NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Reliability and Security Technical Committee

September 8, 2021 | 11:00 a.m.–4:30 p.m. Eastern
Virtual Meeting via WebEx

Attendee WebEx Link: Join Meeting

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement*

Introductions and Chair's Remarks

1. **Administrative items**
   a. Arrangements
   b. Announcement of Quorum
   c. Reliability and Security Technical Committee (RSTC) Membership 2020-2023*
      i. RSTC Roster
      ii. RSTC Organization
      iii. RSTC Charter
      iv. Parliamentary Procedures*
      v. Participant Conduct Policy

Consent Agenda

2. **Minutes - Approve**
   a. June 8-9, 2021 RSTC Meeting*

Regular Agenda

3. **Remarks and Reports**
   a. Remarks – Greg Ford, RSTC Chair
      i. Subcommittee Reports*
      ii. RSTC Work Plan
   b. Report of August 12, 2021 Member Representatives Committee (MRC) Meeting and Board of Trustees Meeting – Chair Ford

4. **Nominating Subcommittee Member Election* – Approve -** Chair Ford

   Due to a member resignation from the RSTC's Nominating Subcommittee (NS), the RSTC held a nomination period to fill the vacant position. Per the RSTC Charter, "The Nominating Subcommittee members are nominated by the RSTC chair and approved by the full RSTC membership." Nominations were sought and a recommended candidate selected by the RSTC

Chair in consultation with the RSTC Executive Committee. The recommended candidate is Edison Elizeh, Sector 4 representative.

5. **Review of RSTC Policy Input and Improvements to the RSTC* - Information –** Chair Ford

   The RSTC received Policy Input in spring of 2021. This information item will provide an overview of the Policy Input highlights as well as changes in the operation of the RSTC as well as collaboration within the ERO Enterprise and with other stakeholder groups.

12:05 -12:25 P.M. – LUNCH BREAK – 20 mins

6. **RSTC Proposed Charter Amendments* – Review –** Nina Johnston

   In November 2019, the NERC Board of Trustees (Board) approved the creation of the RSTC to replace the former Operating, Planning and Critical Infrastructure Protection committees to improve the effectiveness and efficiency of those committees. The Board also approved the charter of the RSTC at this time. The RSTC has been operating under its charter for almost two years. NERC proposes amendments to the RSTC charter to further enhance the efficiency of the RSTC's operations and provide greater clarity.

7. **2021 ERO Reliability Risk Priorities Report and the RSTC Work Plan* – Information –** Thomas Coleman, NERC Staff and Rich Hydzik, RSTC Vice Chair

   This agenda item will review the 2021 ERO Reliability Risk Priorities Report and the process to incorporate risk mitigation activities into the RSTC Work Plan. Efforts to identify and prioritize risks from the report will also be discussed. Chair Ford will request volunteers from the RSTC to participate in the risk prioritization and risk mitigation planning process to develop RSTC subgroup work plan items for approval by the RSTC in December, 2021.

8. **Risk Registry*– Update –** Soo Jin Kim, NERC Staff

   In an effort to continually monitor the existing risks to the bulk power system (BPS) and manage the efforts of the ERO Enterprise to actively identify and address current and new risks, NERC created a Risk Registry. This registry overlaps some with the risk profiles identified in the latest ERO Reliability Risk Priorities Report (RISC Report) and other risks identified in past reports and assessments. In addition to reporting on future emerging risks, the Risk Registry also focuses on reporting on activities addressing current emergent risks to the BPS. Future versions of the Risk Registry will be used as project/resource management tool and will include a consistent risk prioritization method that will be periodically reviewed with the RISC.

9. **Failure Modes and Mechanism Task Force (FMMTF) - Information –** Rick Hackman, NERC Staff | Patrick Doyle, Sponsor

   The joint 2013 NERC Operating and Planning Committees' AC Substation Equipment Task Force report recommended that information on station equipment failures be collected through the NERC Event Analysis process. The Failure Modes and Mechanisms Task Force (FMMTF) was created by the EAS to analyze 14 types of BES substation equipment to determine their failure modes and mechanisms, FMM trends and patterns, and improve BES reliability by providing information useful for reducing station equipment failures. A short video explaining the FMM approach* is available. Currently FMM diagrams for eight types of common station equipment are available in the ERO portal for use and more are being prepared. **https://vimeopro.com/nerclearning/cause-coding/video/208745179*

Recently, a FMM approach was used in discussing February 2021 Cold Weather Generation Problems in the NERC Winter Weather Webinar on September 2.

10. **Security Working Group Update – Information –** Katherine Street, SWG Co-chair | Christine Hasha, Sponsor

    Co-chair Street will provide an update on current SWG projects, new activities, and administrative updates.

2:30 p.m. - BREAK – 15 mins

11. **Restoration Analysis to Evaluate Resilience of the Transmission System under Extreme Weather* – Information –** Svetlana Ekisheva

    The presentation will cover a new analysis included in the *2021 State of Reliability Report* (SOR), an analysis of restoration of the North American transmission system after extreme weather events. Additionally to the material included in the 2021 SOR, we will analyze impact and recovery for the top weather-related transmission events from 2015 to 2020 and discuss similarities and differences in restoration processes for most disruptive types of extreme weather (hurricanes, tornadoes, winter storms etc.).

12. **Cybersecurity for the Operational Technology Environment (CyOTE) Program Information* –** Sam Chanoski, Idaho National Labs

    The Department of Energy's Cybersecurity for Operational Technology Environments (CyOTE™) program provides a methodology for energy sector asset owner-operators to combine network-based sensor data with local context to recognize faint signals of malicious cyber activity before an adversary can cause higher-impact effects. CyOTE began as a pilot sponsored by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) in 2016, transitioned to a program in 2019, and in July 2021 publicly released the "Methodology for Cybersecurity in Operational Technology Environments" report.

    By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection from broader but informative sources in operations and even in the business domain, asset owners can better understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. Visibility is necessary, but the importance of visibility is in the understanding and decisions it drives – complicated by infrastructure changes, new technologies, and determined and sophisticated adversaries. CyOTE's vision is to allow an entity to independently get to the point of making a risk informed business decision on whether to respond to an incident or fix a reliability failure, sooner and with more confidence.

13. **Chair's Closing Remarks and Adjournment**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

RSTC Meetings – Governance Management

Chair will state the governance management of the meeting as follows:

- For each topic, the Chair will state the primary motion, ask for first/second, speaker will present, committee then has discussion.
- **At the conclusion of the discussion,** a secondary motion can be offered, the Chair will ask for first/second, discussion/debate; the Chair will then call for a vote.
- If the secondary motion does not receive a second or is voted down, the Chair will go back and restate the primary motion. At this point, the following actions may proceed:
    - Debate on that primary motion again;
    - Another secondary motion can be offered;
    - Motion could be offered to postpone, table, etc. Management of next action will follow the first two bullets.

The Chair is able to initiate a motion to end a debate.

Motions can encompass accepting minor revisions as provided during the discussions and reflected in the words of the motion.

Guiding principle is one thing at a time.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Types of Documents

Reliability & Security Guidelines	*Reference Documents, Whitepapers and Technical Reports*	*Implementation Guidance*	*Standard Authorization Request*
• *Formulated from best and/or optimal practices* • *Suggested approaches or behaviors* • *"HOW" certain objectives can be met* • *Recommendations for how objectives "could" or "should" be accomplished*	• *Documented technical concepts* • *Definitions of technical terms* • *Defined methods or approaches* • *Can be used as justification to support "WHY" certain practices are needed*	• *Provides examples or approaches for "HOW" Registered Entities could demonstrate compliance with Reliability Standard requirements.* • *Used in Compliance Monitoring and Enforcement activities* Submitted to ERO	• *Defines scope, reliability benefit, and technical justification for a new or modified Reliability Standard or definition.* • *Identifies "WHAT" requirements are needed to ensure the reliable operation of the BPS* Submitted to SC

Reliability Assessment Reports

- Independent and objective evaluations of BPS reliability conducted by the ERO
- Subgroup used to gain industry perspectives, expertise, and validation
- Requires BOT approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Types of Documents: Member Considerations

Reliability & Security Guidelines

- *ACCEPT for public comment*
  - *Is guidance needed on this topic?*
  - *Are there major flaws?*
- *APPROVE*
  - *Has the public and committee comments been sufficiently addressed?*
  - *Do you agree with the recommended guidance?*

Reference Documents, Whitepapers and Technical Reports

- *APPROVE*
  - *Does it provide sufficient detail to support technical, security, and engineering SMEs?*
  - *Has it been peer reviewed and supported by a technical subgroup?*
  - *Is it foundational and/or conceptual*
  - *Does it contain specific recommendations?*

Implementation Guidance

- *ENDORSE*
  - *Does it provide examples or approaches on how to implement a Reliability Standard?*
  - *Does it meet the expectations identified in the Implementation Guidance Development and Review Aid?*

Standard Authorization Request

- *ENDORSE*
  - *Is the SAR form complete?*
  - *Does it contain technical justification?*

Reliability Assessment Reports

- ENDORSE
  - Is there general agreement with findings and recommendations?
  - Was the process followed?

RSTC Actions

- **Approve:** The RSTC has reviewed the deliverable and supports the content and development process, including any recommendations.
- **Accept:** The RSTC has reviewed the deliverable and supports the development process used to complete the deliverable.
- **Remand:** The RSTC remands the deliverable to the originating subcommittee, refer it to another group, or direct other action by the RSTC or one of its subcommittees or groups.
- **Endorse:** The RSTC agrees with the content of the document or action, and recommends the deliverable for the approving authority to act on. This includes deliverables that are provided to the RSTC by other NERC committees. RSTC endorsements will be made with recognition that the deliverable is subject to further modifications by NERC Executive Management and/or the NERC Board. Changes made to the deliverable subsequent to RSTC endorsement will be presented to the RSTC in a timely manner. If the RSTC does not agree with the deliverable or its recommendations, it may decline endorsement. It is recognized that this does not prevent an approval authority from further action.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Meeting Minutes
Reliability and Security Technical Committee

June 8-9, 2021

Webinar

A regular meeting of the NERC Reliability and Security Technical Committee (RSTC) was held on June 8-9, 2021, via webinar. The meeting presentations are available here: June 8, 2021 and June 9, 2021.

Chair Ford called the meeting to order, and thanked everyone for attending. Tina Buzzard reviewed the procedures for the meeting, reviewed the Antitrust Compliance Guidelines, and confirmed quorum, as well as provided an overview of the polling actions to be used for Committee actions during the meeting.

Introductions and Chair's Remarks

Chair Ford provided an overview of the agenda noting that due to the number of action items before the Committee it may be necessary to defer some non-action topics to the next meeting.

Chair Ford called on Nina Johnston to review the meeting governance guidelines which were included in the advance materials package.

Consent Agenda

Chair Ford reviewed the Consent Agenda and asked RSTC members if they concurred with the items on it. Brian Evans Mongeon made a motion to approve the consent agenda, but noted that the RSTC did not need to act on Agenda Item 2 as the RSTC Chair has full authority to appoint working group Chairs. Upon motion duly made and seconded, the Committee approved the minutes under the Consent Agenda.

Regular Agenda

Chair Ford welcomed Jim Piro, NERC Board of Trustees, who has been assigned by Board Chair DeFontes, to act as the Board liaison to the RSTC.

Chair Ford reviewed with the Committee re-implementing executive sessions as previously completed by the prior Operating, Planning, and Critical Infrastructure and Protection Committees. He stated the invite previously sent titled, Informational Session, provided confusion and he made the decision to cancel that session and open to the Committee for input on if Executive Sessions should be re-implemented, if there is a need to conduct informational sessions (where proposed agenda topics are discussed) or continue under current meeting structure. Committee members provided input and Chair Ford asked for additional comments be sent to him directly via email and he would report out at a future meeting a summary of input provided.

Chair Ford referenced the subgroup reports contained in the Agenda package and thanked the Sponsors for reports being submitted in the requested format.

Lastly, Chair Ford provided highlights from the February 2021 Member Representatives Committee and Board of Trustees meetings.

Resources Subcommittee (RS) Documents

Reliability Guideline: ACE Diversity Interchange, Reliability Guideline: Operating Reserve Management and Balancing and Frequency Control Reference Document

Motions were made to approve the reliability guidelines and reference document. RS Chair Greg Park presented that both guidelines and reference document were a three-year review of existing, posted documents, and that all three documents were posted for 45-day comment periods and conforming revisions made to them based on comments received. Clean and redline versions were included in the advance agenda package and upon motions duly made and seconded, the Committee approved Reliability Guideline: ACE Diversity Interchange, Reliability Guideline: ACE Diversity Interchange, Reliability Guideline: Operating Reserve Management and Balancing and Frequency Control Reference Document.

Reliability Guideline: Inadvertent Interchange

Motion was made to post the Reliability Guideline: Inadvertent Interchange for a 45-day comment period. RS Chair Park presented that the guideline is a three-year review of an existing guideline that has been updated and that the Guideline Metrics section has been added in addition to the content update. During discussion, a RSTC member suggested that both clean and redline documents be posted for industry review, the membership and NERC staff concurred and will ensure both versions are posted as part of the 45-day comment period. Upon motion duly made and seconded, the Committee approved to post the Reliability Guideline: Inadvertent Interchange for a 45-day comment period.

Reliability Guideline: Gas and Electrical Operational Coordination Considerations

Motion was made to approve the Reliability Guideline: Gas and Electrical Operational Coordination Considerations. RTOS Chair Chris Pilong presented on the guideline noting that the guideline was revised by the Real Time Operating Subcommittee and the Electric Gas Working Group, and was posted for a 45-day comment period and conforming revisions made to it based on comments received. Clean and redline versions were included in the advance agenda package along with a response to comments. Upon motion duly made and seconded, the Committee approved the Reliability Guideline: Gas and Electrical Operational Coordination Considerations.

Security Guideline for the Electricity Sector: Assessing and Reducing Risk

Motion was made to approve the Security Guideline for the Electricity Sector: Assessing and Reducing Risk. SWG Co-Chair Brent Sessions presented that the Guideline is to help organizations determine their current security and compliance posture and develop an improvement plan for addressing any gaps that are identified. He stated the tool for that analysis maps requirements of the CIP Reliability Standards to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (hereafter referred to as "the framework"), and it can help a responsible entity identify areas that may require further action. The document was posted for a 45-day comment period and conforming revisions made to it based on

comments received, and clean and redline versions were included in the advance agenda package along with a response to comments. Discussion occurred among Committee members on if this document classified as a guideline or reference document. A friendly amendment was offered to approve the document as a reference document, retain the survey, but update all references to guideline in the document. In addition, a secondary motion was offered to table the action on the guideline until such determination on its classification and updates. NERC Legal provided that the Committee would need to first act on the friendly amendment which upon motion duly made and seconded passed. NERC Legal then provided that the primary motion would next need to be acted upon at which time the requesting Committee member could offer the secondary motion to table. That motion was made again and seconded, the secondary motion failed. The Committee then acted on the main primary motion, and upon motion duly made and seconded the Security Guideline for the Electricity Sector: Assessing and Reducing Risk was approved, amended as provided under the approved friendly amendment.

Implementation Guidance: Cloud Solutions and Encrypting BES Cyber System Information
Motion was made to endorse the Implementation Guidance: Cloud Solutions and Encrypting BES Cyber System Information. SWG Co-Chair Sessions presented that the purpose of this Compliance Implementation Guidance is to provide examples for how encryption can be utilized to secure and restrict access to BES Cyber System Information in various commonly used cloud services. He noted the RSTC endorsed this Compliance Implementation Guidance in June of 2020 and it was submitted to the ERO for approval. In addition, Co-Chair Sessions stated the ERO Enterprise identified some concerns with the guidance document and provided feedback to the team, and that the SWG made revisions to the document to address the ERO Enterprise's concerns. Upon motion duly made and seconded, the Committee endorsed submitting the document to the ERO Enterprise as Compliance Implementation Guidance.

MOD-032 Technical Reference Document
Motion was made to approve the MOD-032 Technical Reference Document. PPMVTF Chair Shawn Patterson presented on the technical reference document noting the document provides useful information and materials for entities regarding the development of models for interconnection-wide base case creation. He stated the reference document focuses specifically on the provision of data and models by generator owners to the transmission planner and planning coordinator following MOD-032 requirements, and the document provides details regarding the types of information provided. In addition Chair Patterson stated that this action completed the scope of work for the PPMVTF. Upon motion duly made and seconded, the Committee approved the MOD-032 Technical Reference Document and the disbandment of the PPMVTF. Mr. Lauby thanked the Chair and members of the PPMVTF for their work.

Security Integration and Technology Enablement Subcommittee (SITES) Update and Work Plan
Motion was made to approve the SITES work plan. SITES Chair Benny Naas, presented an update on SITES activities and presented the work plan for approval. Upon motion duly made and seconded, the Committee approved the SITES work plan.

Inverter-based Resources Performance Working Group (IRPWG) San Fernando Disturbance Follow-Up White Paper

Motion was made to approve the Inverter-based Resources Performance Working Group (IRPWG) San Fernando Disturbance Follow-Up White Paper. IRPWG Chair Al Schriver presented that the white paper was developed by the IRPWG as a follow-up to the July 2020 San Fernando Disturbance Report published by NERC. He stated that report contained a set of key findings and recommendations and that the IRPWG discussed each of the key findings and recommendations in detail, provided a brief technical discussion and basis for each item, and where appropriate recommended follow-up action items. He provided that Table 1 shows the key findings and recommendations from the NERC disturbance report on the left-hand column and the IRPWG follow-up and recommendations for each item in the right-hand column. Upon motion duly made and seconded, the Committee approved the Inverter-based Resources Performance Working Group (IRPWG) San Fernando Disturbance Follow-Up White Paper.

IRPWG TPL-001-5 SAR for BPS-Connected Inverter-based Resources

Motion was made to endorse the IRPWG TPL-001-5 SAR for BPS-Connected Inverter-based Resources. IRPWG Chair Schriver provided an overview of the SAR presented. He stated that considering current trends, the NERC IRPWG undertook review of the TPL-001 standard for considering BPS-connected IBRs, and that the review is captured in the RSTC-approved white paper: IRPTF/IRPWG: IRPTF Review of NERC Reliability Standards. He noted that the SAR proposes to update TPL-001-5.1 to address the issues identified in the white paper. During discussion by members, concerns were raised about the applicability to specific entities as well as equipment and BPS vs. BES issues. Upon motion duly made and seconded, the motion failed. The Committee requested the IRPWG take under consideration the input provided during the meeting and consider presenting the SAR at a future meeting.

Vice Chair Election

Motion was made to approve the presented vice chair candidate. RSTC NS member Jody Green presented on the vice chair nomination process and stated that the NS recommended Rich Hydzik be elected as the RSTC vice chair. Upon motion duly made and seconded, the Committee approved Mr. Hydzik as the RSTC vice chair.

Chair's Closing Remarks

Chair Ford provided closing remarks and adjourned the meeting.

Wednesday, June 9, 2021

Chair Ford called the meeting to order, and thanked everyone for attending. Tina Buzzard reviewed the procedures for the meeting, reviewed the Antitrust Compliance Guidelines, and confirmed quorum, as well as provided an overview of the polling actions to be used for Committee actions during the meeting.

Introductions and Chair's Remarks

Chair Ford provided an overview of the agenda noting that due to the number of action items before the Committee it may be necessary to defer some non-action topics to the next meeting. In addition, Chair Ford stated that as there was robust discussion the day prior on the definitions and purpose of the different types of documents, he wanted to confirm with the RSTC that John Moura from NERC is finalizing a presentation for the RSTC that will provide clarity on the different documents and their definitions/purpose and will look to provide that presentation during the 4th quarter meeting.

GADS Section 1600 Data Request

Motion was made to post the GADS Section 1600 Data Request for a 45-day comment period. Mr. Jack Norris, NERC staff presented on the data request and sought Committee concurrence to post for a 45-day comment period the following proposed data collection:

- GADS Conventional – Additional design and event data.
- GADS Photovoltaic (PV) – Configuration, performance and event data as well as outage detail.
- GADS Wind – Configuration, performance and event data as well as outage detail. Clarify reporting requirements related to plant size and commissioning date.

Upon motion duly made and seconded, the Committee approved posting the GADS Section 1600 Data Request for a 45-day comment period.

2021 State of Reliability Report

Mr. John Moura and Ms. Margaret Pate, NERC staff reviewed the highlights of the 2021 State of Reliability Report, as well as reviewed the approval timeline for the report stating an email ballot for endorsement by the RSTC would be conducted from July 7-17, submitted for approval by the Board of Trustees on August 12, and a target release date of August 13.

System Protection and Control Working Group (SPCWG) Scope Document

Motion was made to approve the System Protection and Control Working Group (SPCWG) Scope Document. SPCWG Chair Jeff Iler presented on the scope and reviewed the minor revisions. Upon motion duly made and seconded, the Committee approved the SPCWG scope document.

Probabilistic Assessments Working Group (PAWG) 2020 ProbA Scenario Case Study Report

Motion was made to approve the Probabilistic Assessments Working Group (PAWG) 2020 ProbA Scenario Case Study Report. PAWG Chair Andreas Klaube presented on the report noting the PAWG responded to the RSTC and RAS comments on this study report, that it combined all of the Assessment Areas' sensitivity results from the 2020 Probabilistic Assessment data and compares the results against the base case data. PAWG Chair Klaube also provide that the PAWG had obtained RAS approval. Upon motion duly made and

seconded, the Committee approved the Probabilistic Assessments Working Group (PAWG) 2020 ProbA Scenario Case Study Report.

PAWG Data Collections Technical Reference Document
Motion was made to approve the PAWG Data Collections Technical Reference Document. PAWG Chair Klaube presented on the reference document noting that the PAWG responded to the RSTC on the technical report that discusses the various data sources available to a resource planner when performing probabilistic studies or assessments. Upon motion duly made and second, the Committee approved the PAWG Data Collections Technical Reference Document.

System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) Reliability Guideline: UFLS Studies
Motion was made to post the System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) Reliability Guideline: UFLS Studies for a 45-day comment period. SPIDERWG Chair Kun Zhu presented that the SPIDERWG developed the Reliability Guideline to provide guidance on impacts that higher penetration of DER may have on UFLS. Upon motion duly made and seconded, the Committee approved to post the guideline for a 45-day comment period.

SPIDERWG Presentation on the Modeling Survey
SPIDERWG Chair Zhu presented on the modeling survey stating that the SPIDERWG performed an informal survey of its membership regarding distributed energy resource (DER) modeling practices. He noted the SPIDERWG consists of a wide range of industry experts and a cross-section of industry representation, and 45 entities participated. The survey was primarily geared towards understanding DER modeling practices of Transmission Planners (TPs) and Planning Coordinators (PCs), which are well-represented on SPIDERWG. Chair Zhu stated results from the survey were analyzed to identify any major trends in DER modeling practices, to characterize the level of detail that TPs and PCs are using for DER modeling, and to identify any potential gaps in these practices that should lead future efforts for SPIDERWG and industry.

Energy Reliability Assessments Task Force (ERATF) Update
ERATF Chair Peter Brandien provided an update on the ERATF activities.

Standing Committee Coordination Group (SCCG) Update
Mr. Stephen Crutchfield, NERC staff, provided an update on the SCCG activities.

Risk Registry
Ms. Soo Jin Kim, NERC staff presented on the new risk registry tool noting that in an effort to continually monitor the existing risks to the bulk power system and manage the efforts of the ERO Enterprise to actively identify and address new threats, NERC will work with the SCCG to create a Risk Registry and in an effort to ensure the risk registry captures the right categories of current risks, NERC will seek feedback on the registry as it is developed. She stated the registry will overlap some with the risk profiles identified in the latest ERO Reliability Risk Priorities Report (RISC report), but the Risk Registry will focus on reporting current risks while the RISC report is a forward-looking view of the BPS.

NERC Bylaws Changes

Ms. Lauren Perotti, NERC staff presented an overview of the NERC Bylaw changes which were approved by FERC on April 5, 2021. She stated that among other changes, the revised Bylaws modified the Sector membership definitions to ensure consistency with the intent of fair and balanced participation in NERC governance by stakeholders with a significant role in the reliability and security of the bulk power system.

Forum and Group Reports

Mr. Schriver, NAGF and Mr. Carter, NATF provided highlights of their written reports that were provided in the advance agenda package.

RSTC 2020 Calendar Review

Mr. Crutchfield presented on the remainder of the 2020 calendar noting that the September meeting dates had been adjusted to September 8 and 9 and the time of the meeting was also extended in an effort to ensure the topics presented each day could be addressed.

Closing Remarks and Adjournment

Chair Ford thanked attendees and particularly the sponsors introducing the agenda items and making the motion for approval/endorsement items. He also thanked the Chairs of the subgroups for their efforts in presenting the agenda items. Mr. Hydzik thanked the RSTC for their confidence in him as being the vice chair, and Mr. Lauby praised the sponsor's role and their enthusiasm and thanked the Chairs.

There being no further business before the RSTC, Chair Ford adjourned the meeting.

Next Meeting

The RSTC will meet virtually in September 8, 2021, 11:00 a.m. - 4:30 p.m. eastern time.

Stephen Crutchfield

Stephen Crutchfield
Secretary

RSTC Status Report – Event Analysis Subcommittee (EAS)

Chair: Vinit Gupta
Vice-Chair: Ralph Rufrano
September 8,2021

On Track
Schedule at risk
Milestone delayed

Purpose: The EAS will support and maintain a cohesive and coordinated event analysis (EA) process across North America with industry stakeholders. EAS will develop lessons learned, promote industry-wide sharing of event causal factors and assist NERC in implementation of related initiatives to lessen reliability risks to the Bulk Electric System.

Recent Activity

- The EAS has developed four new Lessons Learned since the June 2021 RSTC meeting.
- Winter Weather Webinar was conducted on September 2nd.
- FMMTF: Two Diagrams Drafted & Two Updated in 2021

Items for RSTC Approval/Discussion:

- None at this time.

Ongoing & Upcoming Activities

- Development of Lessons Learned
- EMSWG will host the 9th annual Monitoring & Situational Awareness Technical Conference (3 Unique Virtual Sessions) in Fall 2021.
- FMMTF Development of Failure Mode & Mechanism Diagrams

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Pandemic Response Lessons Learned		Completed
Review & Input into EA Chapter of 2021 SOR		Completed in coordination with PAS
EAS Scope Document		Approved March 2,2021
Events Analysis Process Review		On going

RSTC Status Report – Electromagnetic Pulse Working Group (EMPWG)

Chair: Aaron Shaw
Vice-Chair: Rey Ramos
February 9th, 2021

On Track
Schedule at risk
Milestone delayed

Purpose: The purpose of the EMPWG is to address key points of interest related to system planning, risks and assessments, modeling, and reliability impacts to the bulk power system (BPS).

Items for RSTC Approval/Discussion:

- **N/A**

Recent Activity

- Solicitation of industry volunteers in EMPWG.

Upcoming Activity

- Formally establish EMPWG team structure by March 31st
- EMP Technical Workshop by end of Q2 2021

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Expand Membership		Industry solicitation was sent out on January 21, 2021
Establish Team Structure and Nominate Team leads		EMPWG Leadership is reviewing incoming nominations received by industry.

RSTC Status Report – Energy Reliability Assessment Task Force (ERATF)

Chair: Peter Brandien
September 8-9, 2021

On Track
Schedule at risk
Milestone delayed

Purpose: The ERATF is tasked with assessing risks associated with unassured energy supplies stemming from the variability and uncertainty from renewable energy resources, limitations of the natural gas system and transportation procurement agreements, and other energy-limitations that inherently exist in the future resource mix.

