North American Transmission FORUM

Community Confidentiality Candor Commitment

North American Transmission Forum External Newsletter

April 2018

Redacted Operating Experience Reports

The NATF works with its members to identify and communicate timely and actionable operating experience and other reliability information regarding risks, vulnerabilities, events, adverse trends, lessons learned, and superior practices. NATF "operating experience" can be either positive or negative and span any transmission (reliability, resiliency, or safety) learning opportunity worth sharing or for potential trending—regardless of actual impact or cause. One of the key benefits for sharing operating experience information is the opportunity for members to learn without experiencing those lessons first-hand.

As an added value for NATF members and benefit to the industry, the NATF has begun to develop redacted operating experience reports, which are posted on the NATF public site at: http://www.natf.net/documents.

Members and other utilities may use the redacted reports internally and share with their contractors to help improve safety, reliability, and resiliency.

NERC Compliance Implementation Guidance Submittals and Endorsement

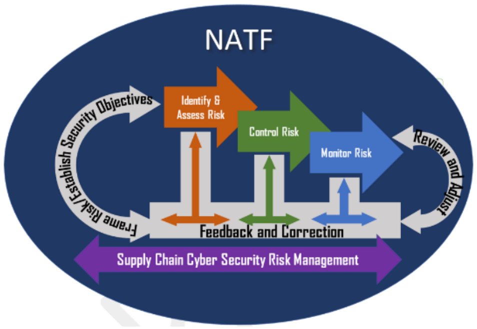
On a case-basis, the NATF develops practice or guidance documents related to topics that are associated with NERC Reliability Standards. Below is an update of documents submitted to NERC for consideration as compliance "Implementation Guidance."

NERC recently posted three NATF documents as "ERO Enterprise-endorsed Implementation Guidance" on its Compliance Guidance website:

- "CIP-014-2_R5_Developing_and_Implementing_Physical_Security_Plans_(NATF)"
  - On NATF site as "NATF Practices Document for CIP-014-2 R5"
- "CIP-010-3 R1.6 Software Integrity and Authenticity"
  - On NATF site as "NATF Guidance for CIP-010-3 Software Integrity"
- CIP-014-2 R4 Evaluating Potential Physical Security Attack"
  - On NATF site as "NATF Practices Document for CIP-014-2 R4"

As noted, the documents are also posted on our public site.

Cybersecurity Supply Chain Risk Management



A cross-functional NATF project team is working to develop a supply chain risk management framework and practices and guidance for cyber security supply chain risk management and the associated Reliability Standards (CIP-013, CIP-005, CIP-010).

As noted above, NERC accepted one of our CIP-010 documents as "ERO Enterprise-endorsed Implementation Guidance." The NATF also submitted two other documents (that address supply chain standards requirements in CIP-010-2 and CIP-005-6) for consideration as Implementation Guidance that NERC chose not to endorse. The NATF drafting teams and staff are reviewing next steps.

Regarding CIP-013, the NATF supply chain group drafted a white paper describing practices for establishing and implementing a supply chain cyber security risk management plan. The draft is being reviewed by NATF members and by leadership, staff, and designated representatives of select industry organizations/groups with whom the NATF team has been collaborating and coordinating (ISO/RTO Council, NRECA/APPA, EEI, NAGF, NERC CIPC). After review, the NATF plans to develop a version of the white paper for industry use and submit an associated document to NERC for consideration as Implementation Guidance as an approach to comply with CIP-013.

Protection System Misoperations Report

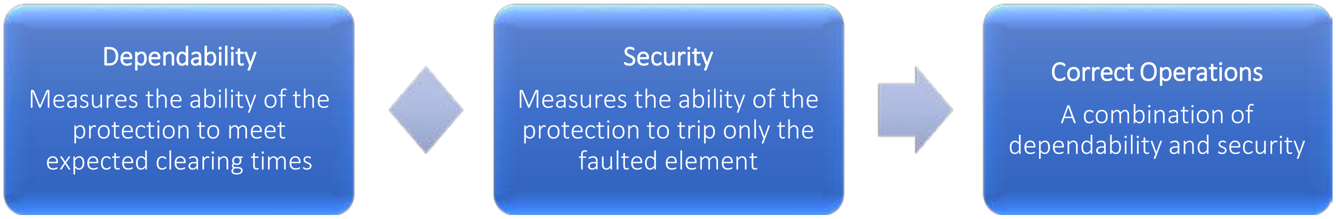
The NATF Protection System Misoperations Analysis Initiative began in 2015. As part of this initiative, the NATF requests Misoperation data from member companies, calculates metrics, and provides an analysis of Misoperation causes. The goals are to support peer-to-peer benchmarking, recommend System Protection Practices Group activities to address significant causes of misoperations, provide information members can use to reduce misoperations, and position NATF as a source of information and insight on protection system performance.

Annual Report

Each year, the Misoperations Analysis Working Group prepares a Protection System Misoperation Analysis Initiative Annual Report to analyze misoperation categories and causes.

Metrics

The NATF calculates three metrics:



Dependability

Measures the ability of the protection to meet expected clearing times

Security

Measures the ability of the protection to trip only the faulted element

Correct Operations

A combination of dependability and security

A small number of misoperations are failures to trip or slow trips, which are reflected in the dependability metric. The majority of misoperations are unnecessary trips, which drives the security metric lower. The separate metrics provided by the NATF initiative help us understand the nature of misoperations and, in some cases, see how different protection system design philosophies affect the balance between dependability and security.

It is important to calculate separate dependability and security metrics. A focus on improving security without monitoring how those improvements affect dependability could allow negative impacts on dependability to go undetected.

Analysis and Recommendations

The most recent annual report provided 31 recommendations to members, the Misoperation Analysis Working Group, and the System Protection Practice Group, ranging from benchmarking approaches to misoperations reporting and cause analysis.

External Coordination

The NATF interfaces with industry partners and regulatory agencies in a variety of ways, including joint workshops and webinars. Recent and upcoming activities include:

- Inverter-Based Resource Webinar Series
- Joint NERC/NATF Human Performance Conference and Workshops (March 27-29)
- NERC-NATF-EPRI 2018 Power System Modeling Conference (June 20-21)

***

For more information about the NATF, please visit www.natf.net.