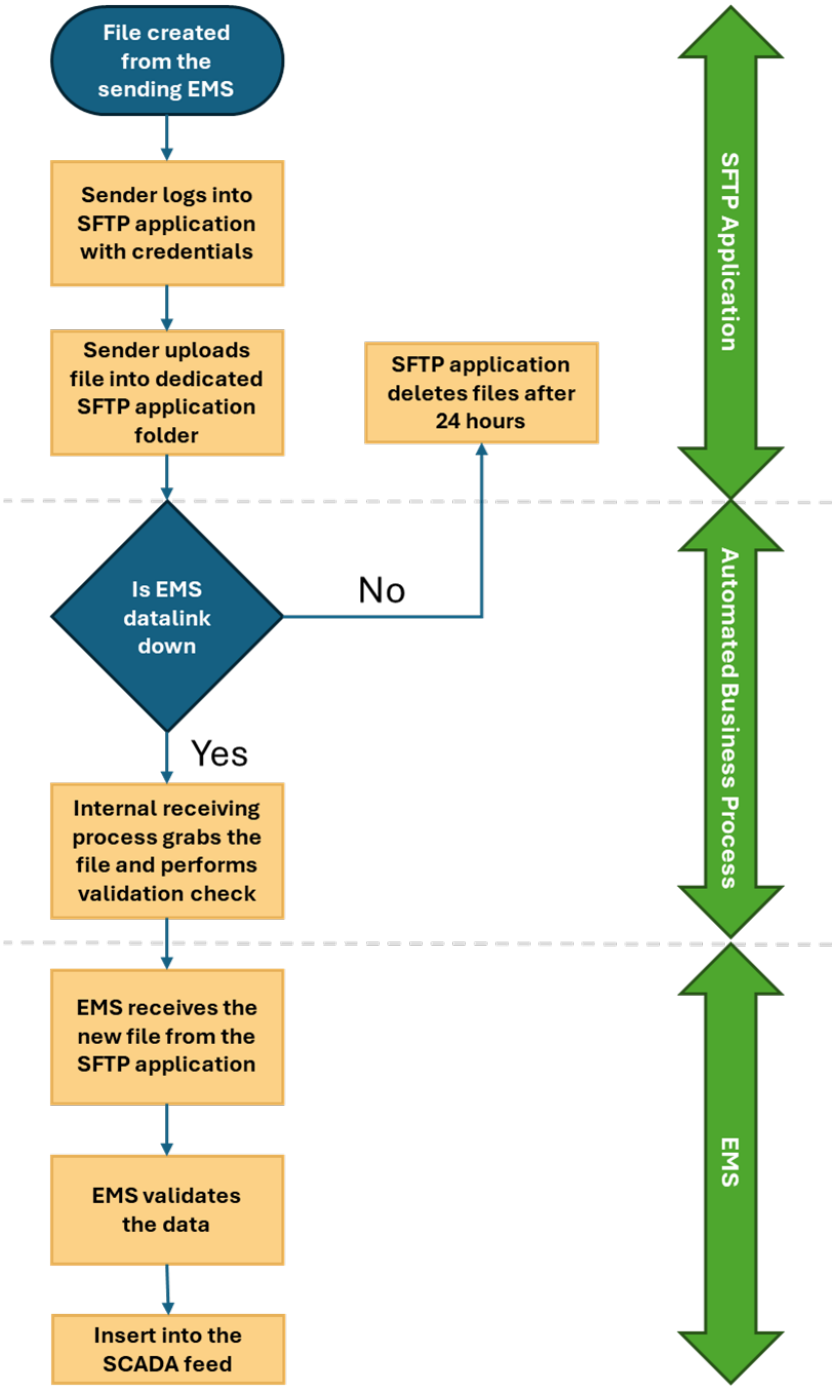

Figure 2. Data Flow

Appendix 4: Code Word Examples

Code words are arranged into lists and paired with an individual/company identity or Operating Instruction. It is recommended to have multiple code words or phrases so that no code word is used more than once. Words or phrases should not be reused if the identity of an individual could not be confirmed or if a third party was involved in relaying messages.

The key to using code words is to identify tasks that need to be completed even in the event of a loss of communications. Critical tasks and Operating Procedures should be reviewed to identify what information would need to be communicated in the event of compromised or lost voice communications. Complex tasks can be broken down into smaller statements that link to the code words.

Table 1 is an example of code word phrases generated by prompting an artificial intelligence tool to generate short, random phrases without including any company information. The generated code words were randomly paired with a definition.

Table 1: Code Word Examples

Code words for confirming identities (external or internal)	
Code word	**Definition**
1. Chasing the morning sun	Company Alpha
2. Whispering winds of change	Company Bravo
3. Dancing in the moonlight	Company Charlie
4. A splash of color	Department Xray
5. Echoes of laughter	Department Yankee
6. Beyond the horizon	Department Zulu
Code words for communicating Operating Instructions	
Code word	**Definition**
7. A moment in time	Implement Conservative Operations
8. Dreams take flight	Implement supplemental operating strategies (SOS)
9. Under the starry sky	EMS is functioning but there is no voice communications
10. Waves of tranquility	All data and voice communications are unavailable
11. A spark of inspiration	Deploy personnel to essential substations
12. Hidden in plain sight	Report status of equipment
13. The road less traveled	Manually document metering information hourly
14. A symphony of silence	Implement Tier 3 Load Shed
15. Through the looking glass	Open your end of line Alpha
16. Glimpses of tomorrow	Maintain tie-line flow
17. Beyond the clouds	Reduce voltage output by 3%
18. Moments of serenity	Operate at minimum MW output
19. A touch of magic	Implement safe shutdown
20. Remembering yesterday	Remain offline until further notice