Recent Activity:

- The questionnaire was sent to the RSTC subcommittees and working groups as well as the ISO/RTOs to gather information on what entities are doing in regards to energy assessments; due back to the ERATF on September 14.
- The ERATF evaluated the NERC standards to assess whether existing requirements address fuel assurance and resulting energy limitations for the immediate and future time frames.
- The ERO Winter Weather Roadmap was presented to the ERATF team.

Items for RSTC Approval/Discussion:

- **Discussion**: Update the RSTC on the coordination activities between the ERATF and RSTC subcommittees and working groups.

Upcoming Activity:

- The task force will review the RSTC subcommittees and working group questionnaires and draft a summary report.
- The task force will engage and coordinate with research and development organizations to validate work in the focus areas.
- The task force will coordinate studies and plans with adjacent Balancing Authorities to identify enhanced collaborative regional support.
- The ERATF will implement the recommendations documented in the ERO Winter Weather Roadmap.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Assemble the subject matter experts for Focus Areas.		On track.
The subject matter experts complete the deliverables as outlined in the work plan.		On track.
Engage industry research and development organizations to validate work from Focus Areas		On track.

RSTC Status Report – Load Modeling Working Group (LMWG)

Chair: Kannan Sreenivasachar,
Vice-Chair:

On Track
Schedule at risk
Milestone delayed

Purpose:
The LMWG is transitioning utilities from the CLOD model to the CMLD Composite Load Model. The CLOD model lacks the capability to model events like FIDVR, which can have significant consequences on planning decisions.

Items for RSTC Approval/Discussion:

- **Approve**: LMWG *Work Plan*

Recent Activity

- Completed CMLD Phased Field Tests
- Update to Motor D base parameters
- EPRI initial test results on AC phasor model in PSLF
- Inclusion of CMLD model in MMWG 2021 Series Cases

Upcoming Activity

- *CMLD Field Test Survey Summary*
- *CMLD Field Test Report*
- *Transient Voltage Response Whitepaper*
- *On-going testing by entities with updated Motor D parameters*

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Industry outreach - working with NERC MMWG on data management processes		In progress
Field Test survey Summary		In progress
Field Test Report		In progress
Transient Voltage Response Whitepaper		In progress

RSTC Status Report – Performance Analysis Subcommittee (PAS)

Chair: Brantley Tillis
Vice-Chair: David Penney
September 16, 2020

On Track
Schedule at risk
Milestone delayed
Not started
Complete

Purpose: The PAS reviews, assesses, and reports on reliability of the North American Bulk Power System (BPS) based on historic performance, risk and measures of resilience.

Items for RSTC Approval/Discussion:
- None

Recent Activity

- July:
  - 16th: RSTC endorsed SOR
- August:
  - 12th: NERC Board accepted SOR
- GADS Section 1600 data reporting request delayed. Comments under review.

Upcoming Activity

- SOR official release
- Review GADS Section 1600 data comments received
- Annual Commissioner-led Reliability Technical Conference
- Continue annual metric review
- Review proposed new metrics

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2021 State of Reliability Report		Board accepted
Section 1600 Data Request		Public comment period completed 7/31/21. Volume and content of comments will require additional time to review and address.
Conduct annual metric review		Second half of 2021 – review commenced
Review proposed new metrics		Second half of 2021

RSTC Status Report – Probabilistic Assessment Working Group (PAWG)

Chair: Andreas Klaube
Vice-Chair: Alex Crawford
June XX, 2021

- On Track
- Schedule at risk
- Milestone delayed

Purpose: *The primary function of the NERC Probabilistic Assessment Working Group (PAWG) is to advance and continually improve the probabilistic components of the resource adequacy work of the ERO Enterprise in assessing the reliability of the North American Bulk Power System.*

Items for RSTC Approval/Discussion:

- None

Recent Activity

.

- Met August 2021 to continue planning for the PAF
- RSTC EC "wholeheartedly" approved a new work plan item for the PAWG.
- Ongoing engagement with RAS with probabilistic components of their seasonal assessments.

Upcoming Activity

- *2021 Probabilistic Analysis Forum*– Plan to hold forum in October 2021
- *White Paper: Probabilistic Planning for the Tails* – Plan to complete by 2023
- *2022 Probabilistic Assessment* – Both the Base Case and Scenario Case begin work in 2022.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2021 NERC Probabilistic Analysis Forum		In progress, planned Q2 2021 announcement. Holding forum in October 2021

RSTC Status Report – Reliability Assessments Subcommittee (RAS)

Chair: Lewis De La Rosa (12/2019)
Vice-Chair: Anna Lafoyiannis (12/2019)
September 8-9, 2021

On Track
Schedule at risk
Milestone delayed

Purpose: The RAS reviews, assesses, and reports on the overall reliability (adequacy and security) of the BPS, both existing and as planned. Reliability assessment program is governed by NERC RoP Section 800.

Items for RSTC Approval/Discussion:

Recent Activity

- RAS Meeting July 13-15: topics included LTRA assessment area presentations and planning for the 2021-2022 WRA.

Upcoming Activity

- 2021 LTRA RSTC Review planned for September 2021.
- 2021-2022 WRA RSTC Review planned for November 2021.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2021 Long-Term Reliability Assessment		Report in development. RSTC Review planned for September 2021
2021-2022 Winter Reliability Assessment		Assessment area information request sent out to regions. Narrative and data due back in September.

RSTC Status Report – Supply Chain Working Group (SCWG)

Chair: Tony Eddleman
Vice-Chair: Open
September 8-9, 2021

On Track
Schedule at risk
Milestone delayed

Purpose: To Identify known supply chain risks and address though guidance documentation or other appropriate vehicles. Partner with National Laboratories to identify vulnerabilities in legacy equipment and develop mitigation practices.

Items for RSTC Approval/Discussion:

- **Supply Chain Standard Effectiveness Survey**

Recent Activity

- Met virtually on June 21st, July 19th and August 16th
- Completed development of a Supply Chain Standard Effectiveness Survey
  - Voluntary survey to industry
  - NERC to use the results to brief the Board on the Supply Chain Standards
- Discussing the rapidly changing supply chain environment

Upcoming Activity

- Issue Supply Chain Standard Effectiveness Survey
  - Consolidate and review results
- Guidance documentation on supply chain risk management issues and topics
  - Monitoring FERC, Executive Orders, DOE, and CISA for future directions
- Monitor Software Bill of Materials (SBoM) Project by NTIA

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Supply Chain Standard Effectiveness Survey		In Progress
Guidance documentation on supply chain risk management issues and topics		In Progress

RSTC Status Report
Security Integration and Technology Enablement Subcommittee (SITES)

Chair: Benjamin Naas
Vice Chair: Brian Burnett
September 8-9, 2021

On Track
Schedule at risk
Milestone delayed

Purpose: To identify, assess, recommend, and support the integration of technologies on the bulk power system (BPS) in a secure, reliable, and effective manner.

Items for RSTC Approval/Discussion:

- **Accept**: *None*
- **Approve**: *None*

Recent Activity

- BES operations in the cloud whitepaper: Subgroup has been formed and initial working draft has been developed.
- Zero-trust whitepaper: Subgroup has been formed.

Upcoming Activity

- BES operations in the cloud whitepaper public comment period. Date TBD.
- Zero-trust whitepaper initial draft and prep for public comment period. Date TBD.

Workplan Status *(6-month look-ahead)*

Milestone	Status	Comments
BES Operations in the Cloud	🟡	In progress Q4/2021
Zero-Trust Concepts	🟡	In progress Q4/2021
Security Integration	🟢	Planning phase Q1/2022
IT/OT Convergence	🟢	Planning phase Q1/2022
Reliability/Resilience/Security balance	🟢	Planning phase Q1/2022
Emerging Technologies	🟢	Planning phase Q1/2022
Risk Identification	🟢	Planning phase Q1/2022
Security Implementation	🟢	Planning phase Q1/2022

RSTC Status Report – System Planning Impacts from DER Working Group (SPIDERWG)

On Track
Schedule at risk
Milestone delayed

Chair: Kun Zhu
Vice-Chair: Bill Quaintance
June XX, 2021

Purpose: *The NERC Planning Committee (PC) identified key points of interest that should be addressed related to a growing penetration of distributed energy resources (DER). The purpose of the System Planning Impacts from Distributed Energy Resources)SPIDERWG) is to address aspects of these key points of interest related to system planning, modeling, and reliability impacts to the Bulk Power System (BPS). This effort builds off of the work accomplished by the NERC Distributed Energy Resources Task Force (DERTF) and the NERC Essential Reliability Services Task Force/Working Group (ERSTF/ERSWG), and addresses some of the key goals in the ERO Enterprise Operating Plan.*

Items for RSTC Approval/Discussion:

- **Approval**: *DER Modeling Survey (Includes informative presentation)*
- **Accept to post**: *Reliability Guideline: DER Forecasting Practices and Relationship to DER Modeling for Reliability Studies.*

Workplan Status *(6 month look-ahead)*

See next slide

Recent Activity

- Met in August 2021 to update work products and refocus on high priority items.
- Beginning engagement on software vendors to enhance sub-group work products.
- Discussed best path forward to addressing RSTC EC approved restoration of the MOD-032 SAR.

Upcoming Activity

- *Many deliverables targeted for RSTC action in Q3 and Q4 of 2021. Currently consisting of:*
  - *Five White Papers for review/ approval*
  - *One Reliability Guidelines to request posting for industry comment periods*
  - *One Reliability Guideline (UFLS) requesting approval*

Work Look Ahead

- On Track
- Schedule at risk
- Milestone delayed

Workplan Status (6 month look-ahead)

Milestone	Status	Comments
C6 – NERC Reliability Standards Review		Initial draft completed. Responding to various SPDIERWG reviews. Requesting RSTC review later in 2021.
O1 – White Paper FERC Order 2222 and BPS Reliability Perspectives		Initial draft of white paper complete and reviewing drafts. NERC Legal wanted review prior to RSTC engagement, delayed a quarter
S1 – Reliability Guideline: Bulk Power system Planning under Increasing Penetration of Distributed Energy Resources		Nearing completion of initial draft. Targeting RSTC request to post in Q4 2021.
V2 - Reliability Guideline: DER Forecasting Practices and Relationship to DER Modeling for Reliability Studies		Initial draft in review by SPIDERWG. Requesting RSTC to post for industry comment.
S2a – SAR: Updates to TPL-001 Regrading DER Considerations		Targeting RSTC Q4 2021 for turnaround.
S3 – Recommended Simulation Improvements and Techniques		Beginning software vendor engagement. Requesting RSTC Review of white paper
S4b – Whitepaper: DER impacts to UVLS Programs		Drafting underway
S5 – Whitepaper: Beyond Positive Sequence RMS Simulations for High DER Penetration Conditions		Initial draft nearing completion. Targeting RSTC request for review in Q4 2021. Drafting is bringing up a possible rescoping due to technical sections.
S4a – Reliability Guideline: Recommended Approaches for Developing Underfrequency Load Shedding Programs with Increasing DER Penetration		Initial 45 day comment period delayed from June RSTC.

RSTC Status Report – Security Working Group (SWG)

Co-Chair: Brent Sessions
Co-Chair: Katherine Street
September 8, 2021

On Track
Schedule at risk
Milestone delayed

Purpose: Provides a formal input process to enhance collaboration between the ERO and industry with an ongoing working group. Provides technical expertise and feedback to the ERO with security compliance-related products.

Recent Activity

- Assessing and Reducing Risk Tech Paper Document, Work Aide, and Tool Announcement with Survey Link Sent to Industry July 30, 2021
  - Outreach Event and Tool Demo with the Mid-Continent Compliance Forum
- Encryption in the Cloud IG not endorsed by ERO
- BCSI in the Cloud TTX in review. Improvements are needed so new revision likely needed
- ERT Team targeting 8/23/21 to deliver feedback to ERO. Working with ERO on development lifecycle for v6
- FERC CIP-002 Whitepaper initial call on 7/29/21 for scope, format, objectives.

Items for RSTC Approval/Discussion:

- **No Activity**

Upcoming Activity

- Determine next steps for Encryption in the Cloud Implementation Guidance
- Extranet work area reorganization and rollout
- SWG process/procedures development
  - Document approval lifecycle flowchart
  - SITES requests process being developed
- FERC CIP-002 LL strawman IG document development, 1st draft
- New version of BCSI in Cloud TTX document package

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Assess and Reducing Risks Tool Released to Industry		Complete 7/30/21
Complete Encryption in the Cloud Compliance Guidance		Complete, net endorsed 8/12/21
BCSI in the Cloud Tabletop Lessons Learned		Due Q4 for improvements to documentation
FERC CIP-002 WP		Resource constraints

System Protection and Control Working Group (SPCWG) Scope Document

Action
Approve

Summary
Due to a member resignation from the RSTC's Nominating Subcommittee (NS), the RSTC held a nomination period to fill the vacant position. Per the RSTC Charter, "The Nominating Subcommittee members are nominated by the RSTC chair and approved by the full RSTC membership." Nominations were sought and a recommended candidate selected by the RSTC Chair in consultation with the RSTC Executive Committee. The recommended candidate is Edison Elizeh, Sector 4 representative.

Agenda Item 5
Reliability and Security
Technical Committee Meeting
September 8, 2021

Review of RSTC Policy Input and Improvements to the RSTC

Action
Information

Summary
The RSTC received Policy Input in spring of 2021. This information item will provide an overview of the Policy Input highlights as well as changes in the operation of the RSTC as well as collaboration within the ERO Enterprise and with other stakeholder groups.

Policy Input to the NERC Board of Trustees
May 2021

Reliability and Security Technical Committee
Policy Input – Common Themes

General comments – Most input was supportive and many felt that the RSTC has achieved the goals set forth by the Stakeholder Engagement team and that the RSTC was effective and efficient. Some felt that more time was needed to more fully assess effectiveness and efficiency.

- While it is still early to speak to the RSTC's general performance, early actions by the committee throughout the transition point to the creation of a strong foundation for the continued trajectory of the RSTC in achieving its objectives.
- EEI agrees the RSTC has made substantial progress towards achieving the objectives of the transition.
- The Federal PMAs agree that the Reliability and Security Technical Committee (RSTC) is meeting its overall goals and objectives as was set by the Board effectively and efficiently.
- The NAGF believes that notwithstanding the challenges of remote meetings, the RSTC is meeting the objectives of the transition.
- The Cooperative Sector supported the formation of the RSTC and continues to believe the RSTC provides an effective and efficient vehicle to provide stakeholder technical input needed to support the ERO Enterprise.
- The Merchant Electricity Generators agree that the RSTC is meeting its tactical objectives in the transition from multiple technical committees and has done so despite the challenges of the COVID restrictions.
- The reorganization results were delivered in a timely manner.
- The functionality of the subgroups was maintained, and the retirement of subgroups no longer needed was appropriate.
- Best practice retention is being achieved under the new structure.
- The operating model is an improvement over the prior three committee structure in terms of documenting roles, responsibilities, and processes.
- Sector 9 members believe the new process is more effective and efficient in its facilitation of technical input.

Work prioritization and Collaboration **– Many comments included encouragement of collaboration within the ERO enterprise as well as with other stakeholder groups. In particular, close coordination with the Reliability Issues Steering Committee was encouraged. Another point was work plan prioritization and the role of the full RSTC in said prioritization. A discussion of the RISC Report, RSTC work plan and subgroup activities will be added as an agenda item in September. The RSTC will form a team to collaborate with the RISC to prioritize identified risks and develop RSTC subgroup work plan items for review and approval by the full RSTC at the December 2021 meeting. This will enhance full RSTC participation in work plan prioritization. The combined subgroup work plan is posted on the RSTC web site and a link is included in each RSTC meeting agenda The RSTC concurs that improving relationships and collaboration with other industry groups would be beneficial and an efficient means to address risks to the grid. We currently have quarterly reports to the RSTC from the NAGF and NATF for awareness. The Facility Ratings Task Force held a meeting with NATF regarding potential collaboration on their work plan. Several subgroups within the RSTC structure have participants from National labs. These include the security subgroups as well as groups working on inverter-based resource and DER issues. The groups also collaborate with Regional Entity experts.**

- Areas for continued focus as the committee matures include prioritization of work, and working efficiently and effectively within the wider NERC ecosystem.
- EEI encourages the Reliability Issues Steering Committee (RISC) and RSTC to continue their coordination which helps focus and prioritize RSTC activities.
- Consistent with the RSTC charter, the full RSTC membership should lead efforts for prioritizing and mitigating identified risks to ensure transparency and that the mission of the committee is met. Discussion on these issues by the entire membership will permit all viewpoints to be taken into consideration.
- EEI recommends the RSTC Work Product Notional Process be revised to align with the RSTC charter to ensure clarity with respect to roles and expectations.
- NPCC supports the strategic direction the RSTC is taking to achieve the objectives of its transition in accordance with 2019 ERO Risk Priorities Report key reliability risk profiles: Grid Transformation, Extreme Natural Events, Cyber and Physical Security Risks, and Critical Infrastructure Interdependencies.
- NPCC recommends that the RSTC further leverage the diversity within the expanding industry stakeholder community and Regional Entity expertise to support strategic level activities that advance the reliability, security and resilience risk mitigation activities critical to achieving the maintenance of a highly reliable North American bulk power system.
- The Cooperative Sector suggests that improving relationships with technical partners such as the Transmission & Generation Forums, EPRI, CEATI, and national labs to leverage would leverage expertise to provide additional exposure to security and reliability challenges facing the electric utility industry.
- For 2021 the RSTC needs to further engage the subgroups in support of the bottoms-up approach envisioned in the RSTC Charter.
- The RSTC has made significant structural improvements in its initial year. Despite the improvements, the committee's engagement (collaboration and coordination) has been limited by the pandemic and the virtual meeting format. Consequently, it is premature to provide an in-depth assessment of the RSTC.

<u>Stakeholder Engagement and RSTC meetings</u> – Many who provide Policy Input expressed concerns with improving stakeholder engagement and RSTC meeting agendas and meeting length. It was noted by several that the RSTC agendas have been very full and this prevented a more robust discussion of agenda items. In an effort to improve on stakeholder engagement, the RSTC will undertake two initiatives. First, we will have pre-meeting informational sessions prior to RSTC regular quarterly meetings beginning on August 24, 2021 for RSTC members to provide input on concerns or issues with agenda items prior to the actual RSTC meeting. In addition, beginning with the September 2021 meeting, we will expand the meeting time by 2 hours each day. The meeting will begin at 11 a.m. eastern each day and will include a short break for lunch. This will allow for more robust discussion of agenda items and better stakeholder engagement. The September meeting will remain as a virtual meeting while we are still evaluating whether the December meeting will be virtual or a hybrid of in-person and virtual. For 2022 and beyond, we will likely plan in-person RSTC meetings and anticipate enhancing RSTC meeting participation by having virtual participation available to stakeholders.

- NERC should continue to examine how to ensure optimal stakeholder engagement with NERC activities, especially given constrained resources and given the need to ensure the right expertise is represented on appropriate NERC committees.

- With the myriad activities underway by the various subgroups, EEI supports RSTC engagements that ensure there is meaningful opportunity for fulsome discussions by the membership.
- The Cooperative Sector suggests sponsoring group meetings like the MRC Pre- Meeting Informational sessions before or after RSTC meetings to discuss timely industry topics or future actionable items.
- Because of the volume of agenda items, the RSTC members and industry observers may not be providing enough feedback on the highest priority issues. To address this concern there should be consideration of whether to focus RSTC activities to limited number of designated priorities.
- The Cooperative Sector recommends that after the pandemic, all quarterly RSTC meetings should be in-person with an option for virtual participation by non-committee members with Non-committee members allotted a structured opportunity to provide input.
- Once we have reached the post- pandemic time frame, meetings should be in person with the option for participants to participate virtually since it helps increase attendance/participation.
- The current virtual format of two half day sessions may not be adequate to give the topics due consideration and discussion. Perhaps a half day followed by a full day is more appropriate for virtual-only meetings.

Sponsors and RSTC subgroup Coordination – Policy input was received regarding the implementation of Sponsors for RSTC subgroups and a suggestion was made to assign a Sponsor to each subgroup. Initially, the RSTC assigned 12 Sponsors to high priority subgroups. Over the course of time since then, we have assigned additional Sponsors for each subgroup that reports directly to the RSTC. Working Groups and Task Forces that report to a Subcommittee were not assigned Sponsors as we envision the Subcommittee Sponsor coordinating with the subgroups reporting to that Subcommittee. Each Working Group or Task Force in the Risk Mitigation Focus area now has a Sponsor. Effective collaboration between sponsors in each Focus Area will ensure that work items and activities are aligned and completed efficiently and effectively.

- EEI recommends that all subgroups and task forces under the RSTC have an RSTC sponsor to ensure:
    - Coordination and communications between the RSTC and its subgroups; and
    - The Framework to Address Known and Emerging Reliability and Security Risks is followed.

Additional Opportunities - Inverter-based Resources and Distributed Energy Resources – Policy Input was received regarding integration of intermittent resources and the development of SARs, guidance and technical documents to improve the reliability of such integrations. It was also noted that there are a number of state and provincial efforts to decarbonize and this will have an impact on the reliability of the grid. The RSTC will continue to work with industry to address Inverter-based Resources for operations, planning and security through the work of the IRPWG. The RSTC will continue to work with industry to address DER integration for operations planning and security through the SPIDER WG and the Energy Assessment Reliability Task Force. These RSTC subgroups will need to collaborate with Regional Entity and Provincial governments to ensure that government mandates are included in reliability assessments and to ensure that reliability and resilience are maintained.

- NPCC observes as the industry moves forward with grid transformation and the reliable integration of intermittent resources and new technologies there are additional opportunities for the RSTC and its subcommittees, in conjunction with the Reliability Issues Steering Committee, to further enhance Standards Authorization Requests (SARs), guidance documents, and technical whitepapers.
- NPCC recommends the RSTC address the reliable integration of the resources (e.g., offshore wind) and programs (e.g. electric vehicle goals) currently being mandated by numerous states and provinces for achieving their respective societal decarbonization goals.

Miscellaneous

- EEI recommends that the group selected for addressing the February 2021 Board resolution concerning the need "to expeditiously complete a broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities" be formed in cooperation with the RSTC and that the RSTC identify a RSTC sponsor.
- The Cooperative sector believes the RSTC needs to transition from a "tactical" to a "strategic" review and prioritization of RSTC work plan.
- To maintain efficiency the RSTC should remain a technical and tactical committee.

RSTC Proposed Charter Amendments

Action

Review

Attachment 1: REDLINE – RSTC Charter

Attachment 2: CLEAN – RSTC Charter

Background

In November 2021, the NERC Board of Trustees (Board) approved the creation of the RSTC to replace the former Operating, Planning and Critical Infrastructure Protection committees to improve the effectiveness and efficiency of those standing committees. In accordance with Article VII of the NERC Bylaws and Section 1301 of the NERC Rules of Procedure, the Board may appoint standing committees, by resolution, as the NERC Board deems necessary to carry out its purposes. Standing committees must be representative of members, other interested parties and the public. They must also provide for balanced decision-making as well as participation of persons with technical knowledge and experience.

Charter of the RSTC

The NERC Board shall also approve the charter of a standing committee and assign specific authority to conduct business within that charter. RSTC has been operating under its charter for almost two years. NERC proposes the following amendments to the RSTC charter to further enhance the efficiency of the RSTC's operations and provide greater clarity.

Below is an overview of the proposed changes to the RSTC charter:

Purpose (Section 1)

- NERC proposes to incorporate a third objective of the RSTC to emphasize Committee oversight on how its subgroups implement their work plans and develop risk-mitigating technical solutions.

Functions (Section 2)

- The current charter contains no reference to an RSTC work plan. NERC proposes to establish an RSTC strategic work plan which will be separate from the subgroups' work plans. The strategic work plan will be developed every two years and will align with ERO objectives outlined in other strategic reports such as the business plan and budget, reliability assessments and the State of Reliability report. It will also be socialized with other standing committee work plans through the Standing Committee Coordinating Group.
- NERC proposes that the current, quarterly RSTC updates to the Board will be replaced with semi-annual updates on the strategic work plan. The RSTC would also submit this strategic work plan to the NERC Board on an annual basis for approval.

Membership (Section 3)

- NERC adds a footnote to explain that the new Sector 13 membership group is represented by the at-large representatives on the RSTC.
- NERC clarifies that it is not NERC membership is not a prerequisite to serve as an RSTC member.
- NERC proposes to streamline the process for resolving affiliate conflicts amongst members by calling for the Nominating Subcommittee to make a recommendation to the NERC board to make a final decision if the impacted members cannot resolve the matter.
- NERC clarifies that during an annual election, if a sector seat cannot be filled and it is converted to an at-large seat, the converted at-large seat will revert back to a sector seat at the end of the term.
- NERC proposes that members of the Executive Committee, aside from the Vice-Chair not serve on the Nominating Subcommittee.
- NERC includes an additional Nominating Subcommittee seat and provides that at-large members shall recuse themselves from recommendations for at-large representative seats if they are seeking reappointment.
- NERC aligns the charter with the NERC Bylaws in noting that the RSTC Vice-Chair does not need to recuse him or herself from the Nominating Subcommittee so long as he or she is not seeking re-election.
- NERC clarifies that international representation on the RSTC will be consistent with the NERC Bylaws.
- NERC identifies a few criteria that the RSTC Nominating Subcommittee can balance in the selection of at-large members. These criteria are borrowed from the Compliance and Certification Committee charter to select at-large members.

Meetings (Section 4)

- NERC clarifies that the RSTC may consult Robert's Rules of Order for open meetings if the charter does not provide the needed guidance.
- NERC proposes that quorum be established once at each meeting and not prior to each vote to emphasize the need for Committee members to participate throughout a meeting, regardless of the format of the meeting. NERC also proposes to grant the Chair sole discretion to allow discussion of agenda items in the absence of quorum.
- NERC proposes to change the requirement for approval of an action item by the RSTC from 2/3 votes "present" to 2/3 votes "cast." This change enables the RSTC to exclude abstentions (i.e., those members in attendance, but who either chose not to vote or stepped away and did not vote) from the approval calculation. This approach encourages membership to be proactive in getting the required clarity to approve or fail an agenda item.
- NERC also notes that voting procedures are not impacted by the format of the meeting.

- NERC proposes that the RSTC can host three types of sessions: executive, open, and closed. Executive sessions and meetings of the Nominating Subcommittee are closed. The Chair may also hold other closed sessions in advance of open meetings with limited attendance, similar to the NERC Board committees. Attendance at such closed sessions will be determined on a non-discriminatory basis and to the extent that Confidential Information is discussion, Section 1500 of the NERC Rules of Procedure will apply. NERC adds that examples of a closed meeting are a meeting with subgroup sponsors or with members of a subgroup.
- NERC also confirms that only members can vote during open meetings.
- NERC memorializes that any actions taken by the Executive Committee will be announced at the open meetings and included in the minutes of the open meetings.
- In the Chair's proposed semi-annual update to the Board on the progress made in executing the RSTC's strategic work plan, the Chair will capture any challenges that the committee is facing; however, the Board will not be presented with results of votes on actions.

Subordinate Groups (Section 6)

- NERC proposes that the RSTC will update the NERC Board on its strategic work plan rather than on the specific works plans of its subgroups.
- The chair of any subgroup will be consistently selected by the RSTC Chair.

Meeting Procedures (Section 7)

- NERC proposes to change the default procedure for voting from a voice vote to polling consistent with the future hybrid meeting format which includes potential virtual attendance.

RSTC Deliverables and Approval Processes (Section 8)

- NERC memorializes standard authorization requests as a deliverable of the RSTC subgroups.
- NERC clarifies that in the definition of SAR deliverables endorsed by the RSTC, the Standards Committee can remand a SAR to the RSTC, but not on grounds of the technical justification. This is consistent with the NERC Rules of Procedure.

Meeting Governance (Section 9)

- NERC proposes a list of motions to guide actions during open meetings. This guidance aligns with the Standards Committee.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability and Security Technical Committee Charter

November ~~2019~~2021

Approved by the NERC Board of Trustees: XX XX, ~~2019~~2021

RELIABILITY | RESILIENCE | SECURITY




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

Table of Contents

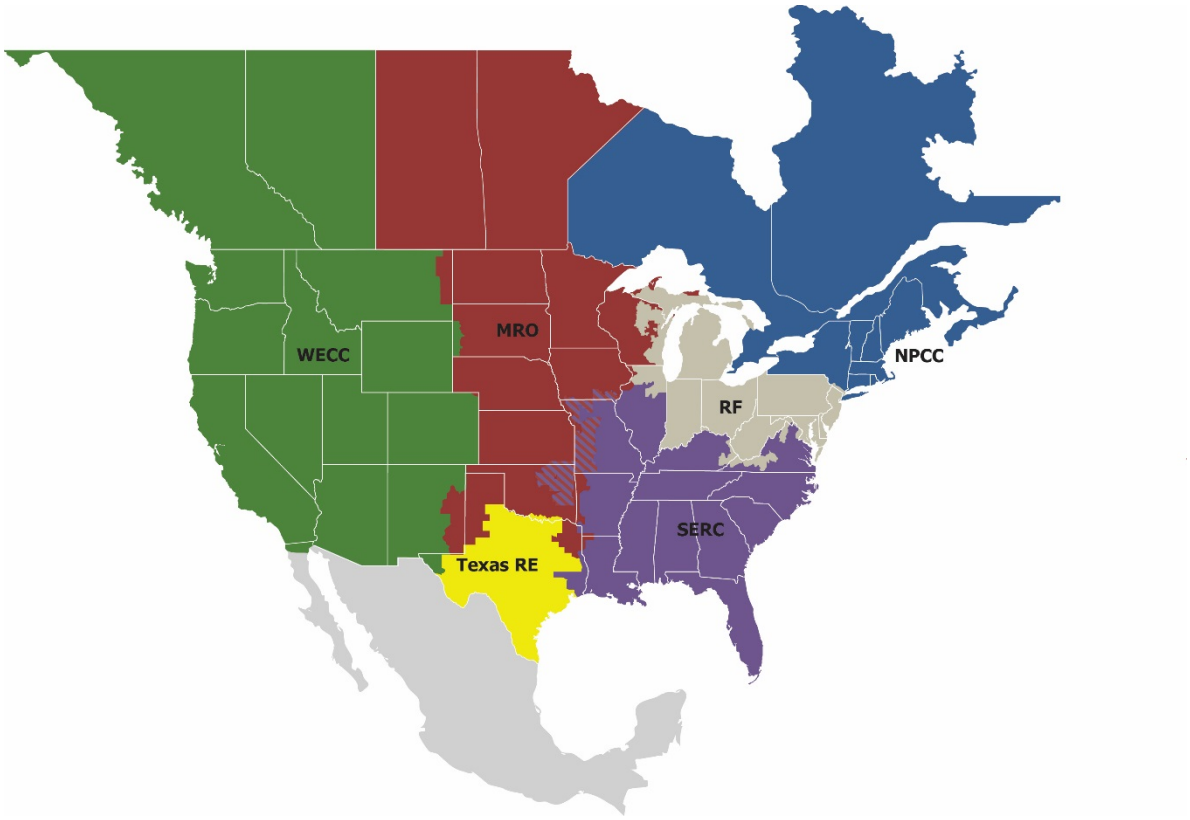
Preface

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 divided into six ~~RE~~ Regional Entities' boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



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

Section 1: Purpose

The Reliability and Security Technical Committee (RSTC) is a standing committee that strives to advance the reliability and security of the interconnected BPS of North America by:

- Creating a forum for aggregating ideas and interests, drawing from diverse industry stakeholder expertise, to support the ERO Enterprise's mission; ~~and,~~
- Leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks to the BPS for the benefit of industry stakeholders, the NERC Board of Trustees (Board) and ERO Enterprise staff and leadership~~.~~; and,
- Overseeing the implementation of subgroup work plans that drive risk-mitigating technical solutions.

Section 2: RSTC Functions

Create a forum for industry stakeholders to support NERC programs in the development of key ERO Enterprise deliverables.

- Facilitate and advocate information sharing among relevant industry stakeholders;
- Review and provide guidance in developing deliverables critical to ERO functions, such as Reliability Standards, reliability assessments, requests for data (pursuant to Section 1600 of the NERC Rules of Procedure Section (ROP)), Implementation Guidance, and other analyses, guidelines, and reports;
- Solicit and coordinate technical direction, oversight activities, and feedback from industry stakeholders;
- Disseminate ERO deliverables to industry to enhance reliability;
- Develop internal and review external requests for industry actions and informational responses;
- Develop appropriate materials, as directed by ERO functions or the NERC Board, to support ERO Enterprise functions; and,
- Coordinate with ERO staff and liaise with government agencies and trade associations.
- Provide technical input and analyses on operating and planned BPS reliability and security, emerging issues and risks, and other general industry concerns at the request of the NERC Board or NERC staff.

Develop a ~~rolling,~~two-year strategic work plan to guide the deliverables of the RSTC ~~subgroups~~.

- Ensure alignment of the strategic work plan with ERO reports and analyses, including the NERC Business Plan and Budget, ERO Enterprise Long-Term Strategy, Operating Plan, biennial Reliability Issues Steering Committee (RISC) ERO Reliability Risk Priorities report, State of Reliability report recommendations, Long-Term, Seasonal and Special Reliability Assessment recommendations and ongoing event~~s~~ analysis trends;
- Coordinate the objectives in the strategic work plan with the Standing Committees Coordinating Group; and,
- Obtain annual NERC Board approval.

Coordinate and oversee implementation of RSTC subgroup work plans.

- Create and disband subcommittees, working groups and task forces to support ERO Enterprise functions;
- Harmonize and approve the work plans of subcommittees, working groups, and task forces ~~to ensure alignment with strategic reports and analyses, such as the Business Plan and Budget, ERO Enterprise Long-Term Strategy, Operating Plan, biennial RISC report, State of Reliability report recommendations, Long-Term, Seasonal and Special Reliability Assessment recommendations and ongoing events analysis trends; and,~~with the strategic work plan; and,
- Track the progress of the subcommittees, working groups, and task forces to ensure that they complete assigned activities ~~in implementing~~as outlined in their work plans.

Advise the NERC Board of Trustees.

- ~~Approve, accept, remand or endorse[1] ERO processes, analyses, reports, and other~~Update the NERC Board semi-annually on progress in executing the strategic work plan; and
- Present appropriate deliverables ~~for~~to the NERC Board~~; and,~~.

[1] ~~See Section 8 for further details on these actions.~~

- ~~Provide technical input and analyses on operating and planned BPS reliability and security, emerging issues and risks, and other general industry concerns at the request of the NERC Board or NERC staff.~~

Section 3: Membership

Representation Model

The RSTC has a hybrid representation model consisting of the following types of memberships:

- Sector members;
- At-large members; and,
- Non-voting members.

Two members shall be elected to each of the following membership sectors:

- Sector 1 - Investor-owned Utility;
- Sector 2 ~~–~~ State or ~~/~~Municipal Utility;
- Sector 3 - Cooperative Utility;
- Sector 4 - Federal or Provincial Utility/Power Marketing Administration;
- Sector 5 - Transmission-~~dependent~~Dependent Utility;
- Sector 6 - Merchant Electricity Generator;
- Sector 7 - Electricity Marketer;
- Sector 8 - Large End Use Electricity Customer;
- Sector 9 - Small End Use Electricity Customer;
- Sector 10 - ISO/RTO; and,
- Sector 12 - Government Representatives.

Selection of at-large members will allow for better balancing of representation on the RSTC of the following:[2]

- Regional Entity and Interconnection diversity (i.e., goal of having at least one representative from each Interconnection and Regional Entity footprint);
- Subject matter expertise (Planning, Operating, or Security);
- Organizational types (Cooperatives, Investor-Owned Utilities, Public Power, Power Marketing Agencies, etc.); and,
- North American countries, consistent with the NERC bylaws (Canada, Mexico, and U.S.).

Below is a breakdown of voting and non-voting membership on the RSTC:

Voting Membership	
Name	**Voting Members**
Sectors 1-10 and 12	22
At-Large	10
Chair and Vice Chair	2
Total	**34**

[2] *See,* NERC Sector 13 in the NERC Bylaws (2021).

Non-Voting Membership[3]	
Non-Voting Member	**Number of Members**
NERC Secretary	1
United States Federal Government	2
Canadian Federal Government	1
Provincial Government	1
Total	**5**

Member Selection

~~It is expected that~~ RSTC members will be from organizations who are NERC members, but it is not required.

Members are appointed to the RSTC upon approval of the NERC Board and serve on the RSTC at the pleasure of the NERC Board.

1. **Affiliates**

   A company, including its affiliates, may not have more than one member on the RSTC. Any RSTC member who is aware of a membership conflict of this nature is obligated to notify the RSTC secretary within 10 business days. The RSTC secretary will in turn report the conflict to the RSTC chair.

   Members impacted by such a conflict, such as through a merger of organizations, ~~may~~must confer among themselves to determine which member should resign from the RSTC and notify the secretary and chair; however, if they ~~are within the same industry sector and~~ cannot reach an amicable solution to determine who will remain, the Nominating Subcommittee~~Eexecutive Ccommittee~~ will review the qualifications of each member and make a recommendation to the NERC Board for final approval.~~The RSTC will determine which member shall continue to serve, subject to NERC Board approval~~final decision~~.~~

   ~~If the conflict is not resolved in a timely manner by the impacted members, the chair shall notify all members of the affected industry sectors and recommend actions to resolve the conflict. If the membership conflict remains unresolved, the chair shall refer the conflict to the NERC Board for resolution.~~

2. **Election of Sector Members**

   NERC members in each sector will annually elect members for expiring terms or open seats using a nomination and election process that is open, inclusive, and fair. In the event that a sector has no nominations for one or both sector seats at the annual election, the RSTC will ~~must first~~will ~~attempt to fill~~convert those empty sector ~~positions with~~seats to at-large ~~members. Otherwise, the sector seat will remain vacant~~seats until the ~~next annual election~~end of the term.

   Sector elections will be completed in time for the Nominating Subcommittee to identify and nominate at-large representatives as well as for the secretary to send the full RSTC membership list to the NERC Board for ~~its~~ approval at ~~the~~ its annual February meeting.

   ~~After the secretary announces the election results, newly elected members will serve on the RSTC pending approval by the Board.~~

   If an interim vacancy is created in a sector, a special election will be held unless it would coincide with the annual election process. If a sector cannot fill an interim vacancy, then that sector seat will remain vacant until the next annual election. Interim sector vacancies will not be filled with an at-large representative.

[3] Upon recognition of NERC as the Electric Reliability Organization, Mexican Government representation will be equitable and based approximately on proportionate Net Energy for Load.

3. Nominating Subcommittee

The Nominating Subcommittee (RSTC NS) will consist of six~~five~~ members (the RSTC Vice-Chair and five~~our~~ members drawing from different sectors and at-large representatives). Apart from the Vice-Chair, members of the RSTC EC shall not serve on the RSTC NS.

The ~~Nominating Subcommittee~~NS members are nominated by the RSTC chair and ~~approved~~voted on by the full RSTC membership.

The term for members of the ~~Nominating Subcommittee~~NS is two years.

~~In addition to~~The RSTC NS is responsible for (a) recommending individuals for at-large representative seats, ~~the Nominating Subcommittee manages~~and, (b) managing the process to select the chair and/or vice chair of the RSTC. The RSTC vice-chair shall recuse him or herself from this process unless he or she is not seeking re-election. At-large members on the RSTC NS shall recuse themselves from recommendations for at-large representative seats if they are seeking reappointment.

4. Selection of At-Large Members

The RSTC NS solicits and reviews nominations from the full RSTC and industry to fill at-large representative seats. ~~The~~After reaching consensus, the ~~Nominating Subcommittee~~ RSTC NS ~~recommends~~ submits a recommended slate of at-large candidates ~~individuals to fill at-large representative seats on the RSTC, following consultation of.~~to the Board at its annual February meeting for approval. To the extent practicable, the RSTC NS will balance the following criteria to select at-large members: (a) geographic diversity from all Interconnections and ERO Enterprise Regional Entities; (b) high-level understanding and perspective on reliability risks based on experience at an organization in a sector; and, (c) experience and expertise from an organization in the sector relevant to the RSTC.

The Board votes to appoint the ~~full RSTC~~at-large members.~~—~~

5. Non-Voting Members

At the start of the annual RSTC nomination process ~~and prior to voting by the full RSTC,~~ the RSTC secretary will coordinate with entities entitled to non-voting membership to identify representatives for the non-voting seats~~. If a non-voting seat cannot be filled, then it will remain vacant until the next annual election.~~

6. International Representation

~~Canadian~~International representation on the RSTC shall be consistent with Article VIII Section 4 of the NERC Bylaws.

Member Expectations

RSTC members are expected to act in accordance with this charter, ~~-~~as well as to accomplish the following:

- Adhere to NERC Antitrust Guidelines and Participant Conduct Policy;
- Demonstrate and provide knowledge and expertise in support of RSTC activities;
- Where applicable, solicit comments and opinions from constituents and groups of constituents or trade organizations represented by the member and convey them to the RSTC;
- Respond promptly to all RSTC requests, including requests for reviews, comments, and votes on issues before the RSTC; and,

- During meetings, ~~C~~comply with the procedures outlined ~~during meetings~~for that meeting and identified in this Charter ~~and Robert's Rules of Order~~(see **Section 9**) ~~during meetings~~.

Term

~~Upon the initial establishment of the RSTC, one half of members will serve for two year terms (with terms ending in even years) and the remaining half will serve for three year terms (with terms ending in odd years).~~

When the initial ~~terms~~ staggered, two- and three-year terms of RSTC members ~~are complete~~have expired~~, (2022 and 2023)~~, all subsequent terms will ~~have a standard length of~~be two years ~~to ensure staggered membership~~.

~~Terms~~An RSTC member may serve a term shorter than two years ~~may be required for several reasons~~if:

- ~~If T~~two members are simultaneously selected to a sector that did not have any existing members, in order to stagger their terms, one member will be assigned a one-year term and the second member will be assigned a two-year term.
- ~~If a~~ A member is selected to fill a vacant member ~~position~~seat~~s~~ between elections, the term will end when the term for that vacant ~~position~~seat~~s~~ ends.

There are no limits on the number of terms that members can serve.

Vacancies and Proxies

~~Any membership~~Membership vacancies may be filled between annual elections using the aforementioned selection process.

1. **Vacancies Created By the Member**

   In the event a member can no longer serve on the RSTC, that member will submit a written resignation to the RSTC chair or the secretary.

2. **Vacancies Requested by the Chair**

   The chair may request any RSTC member who ceases to participate in the RSTC consistent with member expectations (above) and to the satisfaction of the chair, to submit a resignation or to request continuation of membership with an explanation of extenuating circumstances. If a written response is not received within 30 days of the chair's request, the lack of response will be considered a resignation. If the chair is not satisfied with a written response, the RSTC chair will refer the matter to the NERC Board.

3. **Vacancies Requested By the Board**

   RSTC members serve at the pleasure of the NERC Board. The NERC Board may initiate a request for resignation, removal, or replacement a member from the RSTC, as it deems appropriate or at the request of the RSTC chair.

4. **Proxies**

   A voting member may select a proxy who attends and votes during all or a portion of a committee meeting in lieu of a voting member, provided that the absent voting representatives notifies the RSTC chair, vice chair, or secretary of the proxy. A proxy may not be given to another RSTC member. A proxy must meet the RSTC's membership eligibility requirements, including affiliate restrictions.

   To permit time to determine a proxy's eligibility, all proxies must be submitted to the secretary in writing at least one week prior to the meeting (electronic transmittal is acceptable) for approval by the chair. Any proxy submitted after that time will be accepted at the chair's discretion.

Section 4: Meetings

Open meetings will be conducted in accordance with governance procedures in **Section 9**. ~~In the absence of specific provisions in this charter, all committee meetings will follow Roberts Rules of Order~~The Chair may ~~follow~~consult Robert's Rules of Order ~~for open committee meetings. See~~for additional guidance. ~~**Section 9** for additional governance procedures used during open meetings of the committee~~.

Quorum

The quorum necessary for transacting business at meetings of the RSTC is two-thirds of the voting members currently on the RSTC's roster and is determined once at each meeting.

If a quorum is not ~~present at the time of the vote~~determined, the RSTC may not take any actions requiring a vote; however, the chair may~~, with the consent of the majority of voting members present, elect to~~ allow discussion of the agenda items.

Voting

Actions by the RSTC will be approved upon receipt of the affirmative vote of two-thirds of the votes ~~present~~cast at any meeting at which a quorum is present. An abstention ("present" vote) does not count as a vote cast.

Voting may take place during regularly scheduled in-person/hybrid meetings~~-~~ with some attendance virtual ~~or may take place,~~ via electronic mail, or via conference call/virtual meeting.

Executive, Open ~~Meetings~~and Closed Sessions

The RSTC holds meetings ~~will be~~ open to the public, except as noted ~~below under Confidential Information~~herein. Although meetings are open, only voting members may offer and act on motions.

~~Confidential Sessions~~

~~At~~The chair may hold closed sessions with the ~~discretion~~eExecutive ~~c~~Committee.

The chair may also hold closed sessions in advance of the ~~chair, a~~open meeting ~~or portion of an RSTC meeting may have~~ with limited attendance (e.g., with sponsors and/or members of subgroups) ~~limited based on confidentiality of the information to be disclosed at the meeting. Such limitations should be~~ applied sparingly ~~—~~and on a non-discriminatory basis. ~~Confidential Information will only be disclosed as provided by~~ Any discussion of confidential information in a closed session shall be consistent with Section 1500 of the NERC ROP.

All meetings of the RSTC NS shall be conducted in closed session.

Majority and Minority Views

All members of a committee will be given the opportunity to provide alternative views on an issue. The results of committee actions, including recorded minutes, will reflect the majority as well as any minority views of the committee members. ~~The chair will communicate both the majority and any minority views in presenting results to the NERC Board.~~

Action without a Meeting

Any action required or permitted at a meeting of the committee may be taken without a meeting at the request of the chair.

Such action without a meeting will be performed by ~~mail or~~ electronic ballot (e.g., telephone, email, or Internet survey) ~~and will be recorded in the minutes as~~ and considered a roll call ballot. The secretary will announce the action required at least five business days before the date on which voting commences. As time permits, members should be allowed a window of 10 business days to vote. The secretary will document the results of such an action within 10 business days of the close of the voting period. Such action must meet the regular meeting quorum and voting requirements above.

Section 5: Officers and Executive Committee

Officers

The RSTC will have two officers – one chair and one vice-chair.

Officers shall be selected as follows:

- The ~~Nominating Subcommittee~~NS solicits nominations for chair and vice-chair through an open nomination process. Self-nominations are permitted during the open nomination period.
- ~~The Nominating Subcommittee proposes~~At the close of the nomination period, the NS will propose a chair and a vice-chair ~~candidates~~candidate. The full RSTC will elect the chair and vice chair.
- The chair and vice chair must be a committee member and shall not be from the same sector ~~and may be an at-large member~~.
- The elected chair and vice-chair are ~~approved~~appointed by the NERC Board.
- ~~Unless an exception is approved by the Board, no~~No individual may serve more than one term as vice chair and one term as chair unless an exception is approved by the Board.

Secretary

NERC will appoint the RSTC secretary.

A member of the NERC staff will serve as the secretary of the RSTC. The secretary will do the following:

- Manage the day-to-day operations and business of the RSTC;
- Prepare and distribute notices of the RSTC meetings, prepare the meeting agenda, and prepare and distribute the minutes of the RSTC meetings;
- Facilitate the election/selection process for RSTC members; and,
- Act as the RSTC's parliamentarian.

Chair

The chair will direct and provide general supervision of RSTC activities, including the following:

- Coordinate the scheduling of all meetings, including approval of meeting duration and location;
- Develop agendas and rule on any deviation, addition, or deletion from a published agenda;
- Preside at and manage meetings, including the nature and length of discussion, recognition of speakers and proxies, motions, and voting;
- Act as spokesperson for the RSTC at forums inside and outside of NERC; and,
- Attend meetings of the NERC Board when necessary to report on RSTC activities.

Vice Chair

The vice chair will assume the responsibilities of the chair under the following conditions:

- At the discretion of the chair (for brief periods of time);
- When the chair is absent or temporarily unable to perform the chair's duties; or,

- When the chair is permanently unavailable or unable to perform the chair's duties. In the case of a permanent change, the vice chair will continue to serve until a new chair is nominated and appointed by the NERC Board.

Executive Committee

The ~~RSTC will select an e~~Executive ~~c~~Committee (RSTC EC) shall consist of six members ~~as follows~~:

- Chair;
- Vice-chair;
- Four RSTC voting members selected by the RSTC chair and vice-chair with a reasonable balance of subject matter expertise in Operations, Planning, and/or Security and with consideration for diversity in representation (i.e., sectors, Regional Entities, Interconnections, etc.).

The EC~~executive committee~~ of the RSTC is authorized by the RSTC to act on its behalf between regular meetings on matters where urgent actions are crucial and full RSTC discussions are not practical. Actions taken by the ~~executive committee~~EC shall be announced at the open meetings and included in the minutes of the open meetings.

Ultimate RSTC responsibility resides with its full membership whose decisions cannot be overturned by the EC~~executive committee, and which~~. The RSTC retains the authority to ratify, modify, or annul RSTC EC~~executive committee~~ actions.

Section 6: RSTC Subordinate Groups

The RSTC organizational structure will be aligned as described by the NERC Bylaws to support a superior-subordinate hierarchy.

The RSTC may establish subcommittees, working groups, and task forces as necessary. The RSTC will be the responsible sponsor of all subordinate subcommittees, working groups, or task forces that it creates, or that its subordinate subcommittees and working groups may establish. ~~The RSTC will keep the NERC Board informed of all groups subordinate to the RSTC.~~

Officers of subordinate groups will be appointed by the chair of the RSTC.

Subcommittees, working groups, and taskforces will conduct business in a manner consistent with all applicable sections of this ~~manual and Robert's Rules of Order~~Charter.

Subcommittees

The RSTC may establish subcommittees to which the RSTC may delegate some of RSTC's functions. The RSTC will approve the scope of each subcommittee it forms. The RSTC chair will appoint the subcommittee officers (typically a chair and a vice chair) for a specific term (generally two years). The subcommittee officers may be reappointed for up to two additional terms. The subcommittee will work within its assigned scope and be accountable for the responsibilities assigned to it by the committee. The formation of a subcommittee, due to the permanency of the subcommittee, will be approved by the NERC Board.

Working Groups

The RSTC may delegate specific continuing functions to a working group. The RSTC will approve the scope of each working group that it forms. The RSTC ~~or subcommittee~~chair will appoint the working group officers (typically a chair and a vice chair) for a specific term (generally two years). The working group officers may be reappointed for one additional term. The RSTC will conduct a "sunset" review of each working group every year. The working group will be accountable for the responsibilities assigned to it by the RSTC or subcommittee and will, at all times, work within its assigned scope. The RSTC should consider promoting to a subcommittee any working group that is required to work longer than one term.

Task Forces

The RSTC may assign specific work to a task force. The RSTC will approve the scope of each task force it forms. The RSTC chair ~~of the RSTC~~ will appoint the task force officers (typically a chair and a vice chair). Each task force will have a finite duration, normally less than one year. The RSTC will review the task force scope at the end of the expected duration and at each subsequent meeting of the RSTC until the task force is retired. Action of the RSTC is required to continue the task force past its defined duration. The RSTC should consider promoting to a working group any task force that is required to work longer than one year.

Section 7: Meeting Procedures

Voting Procedures for Motions

- ~~The default procedure is a voice vote.~~
- ~~If the chair believes the voice vote is not conclusive, the chair may call for a show of hands.~~
- ~~The chair will not specifically ask those who are abstaining to identify themselves when voting by voice or a show of hands.~~All voting shall default to being conducted through use of a poll unless a need to record each member's vote is identified or requested. Where a need to record each member's vote is requested or identified, the RSTC may conduct voting via a roll call vote.

~~All voting will be conducted through a poll.~~

-
- ~~The committee may conduct a roll-call vote in those situations that need a record of each member's vote.~~
- The committee must approve conducting a roll call vote for the motion.
- For roll call votes, ~~T~~the secretary will call each member's name.
- Members answer "yes," or "no," but may answer "present" if they wish to abstain from voting. As provided above, an abstention does not count as a vote cast.

Minutes

- Meeting minutes are a record of what the committee did, not what its members said.
- Minutes should list discussion points where appropriate, but should usually not attribute comments to individuals. It is acceptable to cite the chair's directions, summaries, and assignments.
- ~~Do not list the person who seconds a motion.~~
- ~~Do not record (or even ask for) abstentions.~~
- All Committee members are afforded the opportunity to provide alternative views on an issue. The meeting minutes will provide an exhibit to record minority positions. ~~The chair shall report both the majority and any minority positions in presenting results to the NERC Board.~~
-

Section 8: RSTC Deliverables and Approval Processes

The RSTC will abide by the following parameters regarding approval, endorsement, or acceptance of committee deliverables.

Reliability Guidelines, Security Guidelines and Reference Documents ~~Reliability Guidelines~~

Reliability Guidelines and Security Guidelines are documents that suggest approaches or behavior in a given technical area for the purpose of improving reliability. Reliability Guidelines and Security Guidelines are not binding norms or mandatory requirements. Reliability Guidelines and Security Guidelines may be adopted by a responsible entity in accordance with its own facts and circumstances.

1. **New/updated draft guideline approved for industry posting.**

   The RSTC approves for posting for industry comment the release of a new or updated draft guideline developed by one of its subgroups or the committee as a whole.

   The draft guideline is posted as "for industry-wide comment" for 45 days. If the draft guideline is an update, a redline version against the previous version must also be posted.

   After the public comment period, the RSTC will post the comments received as well as its responses to the comments. The RSTC may delegate the preparation of responses to a committee subgroup.

   A new or updated guideline which considers the comments received, is approved by the RSTC and posted as "Approved" on the NERC website. Updates must include a revision history and a redline version against the previous version.

   After posting a new or updated guideline, the RSTC will continue to accept comments from the industry via a web-based forum where commenters may post their comments.

   a. Each quarter, the RSTC will review the comments received.

   b. At any time, the RSTC may decide to update the guideline based on the comments received or on changes in the industry that necessitate an update.

   c. Updating an existing guideline will require that a draft updated guideline be approved by the RSTC in the above steps.

2. **Review of Approved Reliability Guidelines, Security Guidelines and Reference Documents**

   Approved Reliability Guidelines or Reference Document shall be reviewed for continued applicability by the RSTC at a minimum of every third year since the last revision.

3. **Communication of New/Revised Reliability Guidelines, Security Guidelines and Reference Documents**

   In an effort to ensure that industry remains informed of revisions to a Reliability Guideline or Reference Document or the creation of a new Reliability Guideline or Reference Document, the RSTC subcommittee responsible for the Reliability Guideline will follow an agreed upon process.

4. **Coordination with Standards Committee**

   Standards Committee authorization is required for a Reliability Guideline or Security Guidelines to become a supporting document that is posted with or referenced from a NERC Reliability Standard. See Appendix 3A in the NERC's ROP under "Supporting Document."

Section 1600 Data or Information Requests

A report requested by the RSTC that accompanies or recommends a Rules of Procedure (ROP) Section 1600 - Data or Information Request will follow the process outlined below:

1. This Section 1600 request, with draft supporting documentation, will be provided to the RSTC at a regular meeting.
2. The draft Section 1600 data request and supporting documentation will be considered for authorization to post for comments at the RSTC regular meeting.
3. A committee subgroup will review and develop responses to comments on the draft Section 1600 data request and will provide a final draft report, including all required documentation for the final data request, to the RSTC at a regular meeting for endorsement.
4. The final draft of the 1600 data request – with responses to all comments and any modifications made to the request based on these comments – will be provided to the NERC Board.

Other Types of Deliverables

1. **Policy Outreach**

   On an ongoing basis, the RSTC will coordinate with the forums, policymakers, and other entities to encourage those organizations to share reliability guidelines, reference documents and lessons learned to benefit the industry.

   Reports required under the NERC ROP or as directed by an Applicable Governmental Authority or the NERC Board: documents include NERC's long-term reliability assessment, special assessments, and probabilistic assessments. These reports may also be used as the technical basis for standards actions and can be part of informational filings to FERC or other government agencies.

2. **White Papers**

   Documents that explore technical facets of topics, often making recommendations for further action. They may be written by subcommittees, working groups, or task forces of their own volition, or at the request of the RSTC.

3. **Reference Documents and Technical Reports**

   Documents that serve as a reference for the electric utility industry and/or NERC stakeholders regarding a specific topic of interest. These deliverables are intended to document industry practices or technical concepts at the time of publication and may be updated as deemed necessary, per a recommendation by the RSTC or its subgroups to reflect current industry practices.

4. **Implementation Guidance**

   Documents providing examples or approaches for registered entities to comply with standard requirements. The RSTC is designated by the ERO Enterprise as a pre-qualified organization for vetting Implementation Guidance in accordance with NERC Board -approved Compliance Guidance Policy. Implementation Guidance that is endorsed by the RSTC can be submitted to the ERO Enterprise for endorsement, allowing for its use in Compliance Monitoring and Enforcement Program (CMEP) activities.

5. **Standard Authorization Requests (SAR)**

   A form used to document the scope and reliability benefit of a proposed project for one or more new or modified Reliability Standards or definitions or the benefit of retiring one or more approved Reliability Standards. RSTC endorsement of a SAR supports: (a) initial vetting of the technical material prior to the formal

Standards Development Process, and, (b) that sound technical justification material has been developed, and the SAR will not be remanded back to the RSTC to provide such justification per the Standard Processes Manual.

Review Process for other Deliverables

Deliverables with a deadline established by NERC management or the NERC Board will be developed based on a timeline reviewed by the RSTC to allow for an adequate review period, without compromising the desired report release dates. Due to the need for flexibility in the review and approval process, timelines are provided as guidelines to be followed by the committee and its subgroups.

A default review period of no less than 10 business days will be provided for all committee deliverables. Requests for exceptions may be brought to the RSTC at its regular meetings or to the RSTC EC~~Executive Committee~~ if the exception cannot wait for an RSTC meeting.

In all cases, a final report may be considered for approval, endorsement, or acceptance if the RSTC, as outlined above, decides to act sooner.

~~Possible~~ Actions for ~~other~~ Deliverables

1. **Approve:**

   The RSTC has reviewed the deliverable and supports the content and development process, including any recommendations.

2. **Accept:**

   The RSTC has reviewed the deliverable and supports the development process used to complete the deliverable.

3. **Remand:**

   The RSTC remands the deliverable to the originating subcommittee, refer it to another group, or direct other action by the RSTC or one of its subcommittees or groups.

4. **Endorse:**

   The RSTC agrees with the content of the document or action, and recommends the deliverable for the approving authority to act on. This includes deliverables that are provided to the RSTC by other NERC committees. RSTC endorsements will be made with recognition that the deliverable is subject to further modifications by NERC Executive Management and/or the NERC Board. Changes made to the deliverable subsequent to RSTC endorsement will be presented to the RSTC in a timely manner. If the RSTC does not agree with the deliverable or its recommendations, it may decline endorsement. It is recognized that this does not prevent an approval authority from further action.

Section 9: Meeting Governance

The RSTC will abide by the following procedures regarding taking actions on committee deliverables.

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and cannot reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	No	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." The vote is subject to a 2/3 majority approval. Also, any member may call the question. This motion is not debatable. The vote is subject to a 2/3 vote.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds

A Motion must have a second to ensure that at least two members wish to discuss the issue.

Announcement by the Chair.

The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to procedure in this Charter.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability and Security Technical Committee Charter

November 2021

Approved by the NERC Board of Trustees: XX XX, 2021

RELIABILITY | RESILIENCE | SECURITY




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

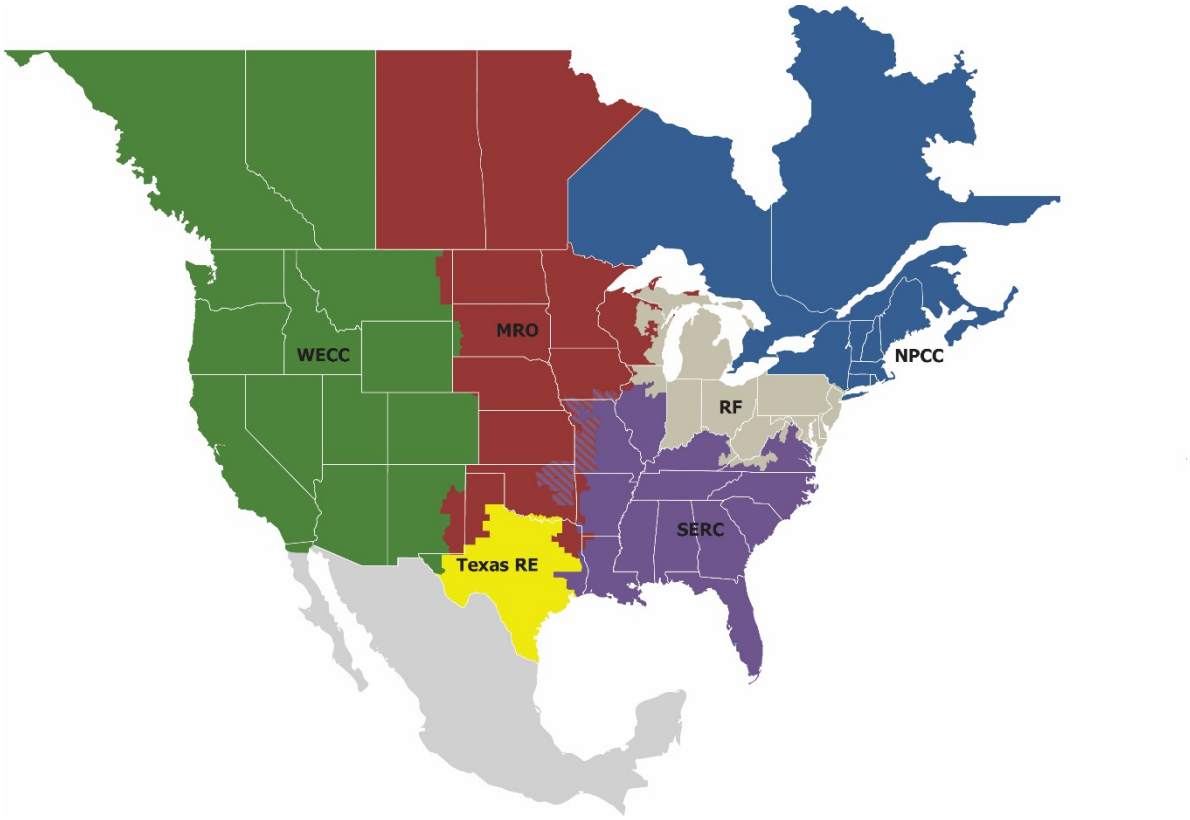
Table of Contents

Preface

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, 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 divided into six Regional Entities' boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



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

Section 1: Purpose

The Reliability and Security Technical Committee (RSTC) is a standing committee that strives to advance the reliability and security of the interconnected BPS of North America by:

- Creating a forum for aggregating ideas and interests, drawing from diverse industry stakeholder expertise, to support the ERO Enterprise's mission;
- Leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks to the BPS for the benefit of industry stakeholders, the NERC Board of Trustees (Board) and ERO Enterprise staff and leadership; and,
- Overseeing the implementation of subgroup work plans that drive risk-mitigating technical solutions.

Section 2: RSTC Functions

Create a forum for industry stakeholders to support NERC programs in the development of key ERO Enterprise deliverables.

- Facilitate and advocate information sharing among relevant industry stakeholders;
- Review and provide guidance in developing deliverables critical to ERO functions, such as Reliability Standards, reliability assessments, requests for data (pursuant to Section 1600 of the NERC Rules of Procedure Section (ROP)), Implementation Guidance, and other analyses, guidelines, and reports;
- Solicit and coordinate technical direction, oversight activities, and feedback from industry stakeholders;
- Disseminate ERO deliverables to industry to enhance reliability;
- Develop internal and review external requests for industry actions and informational responses;
- Develop appropriate materials, as directed by ERO functions or the NERC Board, to support ERO Enterprise functions; and,
- Coordinate with ERO staff and liaise with government agencies and trade associations.
- Provide technical input and analyses on operating and planned BPS reliability and security, emerging issues and risks, and other general industry concerns at the request of the NERC Board or NERC staff.

Develop a two-year strategic work plan to guide the deliverables of the RSTC.

- Ensure alignment of the strategic work plan with ERO reports and analyses, including the NERC Business Plan and Budget, ERO Enterprise Long-Term Strategy, Operating Plan, biennial Reliability Issues Steering Committee (RISC) ERO Reliability Risk Priorities report, State of Reliability report recommendations, Long-Term, Seasonal and Special Reliability Assessment recommendations and ongoing event analysis trends;
- Coordinate the objectives in the strategic work plan with the Standing Committees Coordinating Group; and,
- Obtain annual NERC Board approval.

Coordinate and oversee implementation of RSTC subgroup work plans.

- Create and disband subcommittees, working groups and task forces to support ERO Enterprise functions;
- Harmonize and approve the work plans of subcommittees, working groups, and task forces with the strategic work plan; and,
- Track the progress of the subcommittees, working groups, and task forces to ensure that they complete assigned activities as outlined in their work plans.

Advise the NERC Board of Trustees.

- Update the NERC Board semi-annually on progress in executing the strategic work plan; and
- Present appropriate deliverables to the NERC Board.

Section 3: Membership

Representation Model

The RSTC has a hybrid representation model consisting of the following types of memberships:

- Sector members;
- At-large members; and,
- Non-voting members.

Two members shall be elected to each of the following membership sectors:

- Sector 1 - Investor-owned Utility;
- Sector 2 – State or Municipal Utility;
- Sector 3 - Cooperative Utility;
- Sector 4 - Federal or Provincial Utility/Power Marketing Administration;
- Sector 5 - Transmission-Dependent Utility;
- Sector 6 - Merchant Electricity Generator;
- Sector 7 - Electricity Marketer;
- Sector 8 - Large End Use Electricity Customer;
- Sector 9 - Small End Use Electricity Customer;
- Sector 10 - ISO/RTO; and,
- Sector 12 - Government Representatives.

Selection of at-large members will allow for better balancing of representation on the RSTC of the following:[1]

- Regional Entity and Interconnection diversity (i.e., goal of having at least one representative from each Interconnection and Regional Entity footprint);
- Subject matter expertise (Planning, Operating, or Security);
- Organizational types (Cooperatives, Investor-Owned Utilities, Public Power, Power Marketing Agencies, etc.); and,
- North American countries, consistent with the NERC bylaws (Canada, Mexico, and U.S.).

Below is a breakdown of voting and non-voting membership on the RSTC:

Voting Membership	
Name	**Voting Members**
Sectors 1-10 and 12	22
At-Large	10
Chair and Vice Chair	2
Total	**34**

[1] *See,* NERC Sector 13 in the NERC Bylaws (2021).

Non-Voting Membership[2]	
Non-Voting Member	**Number of Members**
NERC Secretary	1
United States Federal Government	2
Canadian Federal Government	1
Provincial Government	1
Total	**5**

Member Selection

RSTC members will be from organizations who are NERC members, but it is not required.

Members are appointed to the RSTC upon approval of the NERC Board and serve on the RSTC at the pleasure of the NERC Board.

1. **Affiliates**

   A company, including its affiliates, may not have more than one member on the RSTC. Any RSTC member who is aware of a membership conflict of this nature is obligated to notify the RSTC secretary within 10 business days. The RSTC secretary will in turn report the conflict to the RSTC chair.

   Members impacted by such a conflict, such as through a merger of organizations, must confer among themselves to determine which member should resign from the RSTC and notify the secretary and chair; however, if they cannot reach an amicable solution to determine who will remain, the Nominating Subcommittee will review the qualifications of each member and make a recommendation to the NERC Board for final approval.

2. **Election of Sector Members**

   NERC members in each sector will annually elect members for expiring terms or open seats using a nomination and election process that is open, inclusive, and fair. In the event that a sector has no nominations for one or both sector seats at the annual election, the RSTC will convert those empty sector seats to at-large seats until the end of the term.

   Sector elections will be completed in time for the Nominating Subcommittee to identify and nominate at-large representatives as well as for the secretary to send the full RSTC membership list to the NERC Board for approval at its annual February meeting.

   If an interim vacancy is created in a sector, a special election will be held unless it would coincide with the annual election process. If a sector cannot fill an interim vacancy, then that sector seat will remain vacant until the next annual election. Interim sector vacancies will not be filled with an at-large representative.

3. **Nominating Subcommittee**

   The Nominating Subcommittee (RSTC NS) will consist of six members (the RSTC Vice-Chair and five members drawing from different sectors and at-large representatives). Apart from the Vice-Chair, members of the RSTC EC shall not serve on the RSTC NS.

   The NS members are nominated by the RSTC chair and voted on by the full RSTC membership.

   The term for members of the NS is two years.

[2] Upon recognition of NERC as the Electric Reliability Organization, Mexican Government representation will be equitable and based approximately on proportionate Net Energy for Load.

The RSTC NS is responsible for (a) recommending individuals for at-large representative seats, and, (b) managing the process to select the chair and/or vice chair of the RSTC. The RSTC vice-chair shall recuse him or herself from this process unless he or she is not seeking re-election. At-large members on the RSTC NS shall recuse themselves from recommendations for at-large representative seats if they are seeking reappointment.

4. **Selection of At-Large Members**

   The RSTC NS solicits and reviews nominations from the full RSTC and industry to fill at-large representative seats. After reaching consensus, the RSTC NS submits a recommended slate of at-large candidates to the Board at its annual February meeting for approval. To the extent practicable, the RSTC NS will balance the following criteria to select at-large members: (a) geographic diversity from all Interconnections and ERO Enterprise Regional Entities; (b) high-level understanding and perspective on reliability risks based on experience at an organization in a sector; and, (c) experience and expertise from an organization in the sector relevant to the RSTC.

   The Board votes to appoint the at-large members.

5. **Non-Voting Members**

   At the start of the annual RSTC nomination process the RSTC secretary will coordinate with entities entitled to non-voting membership to identify representatives for the non-voting seats.

6. **International Representation**

   International representation on the RSTC shall be consistent with Article VIII Section 4 of the NERC Bylaws.

Member Expectations

RSTC members are expected to act in accordance with this charter, as well as to accomplish the following:

- Adhere to NERC Antitrust Guidelines and Participant Conduct Policy;
- Demonstrate and provide knowledge and expertise in support of RSTC activities;
- Where applicable, solicit comments and opinions from constituents and groups of constituents or trade organizations represented by the member and convey them to the RSTC;
- Respond promptly to all RSTC requests, including requests for reviews, comments, and votes on issues before the RSTC; and,
- During meetings, comply with the procedures outlined for that meeting and identified in this Charter (see **Section 9**).

Term

When the initial staggered, two- and three-year terms of RSTC members have expired , all subsequent terms will be two years.

An RSTC member may serve a term shorter than two years if:

- Two members are simultaneously selected to a sector that did not have any existing members, in order to stagger their terms, one member will be assigned a one-year term and the second member will be assigned a two-year term.
- A member is selected to fill a vacant member seat between elections, the term will end when the term for that vacant seat ends.

There are no limits on the number of terms that members can serve.

Vacancies and Proxies

Membership vacancies may be filled between annual elections using the aforementioned selection process.

1. **Vacancies Created By the Member**

   In the event a member can no longer serve on the RSTC, that member will submit a written resignation to the RSTC chair or the secretary.

2. **Vacancies Requested by the Chair**

   The chair may request any RSTC member who ceases to participate in the RSTC consistent with member expectations (above) and to the satisfaction of the chair, to submit a resignation or to request continuation of membership with an explanation of extenuating circumstances. If a written response is not received within 30 days of the chair's request, the lack of response will be considered a resignation. If the chair is not satisfied with a written response, the RSTC chair will refer the matter to the NERC Board.

3. **Vacancies Requested By the Board**

   RSTC members serve at the pleasure of the NERC Board. The NERC Board may initiate a request for resignation, removal, or replacement a member from the RSTC, as it deems appropriate or at the request of the RSTC chair.

4. **Proxies**

   A voting member may select a proxy who attends and votes during all or a portion of a committee meeting in lieu of a voting member, provided that the absent voting representatives notifies the RSTC chair, vice chair, or secretary of the proxy. A proxy may not be given to another RSTC member. A proxy must meet the RSTC's membership eligibility requirements, including affiliate restrictions.

   To permit time to determine a proxy's eligibility, all proxies must be submitted to the secretary in writing at least one week prior to the meeting (electronic transmittal is acceptable) for approval by the chair. Any proxy submitted after that time will be accepted at the chair's discretion.

Section 4: Meetings

Open meetings will be conducted in accordance with governance procedures in **Section 9**. The Chair may consult Robert's Rules of Order for additional guidance.

Quorum

The quorum necessary for transacting business at meetings of the RSTC is two-thirds of the voting members currently on the RSTC's roster and is determined once at each meeting.

If a quorum is not determined, the RSTC may not take any actions requiring a vote; however, the chair may allow discussion of the agenda items.

Voting

Actions by the RSTC will be approved upon receipt of the affirmative vote of two-thirds of the votes cast at any meeting at which a quorum is present. An abstention ("present" vote) does not count as a vote cast.

Voting may take place during regularly scheduled in-person/hybrid meetings with some attendance virtual, via electronic mail, or via conference call/virtual meeting.

Executive, Open and Closed Sessions

The RSTC holds meetings open to the public, except as noted herein. Although meetings are open, only voting members may offer and act on motions.

The chair may hold closed sessions with the Executive Committee.

The chair may also hold closed sessions in advance of the open meeting with limited attendance (e.g., with sponsors and/or members of subgroups) applied sparingly and on a non-discriminatory basis. Any discussion of confidential information in a closed session shall be consistent with Section 1500 of the NERC ROP.

All meetings of the RSTC NS shall be conducted in closed session.

Majority and Minority Views

All members of a committee will be given the opportunity to provide alternative views on an issue. The results of committee actions, including recorded minutes, will reflect the majority as well as any minority views of the committee members.

Action without a Meeting

Any action required or permitted at a meeting of the committee may be taken without a meeting at the request of the chair.

Such action without a meeting will be performed by electronic ballot (e.g., telephone, email, or Internet survey) and considered a roll call ballot. The secretary will announce the action required at least five business days before the date on which voting commences. As time permits, members should be allowed a window of 10 business days to vote. The secretary will document the results of such an action within 10 business days of the close of the voting period. Such action must meet the regular meeting quorum and voting requirements above.

Section 5: Officers and Executive Committee

Officers

The RSTC will have two officers – one chair and one vice-chair.

Officers shall be selected as follows:

- The NS solicits nominations for chair and vice-chair through an open nomination process. Self-nominations are permitted during the open nomination period.
- At the close of the nomination period, the NS will propose a chair and a vice-chair candidate. The full RSTC will elect the chair and vice chair.
- The chair and vice chair must be a committee member and shall not be from the same sector.
- The elected chair and vice-chair are appointed by the NERC Board.
- No individual may serve more than one term as vice chair and one term as chair unless an exception is approved by the Board.

Secretary

NERC will appoint the RSTC secretary.

A member of the NERC staff will serve as the secretary of the RSTC. The secretary will do the following:

- Manage the day-to-day operations and business of the RSTC;
- Prepare and distribute notices of the RSTC meetings, prepare the meeting agenda, and prepare and distribute the minutes of the RSTC meetings;
- Facilitate the election/selection process for RSTC members; and,
- Act as the RSTC's parliamentarian.

Chair

The chair will direct and provide general supervision of RSTC activities, including the following:

- Coordinate the scheduling of all meetings, including approval of meeting duration and location;
- Develop agendas and rule on any deviation, addition, or deletion from a published agenda;
- Preside at and manage meetings, including the nature and length of discussion, recognition of speakers and proxies, motions, and voting;
- Act as spokesperson for the RSTC at forums inside and outside of NERC; and,
- Attend meetings of the NERC Board when necessary to report on RSTC activities.

Vice Chair

The vice chair will assume the responsibilities of the chair under the following conditions:

- At the discretion of the chair (for brief periods of time);
- When the chair is absent or temporarily unable to perform the chair's duties; or,
- When the chair is permanently unavailable or unable to perform the chair's duties. In the case of a permanent change, the vice chair will continue to serve until a new chair is nominated and appointed by the NERC Board.

Executive Committee

The Executive Committee (RSTC EC) shall consist of six members:

- Chair;
- Vice-chair;
- Four RSTC voting members selected by the RSTC chair and vice-chair with a reasonable balance of subject matter expertise in Operations, Planning, and/or Security and with consideration for diversity in representation (i.e., sectors, Regional Entities, Interconnections, etc.).

The EC of the RSTC is authorized by the RSTC to act on its behalf between regular meetings on matters where urgent actions are crucial and full RSTC discussions are not practical. Actions taken by the EC shall be announced at the open meetings and included in the minutes of the open meetings.

Ultimate RSTC responsibility resides with its full membership whose decisions cannot be overturned by the EC. The RSTC retains the authority to ratify, modify, or annul RSTC EC actions.

Section 6: RSTC Subordinate Groups

The RSTC organizational structure will be aligned as described by the NERC Bylaws to support a superior-subordinate hierarchy.

The RSTC may establish subcommittees, working groups, and task forces as necessary. The RSTC will be the responsible sponsor of all subordinate subcommittees, working groups, or task forces that it creates, or that its subordinate subcommittees and working groups may establish.

Officers of subordinate groups will be appointed by the chair of the RSTC.

Subcommittees, working groups, and taskforces will conduct business in a manner consistent with all applicable sections of this Charter.

Subcommittees

The RSTC may establish subcommittees to which the RSTC may delegate some of RSTC's functions. The RSTC will approve the scope of each subcommittee it forms. The RSTC chair will appoint the subcommittee officers (typically a chair and a vice chair) for a specific term (generally two years). The subcommittee officers may be reappointed for up to two additional terms. The subcommittee will work within its assigned scope and be accountable for the responsibilities assigned to it by the committee. The formation of a subcommittee, due to the permanency of the subcommittee, will be approved by the NERC Board.

Working Groups

The RSTC may delegate specific continuing functions to a working group. The RSTC will approve the scope of each working group that it forms. The RSTC chair will appoint the working group officers (typically a chair and a vice chair) for a specific term (generally two years). The working group officers may be reappointed for one additional term. The RSTC will conduct a "sunset" review of each working group every year. The working group will be accountable for the responsibilities assigned to it by the RSTC or subcommittee and will, at all times, work within its assigned scope. The RSTC should consider promoting to a subcommittee any working group that is required to work longer than one term.

Task Forces

The RSTC may assign specific work to a task force. The RSTC will approve the scope of each task force it forms. The RSTC chair will appoint the task force officers (typically a chair and a vice chair). Each task force will have a finite duration, normally less than one year. The RSTC will review the task force scope at the end of the expected duration and at each subsequent meeting of the RSTC until the task force is retired. Action of the RSTC is required to continue the task force past its defined duration. The RSTC should consider promoting to a working group any task force that is required to work longer than one year.

Section 7: Meeting Procedures

Voting Procedures for Motions

- All voting shall default to being conducted through use of a poll unless a need to record each member's vote is identified or requested. Where a need to record each member's vote is requested or identified, the RSTC may conduct voting via a roll call vote.
- The committee must approve conducting a roll call vote for the motion.
- For roll call votes, the secretary will call each member's name.
- Members answer "yes," or "no," but may answer "present" if they wish to abstain from voting. As provided above, an abstention does not count as a vote cast.

Minutes

- Meeting minutes are a record of what the committee did, not what its members said.
- Minutes should list discussion points where appropriate, but should usually not attribute comments to individuals. It is acceptable to cite the chair's directions, summaries, and assignments.
-
- All Committee members are afforded the opportunity to provide alternative views on an issue. The meeting minutes will provide an exhibit to record minority positions.

Section 8: RSTC Deliverables and Approval Processes

The RSTC will abide by the following parameters regarding approval, endorsement, or acceptance of committee deliverables.

Reliability Guidelines, Security Guidelines and Reference Documents

Reliability Guidelines and Security Guidelines are documents that suggest approaches or behavior in a given technical area for the purpose of improving reliability. Reliability Guidelines and Security Guidelines are not binding norms or mandatory requirements. Reliability Guidelines and Security Guidelines may be adopted by a responsible entity in accordance with its own facts and circumstances.

1. **New/updated draft guideline approved for industry posting.**

   The RSTC approves for posting for industry comment the release of a new or updated draft guideline developed by one of its subgroups or the committee as a whole.

   The draft guideline is posted as "for industry-wide comment" for 45 days. If the draft guideline is an update, a redline version against the previous version must also be posted.

   After the public comment period, the RSTC will post the comments received as well as its responses to the comments. The RSTC may delegate the preparation of responses to a committee subgroup.

   A new or updated guideline which considers the comments received, is approved by the RSTC and posted as "Approved" on the NERC website. Updates must include a revision history and a redline version against the previous version.

   After posting a new or updated guideline, the RSTC will continue to accept comments from the industry via a web-based forum where commenters may post their comments.

   a. Each quarter, the RSTC will review the comments received.

   b. At any time, the RSTC may decide to update the guideline based on the comments received or on changes in the industry that necessitate an update.

   c. Updating an existing guideline will require that a draft updated guideline be approved by the RSTC in the above steps.

2. **Review of Approved Reliability Guidelines, Security Guidelines and Reference Documents**

   Approved Reliability Guidelines or Reference Document shall be reviewed for continued applicability by the RSTC at a minimum of every third year since the last revision.

3. **Communication of New/Revised Reliability Guidelines, Security Guidelines and Reference Documents**

   In an effort to ensure that industry remains informed of revisions to a Reliability Guideline or Reference Document or the creation of a new Reliability Guideline or Reference Document, the RSTC subcommittee responsible for the Reliability Guideline will follow an agreed upon process.

4. **Coordination with Standards Committee**

   Standards Committee authorization is required for a Reliability Guideline or Security Guidelines to become a supporting document that is posted with or referenced from a NERC Reliability Standard. See Appendix 3A in the NERC's ROP under "Supporting Document."

Section 1600 Data or Information Requests

A report requested by the RSTC that accompanies or recommends a Rules of Procedure (ROP) Section 1600 - Data or Information Request will follow the process outlined below:

1. This Section 1600 request, with draft supporting documentation, will be provided to the RSTC at a regular meeting.
2. The draft Section 1600 data request and supporting documentation will be considered for authorization to post for comments at the RSTC regular meeting.
3. A committee subgroup will review and develop responses to comments on the draft Section 1600 data request and will provide a final draft report, including all required documentation for the final data request, to the RSTC at a regular meeting for endorsement.
4. The final draft of the 1600 data request – with responses to all comments and any modifications made to the request based on these comments – will be provided to the NERC Board.

Other Types of Deliverables

1. **Policy Outreach**

   On an ongoing basis, the RSTC will coordinate with the forums, policymakers, and other entities to encourage those organizations to share reliability guidelines, reference documents and lessons learned to benefit the industry.

   Reports required under the NERC ROP or as directed by an Applicable Governmental Authority or the NERC Board: documents include NERC's long-term reliability assessment, special assessments, and probabilistic assessments. These reports may also be used as the technical basis for standards actions and can be part of informational filings to FERC or other government agencies.

2. **White Papers**

   Documents that explore technical facets of topics, often making recommendations for further action. They may be written by subcommittees, working groups, or task forces of their own volition, or at the request of the RSTC.

3. **Reference Documents and Technical Reports**

   Documents that serve as a reference for the electric utility industry and/or NERC stakeholders regarding a specific topic of interest. These deliverables are intended to document industry practices or technical concepts at the time of publication and may be updated as deemed necessary, per a recommendation by the RSTC or its subgroups to reflect current industry practices.

4. **Implementation Guidance**

   Documents providing examples or approaches for registered entities to comply with standard requirements. The RSTC is designated by the ERO Enterprise as a pre-qualified organization for vetting Implementation Guidance in accordance with NERC Board -approved Compliance Guidance Policy. Implementation Guidance that is endorsed by the RSTC can be submitted to the ERO Enterprise for endorsement, allowing for its use in Compliance Monitoring and Enforcement Program (CMEP) activities.

5. **Standard Authorization Requests (SAR)**

   A form used to document the scope and reliability benefit of a proposed project for one or more new or modified Reliability Standards or definitions or the benefit of retiring one or more approved Reliability Standards. RSTC endorsement of a SAR supports: (a) initial vetting of the technical material prior to the formal Standards Development Process, and, (b) that sound technical justification material has been developed, and the SAR will not be remanded back to the RSTC to provide such justification per the Standard Processes Manual.

Review Process for other Deliverables

Deliverables with a deadline established by NERC management or the NERC Board will be developed based on a timeline reviewed by the RSTC to allow for an adequate review period, without compromising the desired report release dates. Due to the need for flexibility in the review and approval process, timelines are provided as guidelines to be followed by the committee and its subgroups.

A default review period of no less than 10 business days will be provided for all committee deliverables. Requests for exceptions may be brought to the RSTC at its regular meetings or to the RSTC ECif the exception cannot wait for an RSTC meeting.

In all cases, a final report may be considered for approval, endorsement, or acceptance if the RSTC, as outlined above, decides to act sooner.

Actions for Deliverables

1. **Approve:**

   The RSTC has reviewed the deliverable and supports the content and development process, including any recommendations.

2. **Accept:**

   The RSTC has reviewed the deliverable and supports the development process used to complete the deliverable.

3. **Remand:**

   The RSTC remands the deliverable to the originating subcommittee, refer it to another group, or direct other action by the RSTC or one of its subcommittees or groups.

4. **Endorse:**

   The RSTC agrees with the content of the document or action, and recommends the deliverable for the approving authority to act on. This includes deliverables that are provided to the RSTC by other NERC committees. RSTC endorsements will be made with recognition that the deliverable is subject to further modifications by NERC Executive Management and/or the NERC Board. Changes made to the deliverable subsequent to RSTC endorsement will be presented to the RSTC in a timely manner. If the RSTC does not agree with the deliverable or its recommendations, it may decline endorsement. It is recognized that this does not prevent an approval authority from further action.

Section 9: Meeting Governance

The RSTC will abide by the following procedures regarding taking actions on committee deliverables.

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and cannot reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	No	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." The vote is subject to a 2/3 majority approval. Also, any member may call the question. This motion is not debatable. The vote is subject to a 2/3 vote.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds
A Motion must have a second to ensure that at least two members wish to discuss the issue.

Announcement by the Chair
The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to procedure in this Charter.

2021 ERO Reliability Risk Priorities Report and the RSTC Work Plan

Action

Information and request for volunteers.

Summary

This agenda item will review the 2021 ERO Reliability Risk Priorities Report and the process to incorporate risk mitigation activities into the RSTC Work Plan. Efforts to identify and prioritize risks from the report will also be discussed. Chair Ford will request volunteers from the RSTC to participate in the risk prioritization and risk mitigation planning process to develop RSTC subgroup work plan items for approval by the RSTC in December, 2021.

Risk Registry

Action
Update

Summary
In an effort to continually monitor the existing risks to the bulk power system (BPS) and manage the efforts of the ERO Enterprise to actively identify and address current and new risks, NERC created a Risk Registry. This registry overlaps some with the risk profiles identified in the latest ERO Reliability Risk Priorities Report (RISC Report) and other risks identified in past reports and assessments. In addition to reporting on future emerging risks, the Risk Registry also focuses on reporting on activities addressing current emergent risks to the BPS. The draft of the Risk Registry identifies a few of the risks or "tasks" to address current risks to the BPS. The most critical and high priority tasks address energy adequacy, extreme natural events, security threats, and inverter performance. The security threats and extreme natural events mirror the risk profiles of the RISC report. Energy adequacy and inverters are a different categorization focused on grid transformation. Future versions of the Risk Registry will be used as project/resource management tool and will include a consistent risk prioritization method that will be periodically reviewed with the RISC.

Failure Modes and Mechanism Task Force (FMMTF)

Action
Information

Summary
The joint 2013 NERC Operating and Planning Committees' AC Substation Equipment Task Force report recommended that information on station equipment failures be collected through the NERC Event Analysis process. The Failure Modes and Mechanisms Task Force (FMMTF) was created by the EAS to analyze 14 types of BES substation equipment to determine their failure modes and mechanisms, FMM trends and patterns, and improve BES reliability by providing information useful for reducing station equipment failures. A short video explaining the FMM approach* is available. Currently FMM diagrams for eight types of common station equipment are available in the ERO portal for use and more are being prepared. (*https://vimeopro.com/nerclearning/cause-coding/video/208745179)

Recently, a FMM approach was used in discussing February 2021 Cold Weather Generation Problems in the NERC Winter Weather Webinar on September 2.

Security Working Group Update

Action
Information

Summary
Co-chair Katherine Street will provide an update on current SWG projects, new activities, and administrative updates.

Agenda Item 11
Reliability and Security
Technical Committee Meeting
September 8, 2021

Restoration Analysis to Evaluate Resilience of the Transmission System under Extreme Weather

Action
Information

Summary
The presentation will cover a new analysis included in the *2021 State of Reliability Report* (SOR), an analysis of restoration of the North American transmission system after extreme weather events. Additionally to the material included in the 2021 SOR, we will analyze impact and recovery for the top weather-related transmission events from 2015 to 2020 and discuss similarities and differences in restoration processes for most disruptive types of extreme weather (hurricanes, tornadoes, winter storms etc.).

Cybersecurity for the Operational Technology Environment (CyOTE) Program

Action
Information

Summary
The Department of Energy's Cybersecurity for Operational Technology Environments (CyOTE™) program provides a methodology for energy sector asset owner-operators to combine network-based sensor data with local context to recognize faint signals of malicious cyber activity before an adversary can cause higher-impact effects. CyOTE began as a pilot sponsored by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) in 2016, transitioned to a program in 2019, and in July 2021 publicly released the "Methodology for Cybersecurity in Operational Technology Environments" report.

By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection from broader but informative sources in operations and even in the business domain, asset owners can better understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. Visibility is necessary, but the importance of visibility is in the understanding and decisions it drives – complicated by infrastructure changes, new technologies, and determined and sophisticated adversaries. CyOTE's vision is to allow an entity to independently get to the point of making a risk informed business decision on whether to respond to an incident or fix a reliability failure, sooner and with more confidence.

Cybersecurity for the Operational Technology Environment (CyOTE™)

Methodology for Cybersecurity in Operational Technology Environments

25 June 2021

CyOTE Cybersecurity for the Operational Technology Environment

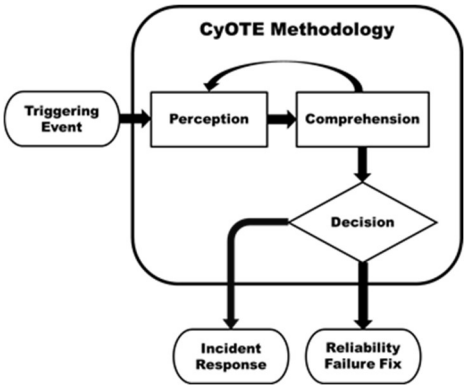
U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, & EMERGENCY RESPONSE

INL Idaho National Laboratory

Table of Contents

EXECUTIVE SUMMARY

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), through the Cybersecurity for the Operational Technology Environment (CyOTE) Program, worked with energy sector asset owners and operators (AOOs), partners, and Idaho National Laboratory (INL) to develop capabilities for AOOs to independently detect adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. Unlike the approach taken with commercial security solutions, CyOTE seeks to tie anomalies in cyber operations to a cyber-attack. By stringing together multiple techniques in the OT environment, AOOs can identify attack campaigns with ever decreasing impacts.



The CyOTE methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) is used as a common lexicon to identify a set of triggering events related to three Use Cases – Alarm Logs, Human-Machine Interface (HMI), and Remote Logins – which together account for 87 percent of the techniques commonly used by adversaries. The CyOTE methodology is also appropriate for OT-related anomalies perceived outside the three Use Cases, such as through the energy system itself.

CyOTE provides a general approach for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation – a triggering event – is perceived, and continues to the point where the anomaly is comprehended with sufficient confidence to make a business risk decision on the appropriate resolution. If sufficient evidence of a malicious nexus is found, the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to the situation addressed through existing organizational corrective maintenance and work management procedures.

By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. CyOTE can assist AOOs in prioritizing their OT environment visibility investments. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

BACKGROUND

Cybersecurity is not easy nor inexpensive to attain and maintain. This is perhaps even more true for operational technology (OT) systems. Too often, security professionals are lulled into thinking the right process or checklist is the key to security, whereas others in the organization may believe acquiring and installing a particular technology will provide security. Although both processes and infrastructure are necessary, individually they are not sufficient, and overemphasis on either can inadvertently drive an organization to pursue compliance with a process or standard as opposed to security. Just because an individual or an organization believes an asset or capability is protected does not mean it cannot be compromised by an adversary with sufficient motivation and resources. Compliance can breed complacency, and complacency is the antithesis of security. A questioning attitude and intellectual curiosity are powerful antidotes to complacency.

Adversaries commonly vary their activities to produce different static indicators of compromise (IOCs). This variance is a straightforward, quick, and low cost way for an adversary to avoid basic automated detection capabilities. Changing these fixed indicators, which already exist in a time-bounded context, results in asset owners and operators (AOOs) expending resources in enduring low-payoff "whack-a-mole"[a] activities. The broader context in which those static IOCs appear as signatures is harder for an adversary to change, however. This is the essence of David Bianco's Pyramid of Pain[1] shown in Figure 1, which relates the volume of different types of indicators to the adversary's difficulty in changing them to avoid detection.

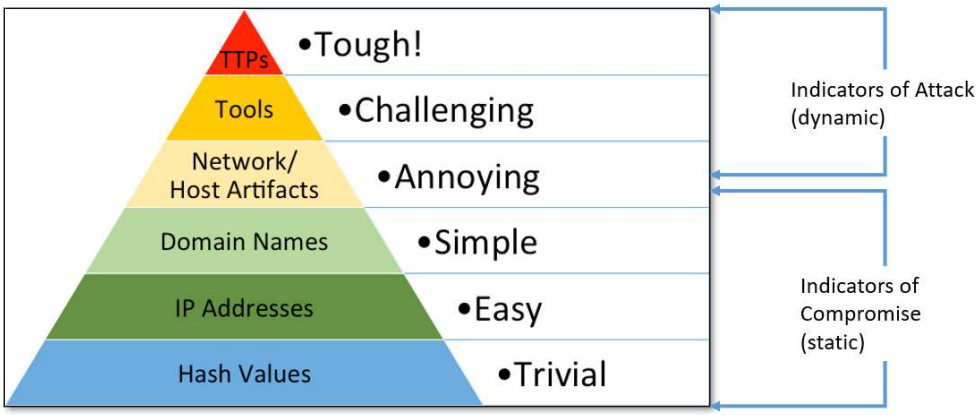


Figure 1. The Pyramid of Pain

Adversary behaviors are at the tip of the pyramid. These indicators of attack are mostly unconcealable and need to be investigated. The challenge is to identify a behavioral indicator of attack that exists not at a fixed logical and temporal location such as an IOC, but rather as a chain

[a] In this context, "whack-a-mole" refers to the practice of surveying defended environments for static IOCs used in previous attacks or shared from an external source with limited context. The term relates to the arcade game, where another mole pops up as soon as one is hit down, where "winning" is a matter of how fast you can respond to the new stimuli. See https://www.securityweek.com/root-cause-analysis-stop-playing-whack-mole for an IT-centric description of why this is a poor strategy.

of related events across time and space. Each individual link in the chain can be obfuscated or hidden to some degree (sometimes substantially obscured, though all events display a signature somewhere), but are much clearer when recognized as a chain instead of a collection of individual links. Behavioral indicators of attack are difficult if not impossible for an adversary to completely hide as faint signals and will always be detectable within the noise of regular operations. Recognizing a behavioral indicator of attack is much more challenging in real life than in hindsight. The faint signals typically appear as anomalies in operations, OT, information technology (IT), and business processes; just as a behavioral indicator of attack can span many of these areas, so must an AOO's internal and independent investigation. Questioning attitudes and intellectual curiosity are critical to this investigative process, just as they are to combatting complacency.

> *"When trouble is sensed well in advance it can easily be remedied; if you wait for it to show itself any medicine will be too late because the disease will have become incurable. As the doctors say of a wasting disease, to start with it is easy to cure but difficult to diagnose; after a time, unless it has been diagnosed and treated at the outset, it becomes easy to diagnose but difficult to cure."*
>
> *Niccolo Machiavelli,* The Prince[2]

Since 2016, the CyOTE Program under the auspices of DOE's CESER Office, in collaboration with INL, partners with industry to develop targeted strategies to increase the cybersecurity and resiliency of America's energy sector. CyOTE was conceived to facilitate OT data sharing and analysis with cleared government resources, philosophically similar to but separate from the IT-centric Cybersecurity Risk Information Sharing Program (CRISP). At the start, CyOTE established collaborative partnerships with a small number of AOOs through a Pilot activity to determine the most useful information to collect from AOO OT environments, and how to share it with other CyOTE Program participants. The goals of the Pilot were to improve AOO cyber defenders' and operators' ability to detect, investigate, and mitigate malicious activity within the OT environment to reduce risk and increase efficiency. The Pilot consisted of two phases which informed the transition to an enduring Program in 2019. Figure 2 depicts the CyOTE Program's evolution.

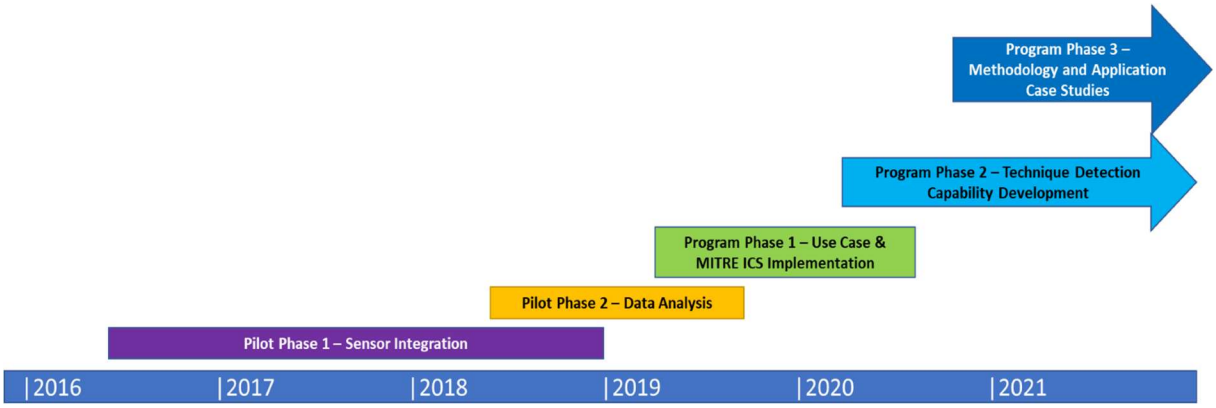


Figure 2. CyOTE Pilot and Program Phases

PILOT PHASE I - SENSOR INTEGRATION

First, the CyOTE team worked with a small representative group of electric industry AOOs through Pilot engagements to identify what data streams to monitor, where to place sensors, and how to bidirectionally share data before and after enrichment while protecting confidentiality and data sources. This effort resulted in Program alignment to the Industrial Control Systems (ICS) Cyber Kill Chain[3] and a feasibility evaluation for creating a repeatable, industry-wide approach for OT threat data analysis. To address how the identified data could be securely collected and transmitted to a central location for analysis and enrichment, the CyOTE team explored research topics such as firmware integrity, OT sensor capabilities, and data anonymization. Several of the lessons learned[b] from Phase I are relevant to the CyOTE methodology, including:

- Data observations of interest, which drive OT alerting and alarming capabilities, should be prioritized based on the potential impacts to the operational process.
- Sensor deployment should align with the organization's overall defensive priorities and be prioritized with an understanding of the overall system's visibility.
- Sensor capabilities should align with the characteristics of OT environments being monitored.
- Accounts, assets, and network activity should be audited at regular intervals to supplement sensor data.

Phase I of the Pilot culminated when further progress began to be impeded by data custodial issues, some related to interpretation of North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements. This challenge eventually drove the realization CyOTE would be most successful in eventual production when its capabilities could be

[b] For a more comprehensive discussion of insights from the Pilot and the Program to date, see the forthcoming "Observations and Lessons Learned from the CyOTE Program" white paper; contact CyOTE.Program@hq.doe.gov for further information.

employed independently by the AOO, free from external dependencies along the critical path, such as data transfer.

PILOT PHASE II – DATA ANALYSIS

The second phase of the Pilot involved administrative and logistical activities to successfully transfer a sizeable volume of AOO data to the CyOTE team for analysis. The analysis of these data sets yielded further lessons learned, including:

- Worthwhile data analysis requires context, not just content.
- Data collected should be filtered according to the analytical questions to be answered. Relevant data is more useful than simply more data, as the law of diminishing marginal returns applies beyond some point.
- Analysis should incorporate understanding of adversary techniques and behaviors, and not rely solely on expertise in the OT domain.
- Data analysis can and should be used to identify gaps in data availability to prioritize further OT monitoring investments.

Phase II of the Pilot culminated when second-party analysis of the transferred data, absent of the deep and broad firsthand context only the originator and owner of such data can truly possess, had proceeded as far as possible. The CyOTE team identified multiple anomalies through analysis of this real-world data, demonstrating the value in the effort. The perception of these anomalies came several months after the data was collected, however, and meaningful comprehension of the anomalies required significant collaboration with the AOO providing the data.

Partially overlapping with the conclusion of this second phase of the Pilot, CyOTE transitioned from a Pilot to a Program in early 2019. As expected, the challenges and barriers identified in the Pilot phases informed the inception of the CyOTE Program as stakeholders recognized the value and efficiency of starting with a recently perceived abnormality instead of analyzing data to find abnormalities after the fact and with less than adequate context. Most importantly, this transition coincided with a fundamental shift in thinking. Rather than collecting bulk raw data from multiple AOOs with centralized analysis, the CyOTE Program realized AOOs must lead this effort with event-driven sharing. AOOs maintain firsthand access to whatever data exists and have the best and most context to accurately interpret that data. Ultimately the AOO owns the most risk and has the most straightforward management options.

PROGRAM PHASE I – USE CASE AND MITRE ICS ATT&CK FRAMEWORK IMPLEMENTATION

Upon its transition to a Program, CyOTE represented the OT portion of CESER's overarching situational awareness Program and capabilities. Collaboration with industry participants identified the need to take a use case approach to identifying types of events with the potential to trigger event-driven metadata sharing through an established and protected channel, and the corresponding metadata elements and sources necessary for effective analysis to be shared.

Like most other industries, the energy sector contains a broad variety of organizational and individual perspectives, beliefs, and words to describe the same universe of items and ideas.[c] Due to the importance of interdisciplinary communication within AOOs, and the need to normalize and thus trend information from multiple AOOs with the eventual goal of sharing actionable insights across the sector, a common language was necessary. The CyOTE team decided the use of MITRE's ATT&CK® Framework for ICS,[4] would provide the shared lexicon necessary for consistent description and understanding of detection and evaluation concepts.

CESER formed three Working Groups to explore OT data Use Cases with volunteers from several participating energy companies. These Working Groups examined the 120+ adversary techniques in the ATT&CK Framework for ICS and mapped them to generic OT data sources not specific to any participant's OT architecture. The three Use Cases—Alarm Logs, HMI, and Remote Logins—were identified by CESER and validated through INL analysis as situations where OT log data may have a high likelihood of containing attack indicators. Together, these three Use Cases provide coverage for 87 percent of all techniques described in the ATT&CK Framework for ICS as shown in Figure 3.[d] With only *a priori* assumptions on adversary behaviors and intentions, detection of a technique relevant to multiple Use Cases (as shown by the colored bars at the bottom of the technique boxes in Figure 3) is a stronger indicator of potential malicious activity.

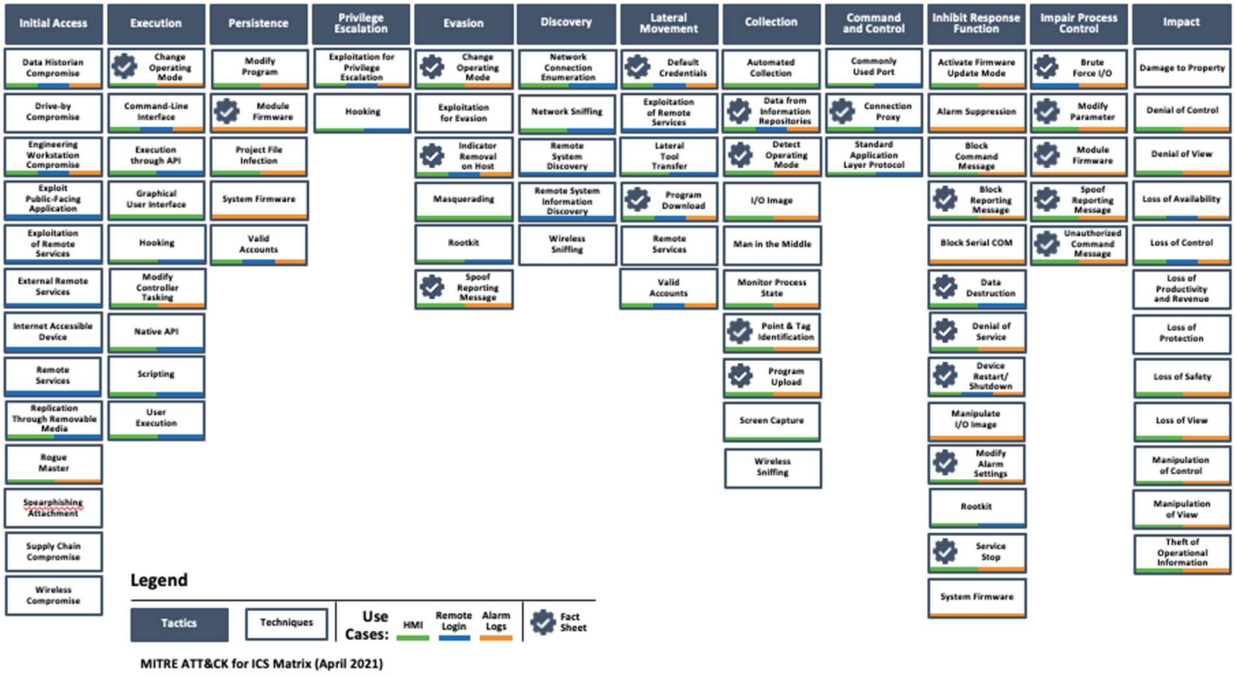


Figure 3. CyOTE Tactics and Techniques Chart

[c] See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3575067/ for a deeper treatment of the importance of shared language to achieve effective communication.

[d] The Use Case analysis work was conducted based on the original (January 2020) release of the ATT&CK Framework for ICS and covered 82 percent (80 of 96) of the techniques in that version. The 87 percent figure is calculated from the current (April 2021) release of the Framework, where 77 of 89 techniques are covered.

With the techniques mapped to Use Cases, the Working Groups moved forward to build out how an AOO could identify evidence of technique use in a production OT environment. This activity centered on triggering events, data sources, and data availability, with the initial goal of enabling programmatic event-driven sharing. For each Use Case, AOOs identified possible triggering events based on their experience which would initiate data collection, analysis, and sharing. These triggering events were then mapped to the adversary techniques for which there could be a signature. Next, the team enumerated a comprehensive set of data fields and elements to support comprehensive analysis, and from what sources those data fields may be available. This "wish list" of data sources and elements was subdivided into three high-level buckets: data collected today; existing data which could be collected today but is not at present; and data that does not exist or cannot be collected without new capabilities. This process is depicted in Figure 4.

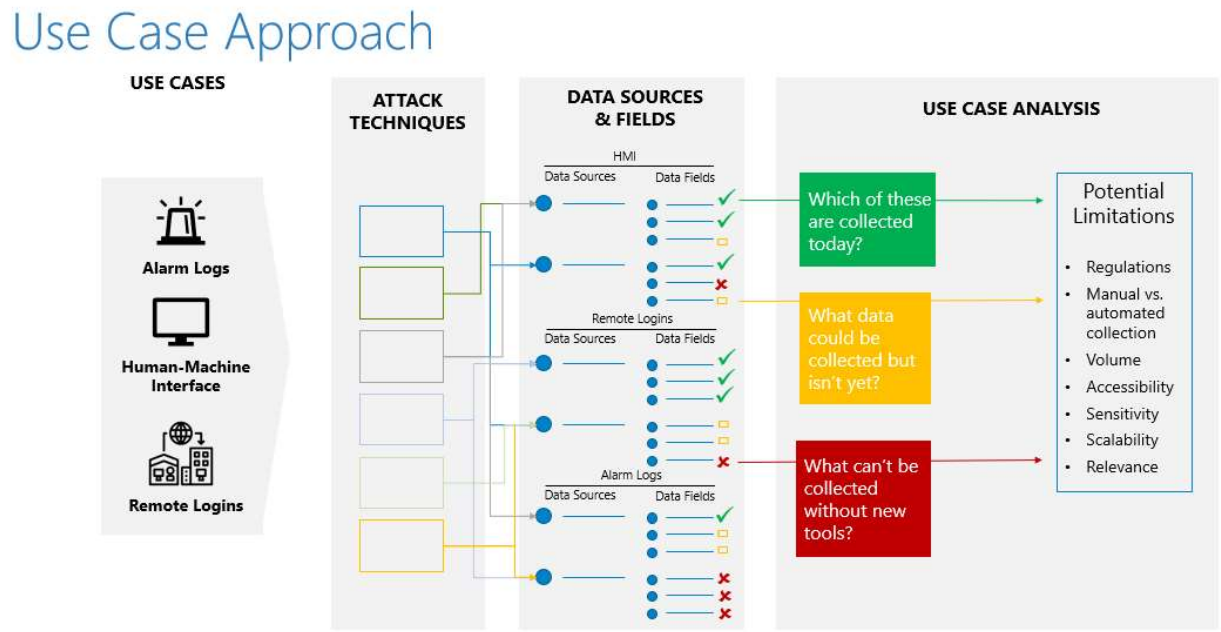


Figure 4. Mapping Adversary Techniques to Data Availability

Coming out of the Working Groups, the AOOs and CyOTE team recognized their findings and insights were applicable to enabling event-driven intelligence sharing as much, if not more, than the initial goal of metadata sharing. Moving from sharing raw information captured following a triggering event, to sharing intelligence[e] based on analysis of that data with the benefit of firsthand context, avoids some of the practical pitfalls common to data-sharing aspirations and may even encourage increased sharing because the data owner retains more control over sharing decisions.

[e] The difference between information and intelligence (in an IT cyber threat intelligence context) is described in this 2015 *Dark Reading* article: https://www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851.

Through this effort, the AOOs and CyOTE team increased the collective understanding of challenges and opportunities, and validated or refuted commonly held, but not rigorously studied, beliefs. Key takeaways from the Use Case identification and ATT&CK Framework for ICS implementation included:

- Current OT data collection primarily supports operations. Data collected and transmitted to control centers is mostly in support of monitoring and control of the operational processes. Much of the data beneficial for cyber-attack technique detection is not currently collected. Some devices could be reconfigured to capture additional useful data, for automated transmission or manual retrieval.
- Data at the field device or substation level may be more valuable, but requires significant effort—and potentially new capabilities—to monitor.
- Today's OT environments mostly lack automated capture capabilities. Event-driven data sharing will likely require manual action by AOOs to retrieve and share data.
- Network-level data gathered from firewalls and switches is far more readily available and easier to collect than system-level or device-level data today.
- Programmatic sharing of data with external parties requires legal agreements and certain regulatory and liability protections. These mechanisms take a significant amount of time to develop and execute.
- AOOs generally desire access to near real-time OT threat information and detection tools to enhance risk mitigation and complement, not replace, existing cybersecurity solutions.
- Large volumes of data are necessary for establishing initial baselines, but programmatic value from large-scale collection is currently confounded by challenges with encryption, transfer, analysis, and privacy.
- Data without context is not helpful in identifying anomalous activity within OT environments.
- Data correlation is necessary to provide context to information and identify anomalous "triggering" events.
- MITRE's ATT&CK Framework for ICS is more useful than the ICS Kill Chain in this situation because of its greater breadth and specificity.
- Interdepartmental and interdisciplinary cooperation within an AOO organization is essential to adequately identify, collect, and understand all the available data and contextual information.
- The value of event-driven information sharing increases when the time and place of the analysis and decision to share shifts earlier and towards AOOs. This has the added benefit of retaining complete control of what to share with the organization who owns the data and has the best context to interpret it.

This activity culminated with the publication of the *Use Case Working Group Results* report[f] in June 2020, documenting the complete findings of the three Use Case Working Groups.

[f] This report is designated Official Use Only and TLP: AMBER; contact CyOTE.Program@hq.doe.gov for more information.

PROGRAM PHASE II – TECHNIQUE DETECTION CAPABILITY DEVELOPMENT

Based on the results of the three Use Case Working Groups' identification of potential triggering events and data sources, CyOTE developed an inventory of Fact Sheets to provide information to AOOs to increase understanding of adversary techniques (Figure 3). These Fact Sheets provide foundational knowledge to enable technique detection capabilities whether manual or automated. The capabilities described in the Fact Sheets can speed the detection of suspicious and potentially malicious activity when implemented in an AOO's OT environment.

The Fact Sheets of technique descriptions are identified in the *CyOTE Technique Detection Capabilities* report.[g] The CyOTE team is working directly with a subset of AOO partners using AOO-supplied data and insights from the Use Case Working Groups to better understand the requirements and efforts needed to deploy a detection capability created from a Fact Sheet to the level where it is implemented in an AOO production OT environment.

Throughout the CyOTE Pilot and Program Phases, participating AOOs and the CyOTE team gained valuable insight from recurring themes across phases. Perhaps the most important realization was to look beyond technologies and networks and recognize *everything* is a sensor.[h] Given the faint signals and operational anomalies available to initially detect malicious cyber activity in an OT environment, an AOO must seek out and take full advantage of every potential source of useful information available to them. The Fact Sheets, with their technology-agnostic and holistic approach, provide a vehicle to begin this journey.

PROGRAM PHASE III – METHODOLOGY AND APPLICATION CASE STUDIES

The CyOTE Program is currently in Phase III, Methodology and Application Case Studies. The goal is to capitalize on the investments in the CyOTE Pilot and Program to build the body of knowledge around OT attacks and defenses to position AOOs for independent success regardless of size, experience, or business model.

A main activity for this phase is to validate the assumption for attacks on OT environments. Although the first point of entry and the final effects realized may vary significantly across incidents, the intermediate adversary techniques and procedures used in the middle of the kill chains are frequently reused. This adversary reuse increases the chances to detect and interdict an attack before the most significant impacts can be realized because the signatures are understood even though they may not have been detected – an AOO knows what to look for in their OT environments.

---

[g] Contact CyOTE.Program@hq.doe.gov for more information regarding the "CyOTE Technique Detection Capabilities" report and Fact Sheets.

[h] The CyOTE team recognizes this perspective is nearly identical in principle to the "every Soldier a sensor" approach used by the U.S. Army in the early 2000s, as described by AUSA: https://www.ausa.org/sites/default/files/TBIP-2004-ES2-Every-Soldier-is-a-Sensor.pdf

Already underway is an initial compilation of Case Studies of historical OT attacks and OT-related incidents analyzed using CyOTE. Although differences exist in a historical application based on external information versus a real-time employment by an AOO, what these Case Studies lack from firsthand context they compensate for with the clarity of hindsight. Over time, the intent is to add voluntarily shared insights and Case Studies from AOOs employing the CyOTE methodology to provide a well-rounded body of knowledge with both broad insights and specific tactics. The CyOTE team expects this effort will provide actionable perception and comprehension recommendations as well as incremental improvements to the CyOTE methodology itself.

CyOTE KEY CONCEPTS

As the CyOTE methodology is focused on identifying certain occurrences of interest and developing an understanding of them in their broad context, it is essential to have a common understanding of the key concepts and terms used throughout. The concepts and terms in this shared mental model are universally applicable to all AOOs regardless of their size, business model, or resources. As concepts, they are also applicable to other sectors and industries with little to no tailoring.

OBSERVABLES, ANOMALIES, AND TRIGGERING EVENTS

First, to establish a common way to describe things happening, Figure 5 below shows the nested relationship between observables, anomalies, and triggering events.

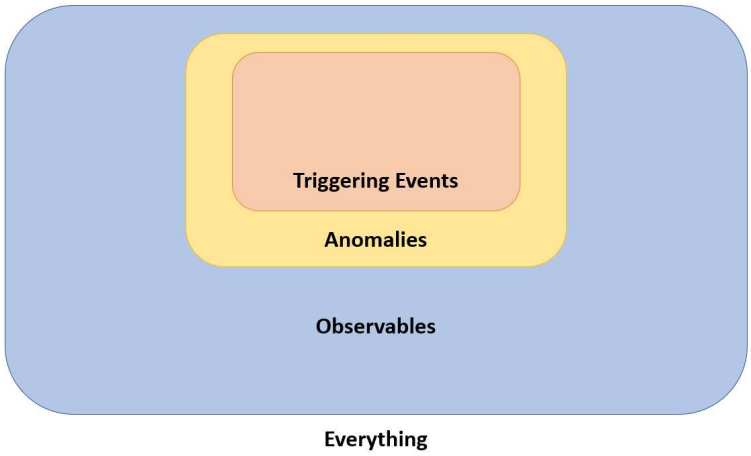


Figure 5. Hierarchy of Observables, Anomalies, and Triggering Events

An observable is the signature of an occurrence – something happened or is happening – that is able to be perceived. Depending on the facts and circumstances, an observable may be immediately comprehended with high confidence, or not yet comprehended. Most events will have a set of associated observables in more than one domain, area, or dimension; this drives

the importance of identifying and leveraging data and perspectives from operations, OT, IT, and business processes.

Anomalies are the subset of observables which deviate from what would be expected and understood as normal in the same or similar circumstances. This implies some comparison to a baseline of what constitutes normalcy, and in the frequent absence of data-driven baselines for OT environments, the baseline defaults to individual experience and organizational memory. Anomalies by definition are not presently comprehended. Anomalies can be occurrences that happened or failed to happen when expected, or they can be conditions that exist deviant from what is expected and intended for a point in time and space. The existence of an anomalous condition does imply some occurrence that produced it; for the purpose of the CyOTE methodology, it is helpful to separate those two situations as practical differences exist in how to approach the investigation of each situation.

A triggering event is an anomaly which, when perceived, initiates investigation and analysis to comprehend the anomaly. It is the first anomaly discovered in a set of related occurrences, but does not need to be (and often is not) the earliest chronological occurrence once additional investigation and analysis are underway. Triggering events in this sense are effects as opposed to causes and can be malicious or non-malicious. They are also just one point in a linked sequence of causes and effects, for which the endpoints are not yet known. The CyOTE methodology helps gain visibility on more links in the chain.

PERCEPTION AND COMPREHENSION

CyOTE uses the terms perception and comprehension as opposed to the more recognizable detection and understanding. This deliberate decision is based on a body of work undertaken by NERC's Operating Committee from 2016 to 2017, which uses Dr. Mica Endsley's 1995 model of situation awareness.[5] Although CyOTE is not designed or intended to support real-time situational awareness, the cognitive processes described in Level 1 (Perception) and Level 2 (Comprehension) as shown in Figure 6 are exceptionally well aligned with CyOTE's approach. Perception requires information and comprehension requires context.

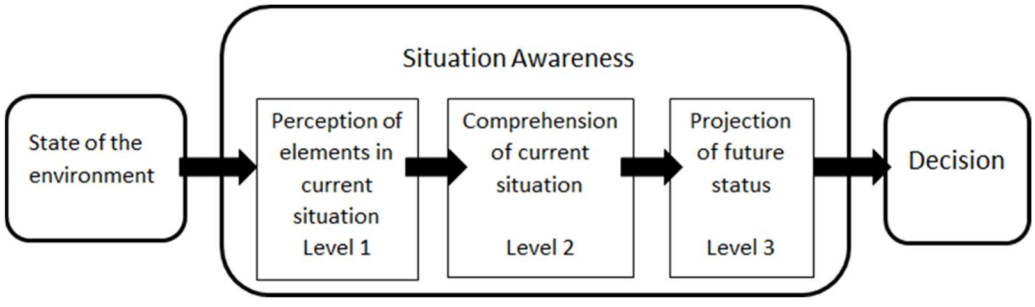


Figure 6. Endsley's Model of Situation Awareness, as Adapted by NERC[6]

Perception is the individual human ability to detect a signature of an occurrence so one or more humans are consciously aware of its existence. For the purposes of CyOTE, the term 'perception'

is a more generalized instance of the capability commonly referred to as 'detection' in earlier CyOTE programmatic references and in general cybersecurity parlance. Perception here means a signature capable of being detected by a human was actually detected; perception here does *not* mean opinion or subjective interpretation. A popular saying in the ICS security industry refers to the value of asset visibility, "you cannot defend something you do not know you have." In a similar vein, one cannot comprehend or act on an anomaly never perceived.

Perception is generally synonymous with detection for the purposes of CyOTE, understanding detection sometimes carries the connotation of automated systems, whereas perception is a deliberately human action and ability. As an example, the existence of a Supervisory Control and Data Acquisition (SCADA) alarm (an observable) never consciously seen by a human was not perceived.

Comprehension is the organizational human ability to understand an observable, in all its relevant context across the operations, OT, IT, business, and cybersecurity domains. Comprehension of anomalies usually requires one or more cycles of deliberate investigation to gather and analyze additional data, which may reveal additional anomalies. Because of the multidisciplinary approach used for a sufficient investigation, comprehension for the purposes of CyOTE is an organizational ability, not an individual one. Absolute certainty is rare in the eventual comprehension of anomalies, and the requisite level of confidence in the comprehension of an anomaly in its context necessary to make a business decision is a matter of organizational risk appetite.

Figure 7 provides a helpful mental model to think about the role of perception and comprehension relative to the popular knowns and unknowns thought framework.[i]

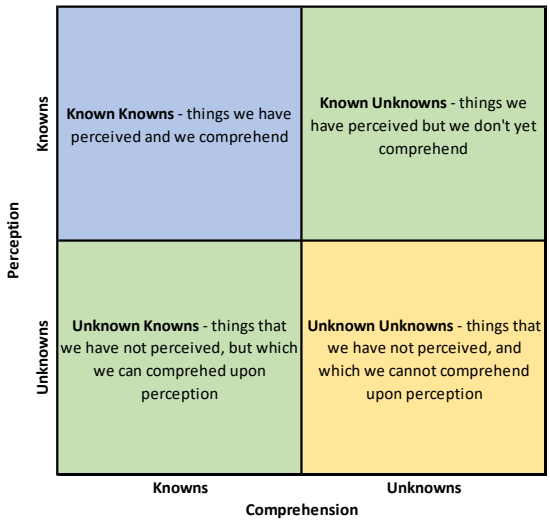


Figure 7. Knowns and Unknowns in Perception and Comprehension

[i] See https://uxdesign.cc/the-knowns-and-unknowns-framework-for-design-thinking-6537787de2c5 for a discussion and examples of the Knowns and Unknowns framework.

Anomalies as defined in CyOTE fall into the 'Known Unknowns' quadrant because something has been perceived, but is not yet able to be assessed for placement into a Known Known subcategory of either malicious or non-malicious (these subcategories are not shown in the graphic, but should be thought of as 'we are here now so what do we do given that' – which is addressed later in The CyOTE methodology). Things in the bottom two quadrants are not anomalies because they may or may not have occurred, but nobody (at least nobody from the AOO) has perceived it. By improving organizational capability to perceive anomalies – moving from the lower right to the upper right quadrant – we are in effect shrinking the volume of the unknown universe and expanding the known (perceived, not all comprehended) universe. This is depicted in Figure 8 below.

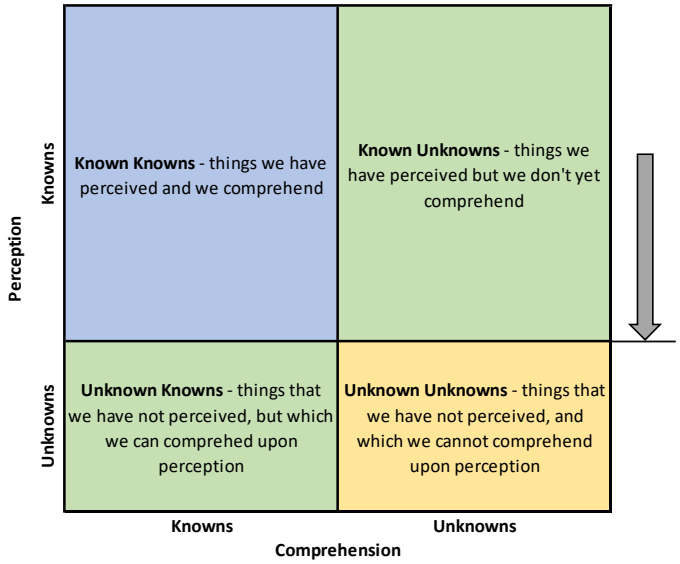


Figure 8. Reducing the Volume of the Unknown World Through Increased Perception

Recently perceived Known Unknowns can then be correlated to malicious cyber activity as enumerated using the ATT&CK Framework for ICS and detected with capabilities such as those described in the technique detection Fact Sheets or equivalent commercial solutions where those capabilities exist. Through disciplined application of a multidisciplinary process to understand perceived anomalies, and the foundational research from the Use Case and ATT&CK Framework for ICS implementation phase to explain the use of malicious techniques against a generic energy sector AOO, the volume of the unknown universe is shrinking and known (comprehended, whether perceived or not) universe is expanding. This is depicted in Figure 9 below.

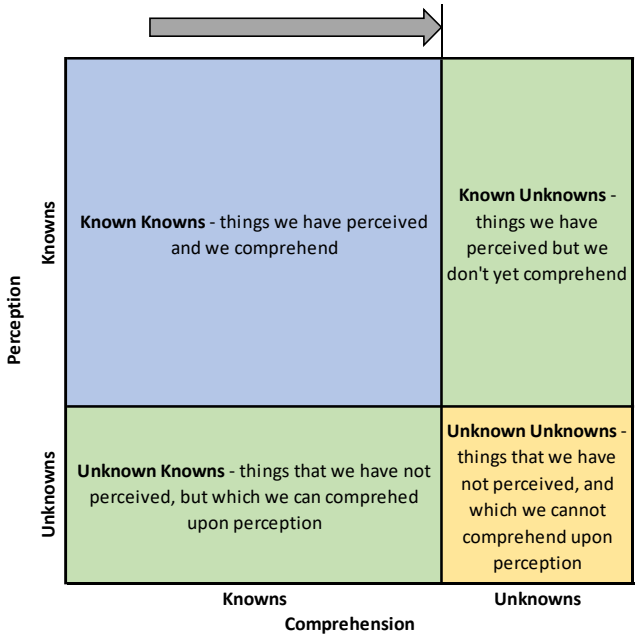


Figure 9. Increasing the Volume of the Known World Through Increased Comprehension

With this mental model of perception and comprehension in a universe of knowns and unknowns in hand, a final key concept must be understood: the Case Study. Born from the insight gained during the Use Case and ATT&CK Framework for ICS implementation activity as the enduring and focused extension of the Use Cases, Case Studies are the process and documentation of analyzing a situation using the CyOTE methodology. Case Studies differ from real-world application of the methodology in their starting point at the logical beginning of the incident as opposed to the time of perception. They can be used to retrospectively learn from noteworthy historical incidents, and also to proactively analyze prospective anomalies of interest to an AOO, whereas the CyOTE methodology is used in the present to investigate actual triggering events. Typically, the historical Case Study is based on external accounts of actual situations and conducted by a third party lacking firsthand access to information and the surrounding context that can only come from the subject AOO involved, but has the benefit of hindsight and no performance pressure.

ORGANIZATIONAL MATURITY AND CAPABILITIES

CyOTE allows an AOO to think innovatively and creatively about proactive solutions for OT security, providing a path to advance beyond more reactive traditional approaches based on monitoring to detect certain situations into a new paradigm of holistic analysis to understand anomalies across the entire organization. Although the barrier to entry and ongoing cost to use the CyOTE methodology is intended to be low, it is not a no-cost proposition. Employing the CyOTE methodology requires effort from several different functions within the organization, some of which do not have existing collaboration structures and most of which are in high demand and low supply.

This section provides an overview of seven organizational capabilities that are enablers and multipliers for the value realized by CyOTE. Although organizations exhibit variability in how they are realized given the facts and circumstances, these capabilities apply to all AOOs regardless of their size, business model, or resources. Each capability is required to some degree to be able to employ the CyOTE methodology, but greater maturity, proficiency, and comfort with each should drive greater results. Some of these enabling capabilities are well aligned with domains in DOE's Cybersecurity Capability Maturity Model (C2M2).[7]

RELATIONSHIPS BETWEEN DEPARTMENTS

The success or failure of CyOTE rests on the input and active cooperation of skilled individuals from disparate parts of the AOO organization. Perhaps more pronounced than other examples, this requirement is fundamentally no different than any other organizational effort requiring interdepartmental collaboration. Techniques already familiar to organizations to achieve this collaboration are likely to be adequate when applied to operations, OT, IT, business management, and cybersecurity in the context of CyOTE as well.

> *"This work cannot be done in a silo. Results come from the awareness and the realization that we need the right smart people in the room to be able to have these conversations and find a solution that works well for all."*
>
> *CyOTE Industry Participant, 2020*

ENERGY MONITORING CAPABILITIES AND PRACTICES

Regardless of size or business model, energy sector AOOs adequately monitor their operations (i.e., energy flow) and energy infrastructure status. Many have expansive and increasing high-fidelity visibility of their real-time operations, and advanced decision support and analytic systems on top of the foundational data. This operational information comes from SCADA alarms and telemetry, outage management systems, and asset and maintenance management systems (e.g., SAP or Maximo).

With years of designing, implementing, maintaining, and using these capabilities comes a refined understanding of how the systems and infrastructure are supposed to work, and a strong familiarity with the patterns associated with normal operations as well as some set of abnormal conditions. This knowledge is best when it exists in shared organizational consciousness, but this is built on the collective individual experience of the operators, engineers, and technicians using these systems 24 hours a day, every day, for years. The more this understanding of the system is an accurate shared mental model across more of the organization, the more efficient employing The CyOTE methodology is likely to be.

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*
>
> *Sun Tzu,* The Art of War[8]

CAPABILITY TO RESPOND TO AND RESOLVE RELIABILITY FAILURES

Similar to the energy monitoring practices described above, AOOs all demonstrate some level of capability to identify, track, and repair the mechanisms of non-malicious failures: equipment failures from old age or mechanical failures, automated systems operating in ways not anticipated by design, damage from the effects of weather and climate, failures compounded by organizational or individual human error, and so on. Without this ability to correct acute deficiencies and to manage the effective age of infrastructures on an ongoing basis, the overall system would have failed catastrophically some time ago.

Different organizations will have a variety of philosophies (e.g., routine diagnostic testing versus run-to-failure), priorities, and resources to impact the mean time to remediate a failure. Whatever this capability may be for an AOO, it represents the default choice for addressing conditions of uncertain causes. This is the null hypothesis in scientific terms, and from a causal analysis perspective it represents a response to the apparent cause, but not necessarily the root cause. Failures whose root cause is not adequately identified and addressed are likely to recur, leading to continued inefficiency and assumption of more risk than necessary.

CAPABILITY TO RESPOND TO AND RESOLVE CYBERSECURITY INCIDENTS

In today's world, cybersecurity is an inescapable aspect of doing business. The capability to respond to and recover from cybersecurity incidents is a necessity for AOOs of any size or business model. Many larger organizations have a robust in-house incident response capability, and some smaller organizations choose to outsource this capability. Others may maintain basic incident response capabilities, and outsource certain niche capabilities (e.g., malware reverse engineering) as needed.

Getting to a high-confidence, risk-informed decision on whether to declare an incident and initiate response actions is the purpose of The CyOTE methodology. Incident response is the alternate hypothesis in scientific terms and in conditions of uncertainty represents a more conservative choice from a security perspective. This capability to respond to and resolve cybersecurity incidents is well aligned with the Event and Incident Response, Continuity of Operations domain in C2M2.

UNDERSTANDING OF ORGANIZATIONAL RISK APPETITE

When the CyOTE methodology is used, there will come a point where a decision must be made based on the results of the investigation. This is a binary decision. Where inadequate evidence has been found to suspect a malicious cyber nexus, the situation will be handled through existing reliability failure processes; this amounts to failure to reject the null hypothesis. With sufficient evidence, the situation will be handled through cybersecurity incident processes. The question of how much evidence or suspicion is sufficient to reject the null hypothesis is the point of interest here.

This threshold is a direct reflection of an organization's overall risk appetite, and where cybersecurity falls in their prioritized risk register. Although it will certainly vary from organization to organization, it is helpful to have a general idea of what the internal evidentiary standard is to decide. This is best accomplished ahead of time, instead of deciding in the heat of the moment. This understanding of organizational risk appetite is well aligned with the Risk Management domain in C2M2.

> *"If you choose not to decide, you still have made a choice."*
> *Neil Peart,* Freewill[9]

CAPABILITY FOR ORGANIZATIONAL LEARNING AND CONTINUOUS IMPROVEMENT

Events initiated and driven by equipment failure and organizational and individual human error offer valuable insight into the fundamental ways in which complex socio-technical systems fail. The observed impacts of these events are part of the intended effects an adversary can focus on creating intentionally, so an organization can identify and implement improved perception capabilities to identify failure scenario precursors whether they are "normal" or intentional and malicious. Organizations should continue (or begin, if not already part of their culture) to conduct high-quality full-spectrum root cause analyses of significant reliability events, as part of or comparable to NERC's Electric Reliability Organization (ERO) Event Analysis Process.[10]

Development and implementation of barriers against recurring causal drivers can drive improved results in reliability, security, and business over time. This requires habitual analysis and trending of an organization's adverse events, however, and a feedback loop to ensure the analytical

insights are available to senior management with the authority to set priorities and allocate resources.

The ability of an AOO to detect fainter and fainter signatures of malicious activity, earlier and earlier in the kill chain over time is what continuous improvement looks like in the context of CyOTE.

> *"It's not enough to do your best. You must first know what to do, and then do your best."*
>
> *W. Edwards Deming*[11]

OT-INSTRUMENTED VISIBILITY

Visibility into network traffic and device behaviors in OT networks today is less than adequate across the sector; no matter the capability of a particular organization in this regard, there is a nearly universal desire for more. As an AOO better understands their OT environment, they may be able to correlate a smaller anomaly to a potential attack, moving the asset owner's threat detection capability earlier into an attack campaign and preventing more significant impacts to operations.

To that end, CyOTE has developed a portfolio of novel technique Fact Sheets, Proof of Concept tools, and Tool Recipes to understand how to detect adversary techniques in a few pilot environments. As CyOTE is not a tool development effort, each of these items provides generalized information for AOOs to procure and deploy their own production-grade tools and capabilities from commercial sources or in-house development. The CyOTE methodology complements these investments by providing a way for AOOs to derive more value from the data they already possess and will acquire through investments in the future.

Both sensors and a way to make sense of the sensor data are needed. The CyOTE Program does not seek to compete with the established and growing commercial sensor market, but rather to provide a way to make sense of the data. Ideally, CyOTE's insights can inform the state of the art in the marketplace. There is a relationship between the capability of OT-instrumented visibility and the Situational Awareness domain in C2M2.

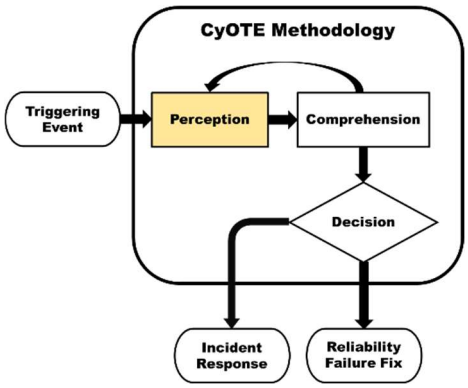
> *"The level of trust we have in our systems has to be limited by the visibility of those systems, and the level of visibility we need must match the consequences of a system failure."*
>
> *Anne Neuberger, 2021 SANS ICS Security Summit Keynote*

EMPLOYING THE CyOTE METHODOLOGY

The prior sections explain the fundamental concepts necessary to understand CyOTE, the prerequisite organizational capabilities needed to employ it, and the history of how these insights were realized. This has set the stage for an explanation of how an AOO starts to put CyOTE into practice and learns how its methodology works with the facts and circumstances of their organization.

PERCEPTION

Perception is the first active step in employing The CyOTE methodology. It provides the starting point—detection of a triggering event in the organization—for investigation during the comprehension step.



Defining a Triggering Event

As described in Key Concepts, triggering events are a subset of anomalies. Not all anomalies are created equal, but can be most generally defined as "any perceived event or lack of an expected event that failed to occur as intended and anticipated, for reasons not presently comprehended." It is important to note that it is expressed as "as intended" not "as designed" since latent error in designs can be a cause of an anomaly, and comparison of as-intended to as-designed to as-built states is useful for the comprehension stage later. In other words, anomalies are something out of the normal and triggering events are anomalies requiring further investigation because they could be a signal of the use of adversary techniques.

Proactively identified triggering events will answer the question of "what anomalies would an adversary's actions to use a particular procedure to implement a technique against my organization create?" Although the adversary techniques of interest are the same, the anomalies that could be generated will vary due to the details of an AOOs' infrastructure and operations. Likewise, it is impossible to standardize the threshold of what constitutes a triggering event resulting in deeper investigation across all AOOs. Rather, the Use Cases generated examples to inform each entity, which must then be tailored for their architecture, organizational structure, asset mix, and philosophy.

An AOO's list of identified triggering events is by necessity a living document, which must be updated as OT environments change, energy infrastructure is commissioned and retired, monitoring and control capabilities evolve, and adversary TTPs and behaviors adapt to changes in their targets and intentions. This living list is the practical embodiment of continuous improvement in an OT cybersecurity context, and also a reflection of the organization's evolving risk appetite as practice at employing the CyOTE methodology over time grows capabilities, which in turn allows the organization to perceive fainter signals, comprehend them more

efficiently, and make timely, confident decisions on whether or not to declare a cybersecurity incident and begin response procedures.

Perceiving a Triggering Event

OT systems are typically predictable in behavior in response to external conditions such as weather, with understood causal relationships behind these predictable fluctuations. Therefore, organizations typically have a well-developed understanding of what normal looks like on their system as seen through their tools and processes. At a human physiology and psychology level, perceiving an anomaly is better thought of as perceiving the absence of normal even though these are linguistically equivalent. CyOTE uses three common ways a triggering event can be perceived: programmed alarms, human pattern matching, and business process exception reporting.

Programmed Alarms

The most common initial perception is via human awareness of an automated alarm. Here, alarm is used in the broadest sense, and includes programmatic or routine manual review of logged data from process instrumentation or ICS and network devices, as well as the more common understanding of a visual or audible alarm intended to alert a human operator in near real time. Because of the nature of alarms, these situations are usually tied to an event that occurred and typically include a date and time attached to the alarm.

The success rate of this is dependent on the alarm logic being complete and correct to fire for the intended condition, and the transmission of the required data elements to make the programmed-in determination from the sampling, transduction, or tap point to where the logic engine resides with no compromise of integrity.

In the operations domain, many alarms are defined and presented to a human system operator in a control center via the HMI of the SCADA system. Most SCADA alarms feature a corresponding alarm in the substation control house and/or at the initiating device itself, usually with more details available than in the control center. Depending on the alarm, the system operator may dispatch an appropriate field employee to the facility for further investigation and response. These alarm frameworks and supporting processes are mature for their intended purposes of maintaining safety and reliability, and in the aggregate over time, also can identify anomalies other than those for which the alarms were specifically designed.

In the energy sector OT domain, however, alarms are rarely aggregated or automatically presented to a human for perception purposes. Alarming and logging capabilities do not exist on the oldest legacy devices still in significant production use, and although such capabilities are increasingly more common with newer devices, they are often not configured or used today. In these instances, the “normal” operations are more dependent on human recognition of the behavior of the systems.

Although enterprise IT is not a focus of CyOTE, as a comparison with the IT domain, alarms are defined by the network or endpoint device generating them and typically presented to a human analyst in a security operations center (SOC) or network operations center (NOC) via a security information and event management (SIEM) tool. Frequently, historical trend data is available from the SOC and NOC. In many cases, the analyst will be able to remotely connect to the initiating device for further investigation. These alarm frameworks and supporting processes are relatively mature for their intended purposes of maintaining information security for an enterprise IT system, and similar to the operations domain, can also be used to identify anomalies through analysis in the aggregate over time. AOOs employing the CyOTE methodology may benefit from adopting modified IT-centric processes and practices for their OT environments, and incorporating threat-focused perspectives more commonly found in IT professionals today.

Human Pattern Matching

Somewhat less frequent, but arguably both more powerful and less dependable at the same time, is human awareness of a situation that, based on their experience and training, is 'out of the normal' but for which there was not an automated alarm. These situations are usually tied to anomalous conditions discovered separately from the event causing them to exist.

Experienced professionals commonly perceive anomalies without the benefit of an automated alarm or a manual review of logs (which could be automated and alarmed) in two ways. The first uses a deadband – a mental model of the acceptable range of results for a given data point – compared to measured values. Assuming a sufficiently well-calibrated mental model, anything falling out of the deadband is an anomaly. Every data point has its own specific deadband parameters for evaluation. The second way humans perceive anomalies is by mentally constructing conditional statements using rules following Boolean if-then-else logic. Related conditionals can also be combined to form more complex logic to be satisfied before human perception is triggered. Much of this cognitive process is subconscious in real time.

Business Process Exception Reporting

A third programmatic way to perceive anomalies is through existing business process monitoring. This is a nontraditional approach for OT cybersecurity, but the practice of exception reporting – identification and explanation of situations where actual performance differs significantly from expectations – is a common business tool. It is most commonly used in accounting and key performance indicators, but in principle can be applied to almost any measure for which data is periodically collected and assessed.

Exception reporting is a type of detective internal control. As such, it is reactive when used as designed, but the anomalies perceptible through exception reporting processes precede the principal harm when it comes to OT cybersecurity, consistent with the ICS Kill Chain. A body of knowledge does not exist to reference here, but possible measures of interest could include increased telecommunications usage, changes in the patterns of service calls, or increased ordering of parts suggesting elevated failure rates. Arguably closer to enterprise IT than business

operations, routine audits of user and administrative accounts, privileges, access logs, and other measures are similarly worthwhile measures to monitor.

The goal of anomaly perception through business process exception reporting is to move the sort of "hindsight is 20/20" recognitions further to the left. Surveying existing business reporting processes and making the results available to those responsible for OT and IT security in the organization is a reasonable first step to develop such capabilities. Identifying information of potential interest generated in the course of ongoing business, and where it is created (and archived, if applicable) would likely come next to permit manual analysis if needed. A significant amount of this exception reporting can be automated using commercial software packages. The challenges in doing this are identifying the measures worth automating, and then developing a baseline of expected results for comparisons.

Who Else Needs to Know?

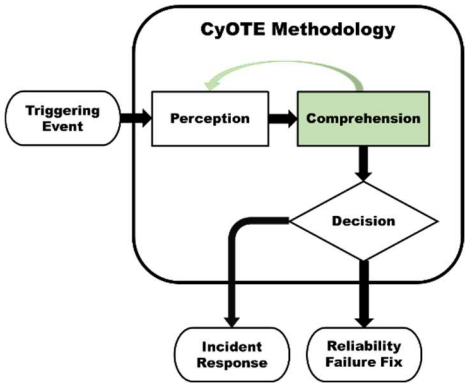
As perception is an individual human activity, transitioning this awareness from the individual to the organization requires a necessary step: reporting and notifications. Although most organizations support an established chain of communications, experience has shown existing communications are inadequate to involve all the necessary groups to investigate triggering events.

An AOO employing the CyOTE methodology should identify the key individuals and departments possibly involved in investigating a triggering event – including, but not limited to those with responsibility for operations, OT, IT, and business processes – and develop a process to notify these points of contact whenever triggering events are perceived.

Beyond triggering events, anecdotal evidence from CyOTE Program participants suggests some departments in otherwise successful organizations maintain less than adequate awareness of relevant occurrences perceived in other departments within the organization. More research and experience are needed to make a confident recommendation in this regard to find a generally acceptable balance between proactive notification of occurrences that could be a triggering event with the added context of other departments, and further loading already strained resources with additional information of infrequent value.

COMPREHENSION

Perception is necessary, but perhaps the easier piece of CyOTE, and arguably of cybersecurity in general. Understanding the nature and possible origins of the triggering event and expanding to develop deeper comprehension and broader awareness of the overall context in which that triggering event came to be—to the point an organization has sufficient confidence to make a risk-informed decision on whether or not to declare a cybersecurity incident and begin response procedures—is the decisive point.



Getting to the risk-informed decision point is a pervasive challenge, however. It is individually and organizationally tempting to take the path of least resistance and choose to categorize anomalies as reliability failures without expending the resources to comprehend the broader context around the triggering event. The significant majority of anomalies do not have malicious causes, and a segment of the industry dismisses the notion an adversary could be behind any anomaly. This is a concerning situation, because advanced adversaries intentionally engineer their activities to leave very few clues, but there is always a faint residual signature that cannot be completely explained away. In this sense, adversaries use our sense of economic stewardship to not "waste resources looking for ghosts" to help the faint but unescapable traces of their presence continue to be not comprehended as malicious.

To build comprehension, an AOO must first identify useful elements of data and information, who in their organization owns the information, and how it can be accessed. Next this information is used to build context around the triggering event and identify questions and related anomalies from the triggering event. From this point, the AOO pivots to investigating these new questions and anomalies in a recursive process.

Sources of Additional Information: Who, What, and Where

To adequately understand the anomaly will likely require data from systems under the control of different departments, and collaboration with practitioners from those departments to correctly interpret the data. Experience in CyOTE and in other real-world and experimental and exercise conditions has consistently shown developing comprehension around an anomaly is most effective and efficient when small core teams of full-time system operators, OT technicians, and cybersecurity analysts from different departments come together to purposefully focus on the problem in the context of their shared organization. In fact, one of the main indicators further investigation is needed is that no single expert, armed with only their department's data sources, can completely and confidently explain an anomaly.

A psychologically safe environment[j] where operators, analysts, technicians, and management alike all feel free to provide well-intentioned input including bad news without fear of reprisal or being ignored, will empower this information gathering process. Many laypeople describe an organization with an enduring environment of psychological safety as having a healthy culture. If the organization lacks this safe environment, limited opportunity exists to create it from scratch during the course of an investigation, but each engagement will either reinforce or incrementally alter the existing culture.

Although the names vary between organizations, System Operations, Engineering, and Cybersecurity departments should all be involved in the investigation.

System Operations Departments – including both control center and field operators, and real-time engineers – should be one of the first sources consulted. Common industry practice likely will have driven the routine production of manual logs, notes from field personnel investigations, or other records if the anomaly involved a disruption in the system above some established threshold. Although these notes are rarely sufficient to adequately comprehend an anomaly for the purpose of the CyOTE methodology, they often provide a useful frame of reference to define the scope and identify questions to guide the investigation. Even without documentation, the collective understanding of normal and abnormal behavior of the organization's portion of the larger grid is useful. Traditional interviews and discovery methods – "let the operators vent and talk" – are often useful because operators frequently know more than they believe they know, and unstructured discussion helps draw out knowledge. This applies to the entire team with knowledge of the systems related to the anomaly, not just the shift supervisor and department manager. Gaining clarity and confidence in core issues usually involves asking the same questions several times in different ways; listen for and expound on the "what if" statements.

Engineering Departments – in this context, meaning those responsible for the design, construction, and maintenance of the ICS infrastructure allowing System Operations to operate the energy infrastructure – can provide unique insight into the environment. Their knowledge of how the system was designed and commissioned for operation most accurately describes normal and abnormal conditions in the context of both network and OT data. Their expertise is required for both the OT communications network and the configuration and operation of the ICS devices on the network.

Cybersecurity Departments – those responsible for the confidentiality, integrity, and availability of the organization's digital assets provide the threat-informed perspective and bring experience and capabilities to analyze situations and data for security issues. Across the energy sector today, there is no single consistent name or organizational construct for the Cybersecurity department, nor a consistent scope of responsibilities and authorities. Identify and enlist the support of those with responsibility for security of OT environments as well as those with knowledge and

[j] See https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Group_Performance/Edmondson%20Psychological%20safety.pdf for more information on the importance of psychological safety to team learning.

experience of adversary behaviors and the investigation of them, however they are aligned in the organization.

Since access to raw data typically requires coordination with human organizational oversight, it is typically better to pursue information and context from different departments within the organization, and when needed have them provide the identified data under their control for shared analysis. These datasets can come in many forms, but from the AOO's perspective for an OT domain observable full packet capture (PCAP) data from network tap points with visibility of the device where the anomaly was perceived, complete device logs (everything that is generated), and netflow data are all valuable sources of information. For observables in the operations physical domain for an AOO example, digital fault recorder (DFR) data including sequence of event recording and oscillography from a point with electrical visibility of the anomaly, discrete event and time-series historian data, and SCADA alarm logs are valuable.

Building Context Around the Anomaly

Anomalies come in many shapes and sizes, so it is counterproductive to follow a one-size-fits-all approach. Comprehension is not a checklist, but rather the creation of a shared mental picture used to form a hypothesis about the non-deterministic world. Although the groupings of the more specific example questions in Appendix B: Questions for Comprehension may appear as a checklist-based approach because of the format, it is important to realize applying it with such a deterministic approach will likely fail to deliver the needed comprehension. For the first pass through this step of the CyOTE methodology these processes apply to the triggering event, and these same comprehension processes apply recursively to additional anomalies discovered while investigating the triggering event.

These groupings of questions should be thought of more like different batteries of medical tests experienced specialist physicians can use to help diagnose a patient whose symptoms are clearly perceived, but not yet comprehended in the context of the patient's particular facts and circumstances[k] – do they have a disease, and if so, what is it? No single list of questions about an anomaly will provide sufficient information to be able to determine if the anomaly has a malicious nexus, and if so, what it implies (i.e., what adversary technique(s) could it map to in the ATT&CK Framework for ICS).

At this point, the organization needs to start a documentation and knowledge management process instance in support of their investigation. Recording and organizing the datasets and contextual information discovered in some logical manner will not only improve the efficiency and effectiveness of the investigation, but will also prevent duplication of effort by those responsible for the eventual resolution action whether that is incident response or reliability failure management.

[k] *How Doctors Think,* by Jerome Groopman, MD, inspired the author's understanding of this challenge. https://www.amazon.com/How-Doctors-Think-Jerome-Groopman/dp/B0029LHWKY

Start with a determination of what was actually perceived in the triggering event. Was it a change in:

- the physical domain (something involving telemetered quantities such as voltage, current, frequency, pressure, flow, volume or temperature, or the physical configuration of a piece of infrastructure); or
- the OT domain (something involving traffic or signals transiting a communication medium, or the logical configuration of a piece of infrastructure); or
- both the physical and the OT domains?

Given the determination of a physical or OT starting point, identify what expected corresponding perceptible observables would exist in the other domain and search for their presence or absence. For example, a circuit breaker physically changing state from closed to open in the physical domain would be expected to have either a relay target set in an associated protective relay, or a manual 'open' command from either local or remote control, and a corresponding SCADA alarm message in either case in the OT domain. Similarly, a DNP3 message requesting a select and operate of a circuit breaker in the OT domain would be expected to have a corresponding physical operation of the circuit breaker, an associated change of local electromechanical indicators including semaphores and status lights at the breaker control and local control house, and a record of the breaker operation command in system operator logs. Consistency between the anomaly as perceived in the first domain and the presence of the expected corresponding signature in the other domain is an indication a potential malicious nexus is beyond the present scope of comprehension, but not necessarily a nexus does not exist.

From this point, several general questions will provide insight into where to look next, based on how the actual answers compare to what would be expected in similar known-good circumstances. They should be augmented by other investigative and cause analysis techniques familiar to the organization. NERC's *Cause Analysis Methods for NERC, Regional Entities, and Registered Entities*[12] provides a helpful survey of the most familiar techniques. A selection of representative questions for use is included as Appendix B, intended to give a better idea of extent-of-condition and apparent causal relationships at a point in time.

There are two goals sought from the information gained through asking such questions. The first is to form a rebuttable hypothesis for what technique implementing which tactic (a technique cell on the ATT&CK Framework for ICS tactics and techniques) this anomaly maps to, keeping in mind for physical anomalies this could require significant generalization given the sector-agnostic design of the ATT&CK Framework for ICS. In some circumstances, such a confident hypothesis cannot be formed; although this suggests a potential malicious nexus is beyond the present scope of the anomaly as presently comprehended, it is not sufficient to rule out the existence of such a nexus.

The second goal, more important to driving the process forward and not dependent on whether the first goal was met, is to enumerate all the lines of questioning identified through this stage of the analysis of the anomaly. At this point it is particularly helpful to begin a node and link

diagram from the information documented in the knowledge management processes to help visualize relationships between observables; this observables linking diagram is colloquially referred to as a "worm diagram" in the CyOTE Program. The triggering event is the first node, with all its related observables radially connected to it; it includes both those observables confirmed and those expected but not found, with some sort of visual discriminator between presence and absence (e.g., solid or dashed lines). The triggering event(s) is highlighted if it is believed to be the implementation of a specific adversary technique, that is, the first goal from the information gathering process described above was met. Links emanating from the triggering event representing the as-yet-unanswered questions considered are included, as well as links and additional nodes for answered questions that confidently satisfy the extent of a particular line of inquiry. A notional example of this diagram, for an investigation in progress, is shown in Figure 10.

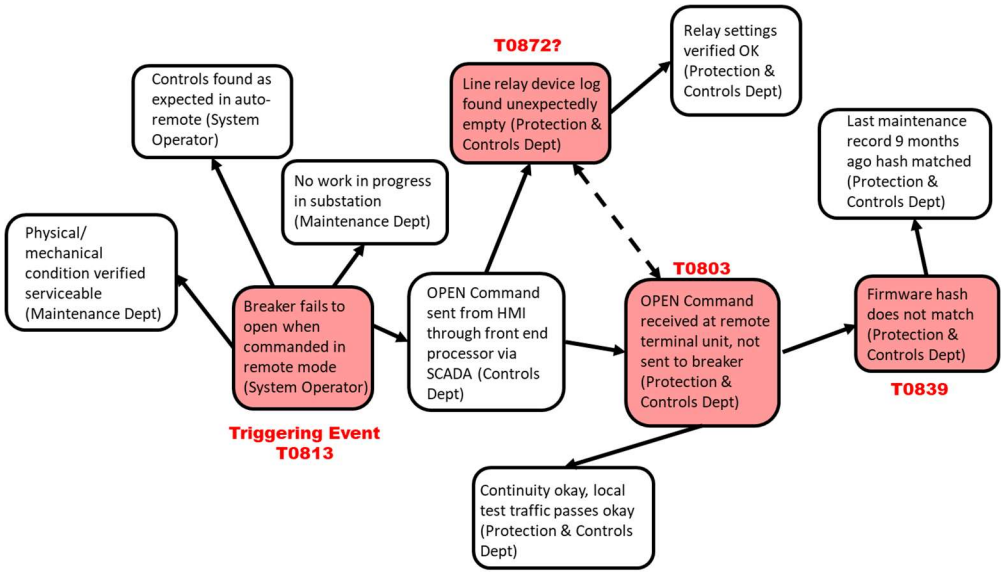


Figure 10. Example CyOTE Observables Link Diagram

Pivoting to Discover Related Anomalies or Show Their Absence

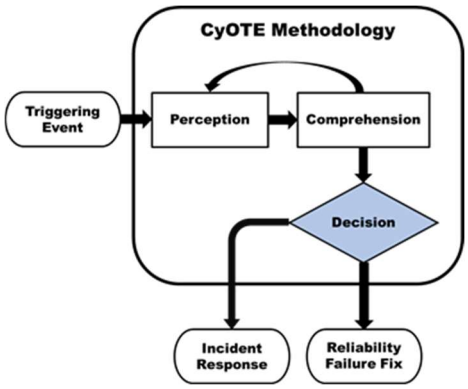
When a triggering event has been comprehended sufficiently to determine its mapping to a technique, the next step is to is repeat the steps above starting from each of the lines of questioning resulting from analysis of the triggering event. The importance of recording and organizing the information discovered in the comprehension process and visualizing it through a node and link diagram becomes exponentially more important as the triggering event expands into a web of postulated, confirmed, and denied relationships between anomalies.

When the presence of a second ATT&CK Framework for ICS technique (or other anomaly the organization would have considered as a triggering event, had it been the first to be perceived) is identified and mapped, another line of effort becomes available. This is an opportunity to compare the two techniques and consider whether an apparent connection between them exists. This should be analyzed from the technical perspective looking at connectivity and device

behavior, as well as from the adversary perspective looking at a plausible sequence of steps in a specific attack campaign. There is not a prima facie assurance the two techniques are sequentially adjacent, and there could be other steps not yet perceived or comprehended to potentially link the two.

This process of pivoting from questions developed in analyzing an anomaly to starting the anomaly comprehension process anew from the starting point should be repeated as needed. Where supported by the data, it may be useful to deliberately switch between the physical and the OT domains in this process of pivoting and expanding. With each iteration through this process, update the node and link diagram to expand the window of visibility into the situation.

ENABLING THE DECISION POINT



The recursive process described above is not intended to be endless. There must come a point to halt this process and make a risk-informed business decision on how to proceed. This decision may be best understood by visualizing the worm diagram of identified techniques, and those occurrences that do not map to an ATT&CK Framework for ICS technique. The presence of one instance of a single technique may be relatively inconsequential in the big picture, but the overall coherence of three or more techniques that do not contradict any un-mapped observations may present compelling evidence of malicious cyber activity.

In the real world, these determinations are unlikely to be clear cut, so the decision may be more of an evolving art form than a hard science. The level of comprehension and detail needed to make the decision will vary from company to company and may be related to resource availability. The length and consistency of a discovered and comprehended worm diagram representing a prospective kill chain fragment needed to decide to proceed with incident response will also vary based on a company's risk tolerance, as discussed earlier.

"The Red Pill" – Incident Response Process

In situations where there is sufficient belief the anomalies perceived and comprehended indicate possible malicious cyber activity, the appropriate organizational action is to initiate their cybersecurity incident response process according to organizational policy and procedures. The information and context developed through CyOTE will be useful to incident handlers for developing and implementing appropriate mitigating actions.

Although conducting incident response has a cost, the expected return on that cost is the restoration of trust in OT/ICS that are critical for safety and reliability. This choice could be seen as a demonstration of due care for security.

"The Blue Pill" – Corrective Maintenance Program

In situations where a plausible indication of malicious cyber activity cannot be established, or is confidently disproved, the null hypothesis of a non-malicious failure cannot be rejected and the appropriate organizational action is to address any deficiencies discovered through corrective maintenance and work management processes according to organizational policy and procedures. It is worthwhile to maintain records of these situations for future reference and comparison to subsequent anomalies.

CASE STUDY EXAMPLES

Case Studies support continued learning through analysis of incidents and events. Some of the richest and most detailed Case Studies are expected to be produced by AOOs who have employed the CyOTE methodology to perceive and comprehend actual triggering events in their OT environments, with the benefit of unfettered access to the best data and context. To bootstrap the learning process and complement anticipated AOO-generated Case Studies, the CyOTE team has begun compiling Case Studies of historical OT attacks and OT-related incidents.

These historical Case Studies are based on publicly available reports of the incidents from media outlets and cybersecurity firms instead of the full context and data that an AOO would have. They are not, nor are intended to be, completely comparable in detail or structure, nonetheless they each provide examples of how key concepts in the CyOTE methodology look in the real world. Perhaps more importantly, these historical incident Case Studies inform learning from the perspective of "how could this have been detected?" instead of "why was this missed?" to grow the body of knowledge on perception, comprehension, and organizational capabilities.

After reviewing a Case Study, AOOs should consider how a similar scenario could unfold in their operating environment, determine the level and location of visibility necessary for them to perceive the triggering event and other anomalies, and identify accessible information sources to build comprehension. The following questions for reflection and discussion can help AOOs prepare to employ the CyOTE methodology in their organization.

- Could you perceive a similar triggering event in your organization? How would it be perceived, and by whom?
- What observables exist that could have been perceived earlier than the triggering event was? How would each be perceived, and by whom?
- Who will you contact from the System Operations, Engineering, and Cybersecurity departments to build comprehension? Would they be willing and able to assist today?
- How much evidence would you need to confidently reject the null hypothesis of a reliability failure, and initiate cybersecurity incident response procedures?
- Who else in your organization needs to be aware of the outcome?

CASE STUDY: OLDSMAR, FLORIDA WATER TREATENT PLANT INCIDENT

On February 5, 2021, an unidentified attacker gained control access to change chemical concentrations of the water supply for nearly 15,000 people at the Oldsmar, Florida water treatment facility. The attacker gained access through a TeamViewer account, which allows remote use of the computer controlling chemical content of an underground water reserve.[13]

The attack occurred in between employee maintenance periods and was discovered when an operator noticed a second occurrence of un-commanded and unusual mouse cursor movement on the computer screen. Although the operator had observed this earlier in the day, there was a lack of comprehension that this was malicious, and it was not registered as being a triggering

event requiring further investigation. The attacker accessed and manipulated the plant engineering and automation systems, and took action to increase sodium hydroxide levels to unsafe levels.[14] Upon observing this a second time, the operator took swift action to restore the process to correct parameters, and the organization initiated its cybersecurity incident response process.

Perception - Triggering Event: The triggering event for this incident was the operator perceiving un-commanded and unusual mouse cursor movement changing a critical process setting. In this incident, an individual human operator actually perceived abnormal mouse cursor movement twice, but it was not recognized as abnormal and thus a triggering event until the mouse movement resulted in an inappropriate change to sodium hydroxide levels. Reportedly, it was not uncommon in the organization for an authorized remote user to briefly take control of the HMI to check readings without notifying the operator beforehand, so the addition of inappropriate actions elevated the mouse movement from an event to a triggering event. This highlights the fact individual baselines of what constitutes normal activity will vary from organization to organization.

Comprehension: The Oldsmar incident involved the use of adversary techniques from two of the three CyOTE Use Cases – Remote Logins and HMI. Four techniques, used in series, were identified as part of this relatively simple incident. These techniques, in chronological sequence as employed by the adversary and not in order of detection by the victim, are shown in Figure 11.

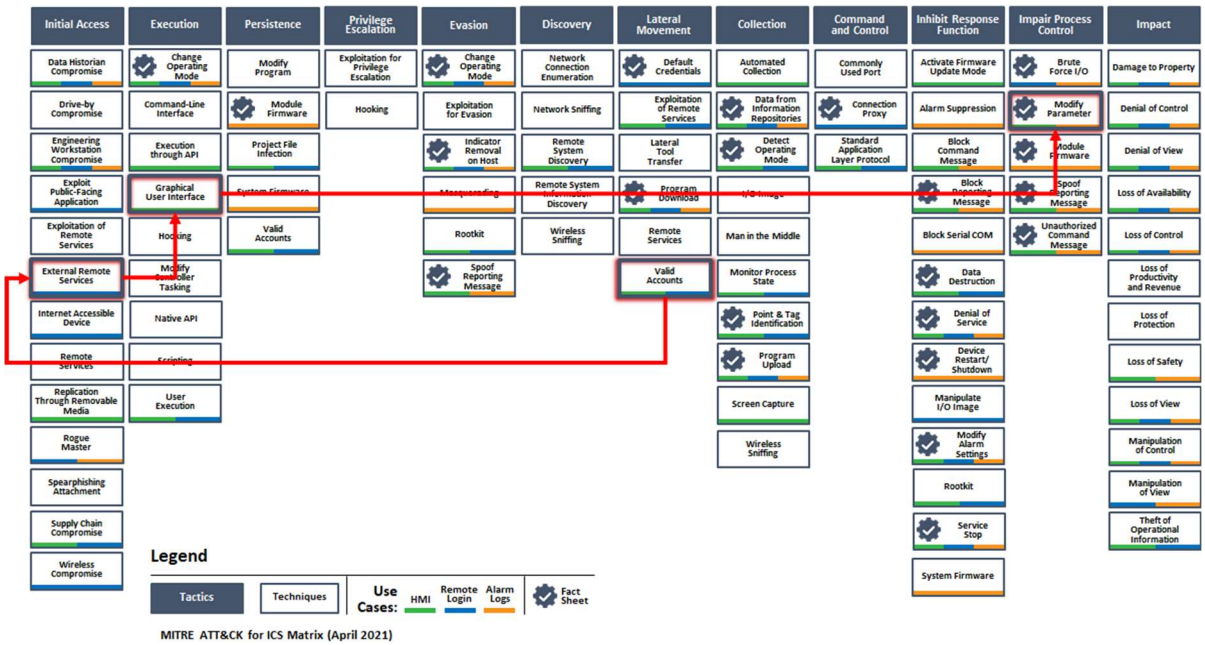


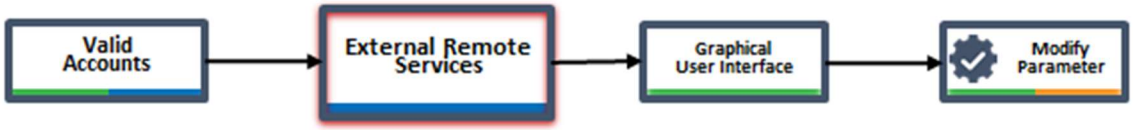
Figure 11. Oldsmar Incident Adversary Techniques Chain

Anomalies, possible related adversary techniques, and example perception methods for the anomalies are detailed below.

Anomaly: Oldsmar passwords were discovered in a password data leak that occurred days prior to the attack.[15]

Technique: Valid Accounts. An attacker gained access to the HMI system using valid user credentials.

Perception Opportunities: Account breach detection services could have alerted the AOO to compromised credentials, which could then be used to alert operators to intrusion attempts if used. A security audit also may have revealed password sharing between employees and services.



Anomaly: With a valid credential, remote access may not appear anomalous on its own.

Technique: External Remote Services. The attacker used the stolen credential to remotely access the system.

Perception Opportunities: Anomalous behavior may be revealed as an unknown source IP, multiple users from the same source IP, one user from multiple source IPs, or a user with valid access pivoting to use the control network in ways not intended or authorized. Remote service logging and monitoring, or VPN host scans or health checks may aid in detection.

Anomaly: Equipment was operated from the HMI, with impacts to the process being controlled, which was not initiated by the control room operator or by an otherwise expected remote access user. This anomaly was the triggering event in this Case Study.

Technique: Graphical User Interface. The attacker used remote access to gain control of the HMI system.

Perception Opportunities: Human operators may identify an uninitiated change on the HMI by observing mouse movement. A more sophisticated attacker may operate the system using keyboard and minimize mouse movement to avoid detection.

Anomaly: The target level of lye in the water treatment facility was raised from 100 to 11,100 parts per million.

Technique: Modify Parameter. The attacker modified an operational parameter outside of safe limits.

Perception Opportunities: Human operators may identify an unexpected change, alarms from the HMI or historian could indicate an out-of-bounds change, automated or human consistency checks with redundant systems could reveal a discrepancy, or downstream alarms from the physical environment could detect the process effects of the change (here, unsafe chemical levels in the water).

CyOTE Proof of Concept Tool: The T836 Modify Parameter uses the ConfigEngine monitors directories and files for modifications. ConfigEngine, one of the Structured Threat Observable Tool Set (STOTS) tools, monitors directories and files for modifications. ConfigEngine uses a custom script to periodically remotely connect to a device, download a user-defined file, and compare it for any changes. If a change is identified, ConfigEngine will generate a Structured Threat Information Expression (STIX™) object and transmit it to the STIX™ monitor.

Decision: Oldsmar's water treatment facility leadership decided this was a cybersecurity incident and initiated their response procedures. In this case, the decision point was reached as soon as the triggering event was perceived, due to the obvious malicious nature of this particular triggering event.

CASE STUDY: TRITON PETRO RABIGH INCIDENT

In June 2017, a section of the Petro Rabigh refinery complex in Rabigh, Saudi Arabia shut down as a result of a Safety Instrumented System (SIS) controller entering a failed "safe state." Since there was no apparent reason for the shutdown, the AOO conducted further analysis.[16] Testing and analysis of a "glitchy" Triconex SIS controller was conducted onsite and in a California laboratory. These analyses drove a review of logs from the plant and determined that the failure was mechanical in nature.

The same incident reoccurred in August 2017, again causing operations disruptions. This prompted engineers to conduct a more thorough causal analysis. Identification of unusual communications beaconing between the complex's IT environment and engineering workstations located in the OT environment were the key to uncovering an ongoing cyber campaign targeting the complex's Triconex SIS controllers.[17]

Perception - Triggering Event: The triggering event for this incident was the discovery of unusual network traffic between the complex's IT environment and engineering workstations in the OT environment subsequent to investigation of the second instance of a shutdown of a section of

the plant with an SIS controller in a failed state. This apparent beaconing traffic was the revelation that changed the effort from an investigation of a repeat equipment failure to an investigation of a security concern.

Comprehension: The Petro Rabigh incident involved the use of adversary techniques from all three CyOTE Use Cases – Alarm Logs, Remote Logins and HMI. Nineteen techniques across six series-parallel steps were eventually identified as part of this complex and protracted attack campaign. These techniques, in chronological sequence as employed by the adversary and not in order of detection by the victim, are shown in Figure 12.

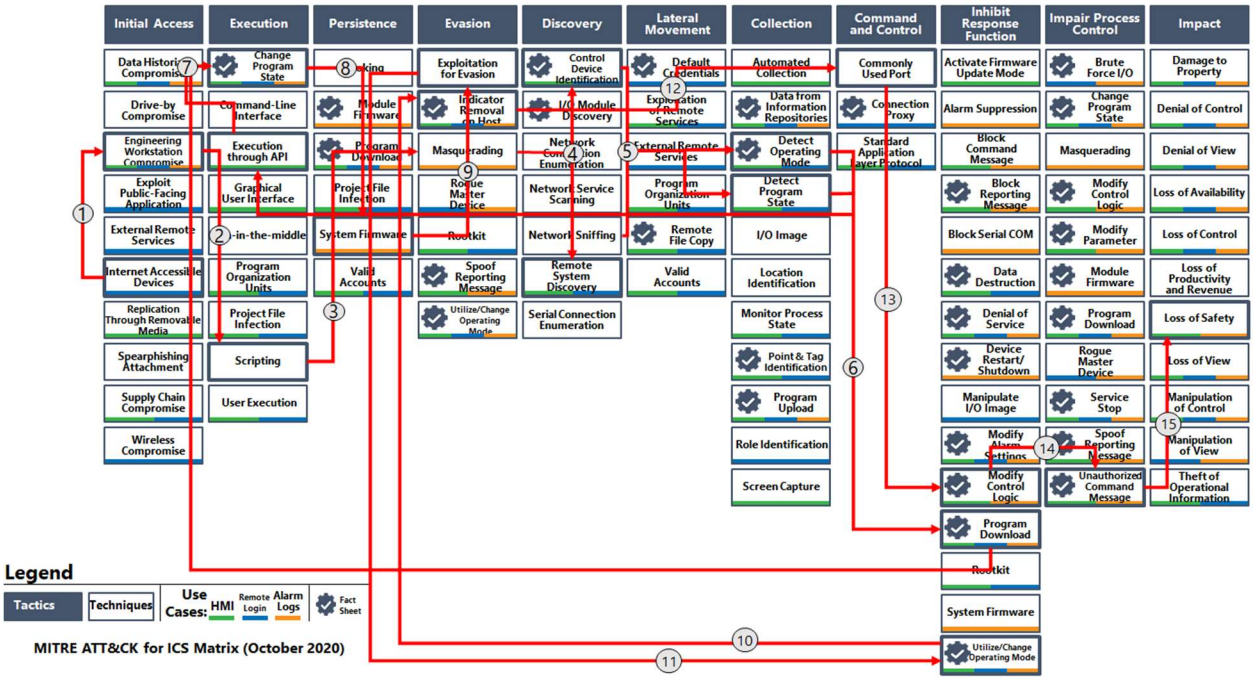


Figure 12. Petro Rabigh Incident Adversary Techniques Chain

Anomalies, possible related adversary techniques, and example perception methods for the anomalies, broken down by general adversary campaign steps, are detailed below.

IT Network Compromise

Anomaly: Increased demilitarized zone (DMZ) traffic between IT and OT networks and beaconing coming from the control network. This anomaly was the triggering event in this Case Study.

Anomaly: Anti-virus software alerted to the presence of the MIMIKATZ credential harvesting tool in the IT network.[18]

Anomaly: Employee phone numbers modified from expected numbers.

Technique: Internet Accessible Device. Remote attackers gained access to corporate computers through a poorly configured firewall, then pivoted to OT networks.

Perception Opportunities: Investigating identified attacks against IT assets for potential to traverse networks. Verifying modifications to important employee information. Monitoring traffic between networks. Assessing new or unusual connections such as Remote Desktop Protocol sessions.

Movement to OT Network

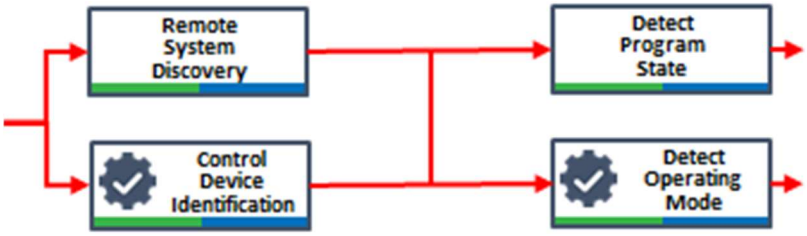
Anomaly: Unfamiliar Py2exe compiled binaries present in an OT environment.

Technique: Engineering Workstation Compromise. "The attacker gained remote access to an SIS engineering workstation and deployed the TRITON attack framework to reprogram the SIS controllers...The malware was delivered as a Py2exe compiled python script dependent on a zip file containing standard Python libraries, open-source libraries, as well as the attacker-developed Triconex attack framework for interacting with the Triconex controllers."[19]

Technique: Masquerading. The name of the Triton malware, "trilog.exe", mimicked the legitimate Triconex Trilog application.

Perception Opportunities: Periodic endpoint scans for unexpected or inappropriate file types or locations.

OT Attack Capability Development



Anomaly: IP addresses for Triconex SIS were discovered in malware code.

Techniques: Control Device Identification, Remote System Discovery. The malware on the engineering workstation contained the ability to send a UDP broadcast packet to identify Triconex devices on the network. This functionality was not used, however, the IP addresses for the Triconex devices were input directly indicating the adversaries had already obtained the IP addresses.

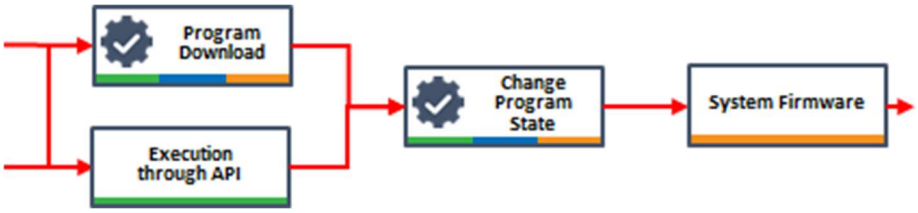
CyOTE Proof of Concept Tool: The T808 Control Device Identification Proof of Concept Tool logs the use of network traffic which can be used to fingerprint or identify a control device. This capability could be leveraged by the AOO to support the Triconex protocol and the broadcast

packets used in this attack. The AOO could use the Control Device Identification tool to monitor supported devices and protocols through either live (via a span port) or recorded (via PCAP files) network traffic. The Proof of Concept tool allows an AOO to define a list of hosts allowed to communicate with a device, such as an engineering workstation.

Techniques: Detect Operating Mode, Detect Program State. The script contained a function which collected key and operating states, and other project information.[20]

CyOTE Proof of Concept Tool: The T868 Detect Operating Mode Proof of Concept tool performs deep packet inspection of Modbus protocols to alert when a "read register" command is identified for the operating mode register. An "allow/deny" configuration file is used to filter alerts from approved hosts and flag unapproved host commands. This capability could be leveraged by an AOO to support the Triconex protocol and command used to detect the operating mode of the device.

OT Attack Capability Delivery



Anomaly: Unexpected shellcode was present on six Triconix SIS controllers.[21]

Techniques: Execution through API, Program Download, Change Program State. A script uses the TriStation protocol for program download, allocation, and modifications. The program was transferred to the Triconex device multiple times overwriting with an empty program checking and then overwriting with the malicious program.

CyOTE Recipe: The T843 Program Download Recipe guides an AOO through the development of a network monitoring capability to detect traffic which would download a device's program. The current capability outlines the process an AOO should consider when building a tool to analyze the OT network traffic and through deep packet inspection to identify potential indicators arising from an attempt to download the program.

CyOTE Recipe: The T875 Change Program State Recipe describes a capability to read and analyze network traffic captures based upon set criteria, located in a separate configuration file. The criteria compare protocol layer fields to static values (e.g., MAC and statically defined IP addresses of hosts). The Recipe identifies the need to alert on trusted IP lists for unauthorized traffic detection, monitors for PLC program download commands from unauthorized host(s), and controllers' running programs forced to a new state (e.g., reset, start, halt) from an operator or engineering workstation

Technique: System Firmware. Shellcode containing two parts, one for running on the system and another for command and control, was injected.

Supporting Attack – Hide

Technique: Exploitation for Evasion. Triton malware disables RAM/ROM consistency checking.

Technique: Utilize/Change Operating Mode. Triton malware only affects controllers left in "Program Mode." Once installed, however, it modifies the system to allow code to ignore key-switch position.

Technique: Indicator Removal on Host. Triton malware attempts to reset the controller to a previous state. If this failed, it would write a dummy program overwriting the malicious program.

CyOTE Recipe: The T872 Indicator Removal on Host Recipe provides industry standard remote process monitoring, remote log aggregation, and best practice host-based access control configuration. The Recipe identifies remote process and log monitoring via a SYSLOG messaging service or a host-based agent, depending on the host's capabilities. The Recipe highlights the data collected and analysis using Elasticsearch and potential alerts resulting from finding indicators of compromise using Kibana messaging.

Technique: Commonly Used Port. The malware communicates with the implant on the Triconex device using specifically crafted legitimate network packets.

OT Attack Execution and Impact

Anomaly: A portion of the plant shut down with the SIS controller in a failed state.

Technique: Modify Control Logic. The malware can reprogram the SIS logic of the Triconex device to trip or shutdown while in a safe state, or conversely to not trip and continue running to allow unsafe conditions to persist.

CyOTE Recipe: The T833 Modify Control Logic Recipe guides an AOO on analyzing OT network traffic and uses deep packet inspection to identify potential indicators arising from an attempt to modify control logic.

Technique: Unauthorized Command Message. An adversary can manipulate the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately.

CyOTE Proof of Concept Tool: The T855 Unauthorized Command Message Proof of Concept tool reads a network traffic capture and analyzes it based upon a set of criteria defined in a separate configuration file. The criteria compare the protocol layer fields to static values, alerting on trusted IP lists for unauthorized traffic detection, and validating the CIP protocol. The tool output provides statistics about triggered criteria, such as number of times triggered, which packets caused the trigger, data about the network streams, and which network streams included the full protocol cycle or only a part. The protocol validation summary also identifies the packets associated with validation (or lack thereof).

Technique: Loss of Safety. The malware has the capability to reprogram SIS logic allowing unsafe conditions to persist or to allow an unsafe state while using the distributed control system (DCS) to create an unsafe state or hazard.

Decision: Petro Rabigh's leadership decided this situation was a cybersecurity incident and initiated their response procedures. Without the firsthand knowledge and records an AOO would have, the specific point in time this decision was reached is not known, but generally understood to be shortly after the perception of the triggering event.

CASE STUDY: NON-MALICIOUS MEMORY EXHAUSTION

The following case study is based on events which took place during the September 2020 iteration of the Defense Advanced Research Projects Agency's (DARPA) Rapid Attack Detection, Isolation, and Characterization Systems[22] (RADICS) experiment, conducted with the support of DOE. The overall RADICS storyline assumes an adversary actively countering AOO efforts to restore power in a blackstart scenario 30 days into a protracted outage. As a unique aspect of this Case Study, through experience in RADICS up to this point, participating AOOs were conditioned to presume most anomalies perceived were due to a cyber threat in the experiment, instead of collecting information and analyzing the situation to determine a likely cause. This scenario event did not directly affect any specific participant.

During the experiment, an AOO's control center unexpectedly lost communications with the automation controller device in a substation. Power-cycling the unresponsive device did not resolve the problem, so a technician was dispatched to the substation to investigate. Following seven different threads of troubleshooting, the AOO ruled out potential use of 18 adversary techniques with sufficient confidence to decide the loss of communications was a reliability failure and not the result of malicious cyber activity. At this point, an onsite device original equipment manufacturer (OEM) representative was brought in and determined the device had lost communications because its memory was full due to a failure of the local log rotation routine. The AOO had focused its troubleshooting on the communications path instead of the device, likely lengthening the time required to reach a decision on response actions. Forensic analysis by the OEM determined a prior software update had been unsuccessful and resulted in a specific log file ceasing to rotate once it exceeded a certain file size; because this log file is infrequently written to, it took several months for the non-rotating log file to grow large enough to consume all the storage on the device.

Perception - Triggering Event: The triggering event for this situation was the loss of communications between the control room and a remote substation automation controller. Of note, although this anomaly initiated further investigation, field devices temporarily losing communication is not typically a noteworthy event in and of itself. The experimental context and environment likely drove the AOO to use a somewhat lower threshold for such a triggering event than may be appropriate in a production environment.

Possible adversary techniques investigated and ruled out, and example perception comprehension methods for use of those techniques, are detailed below.

Techniques: Remote File Copy, Program Organization Units, Project File Infection, Manipulate I/O Image, Modify Control Logic, Program Download, Module Firmware, and System Firmware.

Comprehension Opportunities: These techniques all require file uploads, evidence of which could be seen through PCAP analysis and possibly through SIEM capabilities.

Techniques: Valid Accounts.

Comprehension Opportunities: Reviewing logins for irregularities of user, system, location, time, and duration could provide evidence of inappropriate use of valid credentials.

Techniques: User Execution.

Comprehension Opportunities: Inspection of physical access logs and network traffic, including web interface traffic, commands which are indicative of user interaction, and traffic authenticated as a user could provide evidence of user execution.

Techniques: Modify Parameter.

Comprehension Opportunities: Application layer packets containing device command messages could provide evidence of parameter modification.

Techniques: Execution through API.

Comprehension Opportunities: In the context of the experiment environment, abnormal or unauthorized API usage detected in network traffic associated with recent technician access to the suspect device could provide evidence of API execution.

Techniques: Command Line Interface, Scripting, Data Destruction, Denial of Service, Service Stop, Masquerading.

Comprehension Opportunities: In the context of the experiment environment, cooperation with the AOO's vendors who have remote access capabilities could provide evidence of these techniques.

Techniques: Supply Chain Compromise, Hooking, Exploitation for Evasion, and Rootkit.

Comprehension Opportunities: Deeper forensic inspection of implicated devices after removal from service could provide evidence of these techniques.

Decision: The AOO's staff ultimately decided this situation was a reliability failure, at the point where they took action to replace the involved device with a spare. Their continued investigation into the causes behind the failure, even in the context of the experiment, gives some insight into their organizational risk appetite, and is an indication of their continuous improvement capabilities.

CONCLUSION

The CyOTE methodology is the product of a combination of research, collaboration with AOOs and government partners, and continuous learning over the course of more than five years. As stakeholders materially increased their understanding of the problem space and opportunities to improve, the energy sector as a whole will benefit from all AOOs having the capability to independently identify potential indicators of malicious cyber activity in their OT environments, sooner and with higher confidence.

The paradigm for OT cybersecurity is due for change to a more holistic analysis starting with the identification of anomalies and leveraging information and context from operations, OT, cybersecurity, and business operations. CyOTE offers a framework to assist asset owners in prioritizing their OT visibility investments likely to give the most benefits the soonest (i.e., identify the low-hanging fruit). CyOTE Use Case participation already has encouraged AOOs to partner internally across departments in their organizations, and exchange insights and ideas on how other companies are tackling OT environment monitoring challenges.

Looking forward, CyOTE seeks to improve through use and feedback to grow the body of knowledge for application by AOOs, tailoring to organizational facts and circumstances. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

The CyOTE team would like to hear about experiences using the methodology to define triggering events, to perceive anomalies in environments, and take a holistic analytical approach to gain comprehension of anomalies. Please share observations with the CyOTE team at CyOTE.Program@hq.doe.gov to help the energy sector continue to maintain its OT cybersecurity.

APPENDIX A: GLOSSARY

Anomaly: An observable deviating from what would be expected and understood as normal in the same or similar circumstances. Anomalies by definition are not presently comprehended.

Asset Owner and Operator (AOO): An entity that owns or operates energy infrastructure assets.

Case Study: The process and associated report describing the analysis of an attack using the CyOTE methodology. Identifying the anomalous activity, correlating the technique(s) associated with the anomalous activity, and creating a view of associated (by time, historical attack tactics, etc.) techniques to understand and identify current risks of potential on-going attacks.

Comprehension: The organizational human ability to understand an observable, in all its relevant context across the operations, electrical, operational technology, and cybersecurity domains.

Data Fields: The individual elements of information type contained in a particular Data Source. These are best thought of as the column headers in a spreadsheet format.

Data Sources: The logical and physical locations where information of potential use in comprehending an anomaly are created and stored. In some cases, the point of creation is different from the point(s) of storage.

Fact Sheet: A high level overview of a MITRE ATT&CK Framework for ICS technique and example cyber-attacks that have employed the identified technique.

Observable: A signature of an occurrence able to be perceived.

Operational Tool: A Proof of Concept tool which has been adapted by and for implementation in an asset owner environment.

Procedure: The lowest-level, highly-detailed, environment-specific sequence of steps taken to implement a technique.

Proof of Concept Tool: A representative implementation of a set of steps and methods for detecting techniques.

Recipe: A more detailed product describing a set of steps and methods for detecting techniques.

Tactic: The behavior of an adversary described at a high level in terms of the standalone task to be accomplished.

Technique: A named description of how a tactic can be accomplished.

Triggering Event: An anomaly that, when perceived, initiates investigation and analysis to comprehend the anomaly.

TTP: An acronym for Tactics, Techniques, and Procedures. Often used as a shorthand and informal term to describe the manner in which some action was accomplished, each word has a specific and nested meaning and application such that they are not precisely or formally interchangeable. Unless specified otherwise, TTPs in the context of CyOTE refer to the specific ATT&CK Framework for ICS knowledge base references.

Use Cases: The process followed by asset owners/operators within the CyOTE Program that identified Data Sources and Data Fields within them that would be useful in comprehending anomalies.

APPENDIX B: QUESTIONS FOR COMPREHENSION

These questions are intended to be used as a guide during to gain comprehension of anomalies while employing The CyOTE methodology. They are representative, not exhaustive, and are intended to give a better idea of extent-of-condition and apparent causal relationships at a point in time. AOOs should tailor and augment these suggested questions based on their own experience and context.

- How does the device or system where the anomaly was perceived provide business value to the organization?
    - Describe the tasks (things it does) and purpose (why the organization needs it) for the device or system.
    - Describe what the device is understood to be capable of from its supplier, regardless of whether this functionality is used by the organization.
- Enumerate the observables related to this anomaly, both those perceived and also those expected but not perceived. Although some or most may not be readily apparent, and not all the examples below will relate to every anomaly, there should be multiple observables in different physical and logical locations for most anomalies. These could include, but are not limited to:
    - Digital logs on endpoint ICS devices
    - OT network traffic
    - Telemetered change in system electrical quantities
    - Change in physical status of electrical infrastructure
    - Change in other physical condition e.g., damage or changed operating parameters
    - Don't discount the five senses, such as hot device enclosures or smelling the 'magic smoke' that should remain contained inside the device.
- Was this the first time such an anomaly has been perceived or do records or institutional memory show similar previous occurrences?
    - If the latter, describe the periodicity or any apparent patterns.
- Was a single device involved, or multiple devices?
    - If multiple devices, describe the as-designed physical and logical relationships between the involved devices.
- With which other devices and systems are the involved device(s) communicating or not communicating?
    - From a network perspective do the observed communications match the as-intended expectation in terms of protocol, endpoints, periodicity, rate, sequence, and relationship to other events?
    - From a device perspective do the observed communications match the as-intended expectations in terms of payloads (structure and content) and relationship to other events?
- Was the anomaly perceived at a time of action/change/movement or discovered in as-found static-at-the-moment condition?
    - If the former, how often does that action/change/movement occur, why does it occur, and from what physical and logical places is it observable?

  - If the latter, what other physical and logical locations and systems in the organization could also show such an anomaly?
- Are any observables related to the anomaly attributable to a specific account or source?
  - When was the last time the permissions for this account were audited or changed? Were these changes intended?

REFERENCES

1. David Bianco, "The Pyramid of Pain." Accessed May 21, 2021. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

2. Machiavelli, Niccolo, and George Bull. 2003. *The Prince*. Penguin Classics. London, England: Penguin Classics.

3. Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain," *SANS Institute Information Security Reading* Room, October 2015, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

4. "ATT&CK® for Industrial Control Systems," MITRE, accessed May 21, 2021, https://collaborate.mitre.org/attackics/index.php/Main_Page.

5. Micah R. Endsley, "Situation Awareness Misconceptions and Misunderstandings," *Journal of Cognitive Engineering and Decision Making* 9, no. 1 (March 2015):4 https://doi.org/10.1177%2F1555343415572631.

6. "Reliability Guideline: Situational Awareness for the System Operator," North American Electric Reliability Corporation, accessed May 21, 2021, https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SA_for_System_Operators.pdf.

7. "Cybersecurity Capability Maturity Model (C2M2)," Department of Energy, accessed May 21, 2021, https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

8. Tzu, Sun. 2010. *The Art of War*. PDF. Capstone Classics. Chichester, England: Capstone Publishing.

9. Rush, "Freewill." Recorded September-October 1979. Track 2 on *Permanent Waves*. Mercury, 1980.

10. "EA Program," North American Electric Reliability Corporation, accessed May 21, 2021, https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx.

11. Deming, W. Edwards. 2018. *Out of the Crisis*. The MIT Press. Cambridge, Mass.: MIT Press.

12. "Cause Analysis Methods for NERC, Regional Entities, and Registered Entities (September 2011)," North American Electric Reliability Corporation, accessed May 21, 2021, https://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/Cause%20Analysis%20Methods%20for%20NERC,%20Regional%20Entities,%20and%20Registered%20Entities_09202011_rev1.pdf.

13. "Lye-Poisoning Attack in Florida Shows Cybersecurity Gaps in Water Systems," NBC News, accessed February 11, 2021, https://www.msn.com/en-us/news/us/lye-poisoning-attack-in-florida-shows-cybersecurity-gaps-in-water-systems/ar-BB1dxMlI.

14. "Plant Automation Yields Immediate ROI," McKim & Creed, accessed February 11, 2021, https://www.mckimcreed.com/portfolio-page/plant-automation-yields-immediate-roi/.

15. "Oldsmar, Florida water facility credentials contained in COMB data leak," CyberNews, accessed February 11, 2021, https://cybernews.com/news/oldsmar-florida-water-facility-credentials-contained-in-comb-data-leak/.

16. "Analyzing the TRITON industrial malware," Midnight Blue Labs, accessed May 5, 2021, https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware.

17. "The Inside Story of the World's Most Dangerous Malware," Energywire, accessed May 5, 2021, https://www.eenews.net/stories/1060123327.

18. "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, accessed May 5, 2021, https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661.

19. "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," FireEye, accessed May 5, 2021, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

20. "MDudek-ICS/TRISIS-TRITON-HATMAN," GitHub, accessed May 5, 2021, https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/blob/master/decompiled_code/library/TsHi.py.

21. "The Inside Story of the World's Most Dangerous Malware," Energywire, accessed May 5, 2021, https://www.eenews.net/stories/1060123327.

22. "Technologies to Rapidly Restore the Electrical Grid after Cyberattack Come Online," Defense Advanced Research Projects Agency, accessed June 10, 2021, https://www.darpa.mil/news-events/2021-02-23.