PNNL-30546

ELECTRICITY SUBSECTOR

TRANSMISSION RESILIENCE MATURITY MODEL (TRMM)

Quick Reference

Draft Version 1.0

October 2020

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, nor other organizations participating in the production of this report makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute, or the other organizations participating in the production of this report. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY

operated by

BATTELLE

for the

UNITED STATES DEPARTMENT OF ENERGY

under Contract DE-AC05-76RL01830

Contents

Acknowledgments

The U.S. Department of Energy (DOE), Electric Power Research Institute (EPRI) and North American Transmission Forum (NATF), and Pacific Northwest National Laboratory (PNNL) acknowledge the dedication and technical expertise of the organizations and individuals who have provided the critiques, evaluations, and modifications to enable the development of this first release of the Transmission Resilience Maturity Model (TRMM).

Department of Energy	**PNNL**	**NATF/EPRI Members**	
David Meyer	Cliff Glantz	Jeff Schraufnagel	ATC
EPRI	Paul Skare	Dave McRee	Duke Energy
Kevin Berent	Sri Nikhil Gourisetti	Tom Pruitt	Duke Energy
Laura Fischer	Grace Mcnally	Steve Ladd	Duke Energy
NATF	Devan Farrell	Floyd Galvan	Entergy
Ed Ernst	Easton Gervais	Mark Peterson	Great River Energy
Lynna Estep		Gordie Halt	ITC
Ken Keels		Dennis Snook	OPPD
		Todd Lucas	Southern Company
		Grant Smedley	Salt River Project
		Mark Wehlage	Xcel Energy
		Brian Long	Xcel Energy

Cautionary Note

Intended Scope and Use of This Publication

The guidance provided in this publication is intended to address the implementation and management of resilience practices, most specifically the practices of transmission business units (TBU). This guidance is not intended to replace or subsume other resilience-related activities, programs, processes, or approaches that electricity subsector organizations have implemented or intend to implement. Additionally, this guidance is not part of any regulatory framework and is not intended for regulatory use. Rather, the guidance in this publication is intended to complement a comprehensive resilience program.

1. Introduction

The electric transmission sector is facing a range of threats to its functionality that are either new, more severe than experienced in earlier years, or more well understood. Such threats include more frequent and more severe extreme weather events, wildfires, droughts, and human-caused physical and cyberattacks. They also include geological, electromagnetic, and biological events. The novelty or increasing severity of these threats creates a significant need for transmission owners to implement programs to prevent, prepare for, respond to, and recover from such incidents. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats, and the transmission networks are essential components of that infrastructure.

The Electricity Subsector Transmission Resilience Maturity Model (TRMM) is a tool that transmission organizations can use to evaluate and benchmark their currently established transmission resilience strategies, programs, policies, and investments, in order to target and prioritize enhancements where needed.

The TRMM was developed to address the unique characteristics of the transmission system. The model can enable users to:

- evaluate and benchmark their organization's resilience capabilities
- prioritize actions and investments to improve the resilience of their systems
- share transmission-related knowledge, best practices, and relevant references within their organization and with business partners as a means to improve resilience capabilities
- contribute to increasing the overall resilience of the Nation's transmission systems.

The TRMM provides descriptive rather than prescriptive industry-focused guidance. The model content is presented at a high level of abstraction so that it can be interpreted by transmission organizations of various types, structures, and sizes. The model is designed to an be easy-to-use, self-assessment tool. Additionally, the TRMM is not part of any regulatory framework and is not intended for regulatory use. Rather, the TRMM is intended to complement a comprehensive resilience program.

This document provides quick reference material for TRMM users. It provides a summary descriptions of the model's nine domains, the model's transmission resilience maturity levels, and the approach for scoring the implementation of model practices.

2. TRMM Domains

The TRMM is organized into domains, objectives and practices (Figure 1). Domains are the key topical areas of the model. Each of the model's nine domains is divided into two or more objectives. Performance for an objective is determined by evaluating a structured set of transmission resilience-related practices. The practices evaluate performance at three different maturity indicator levels (MILs).

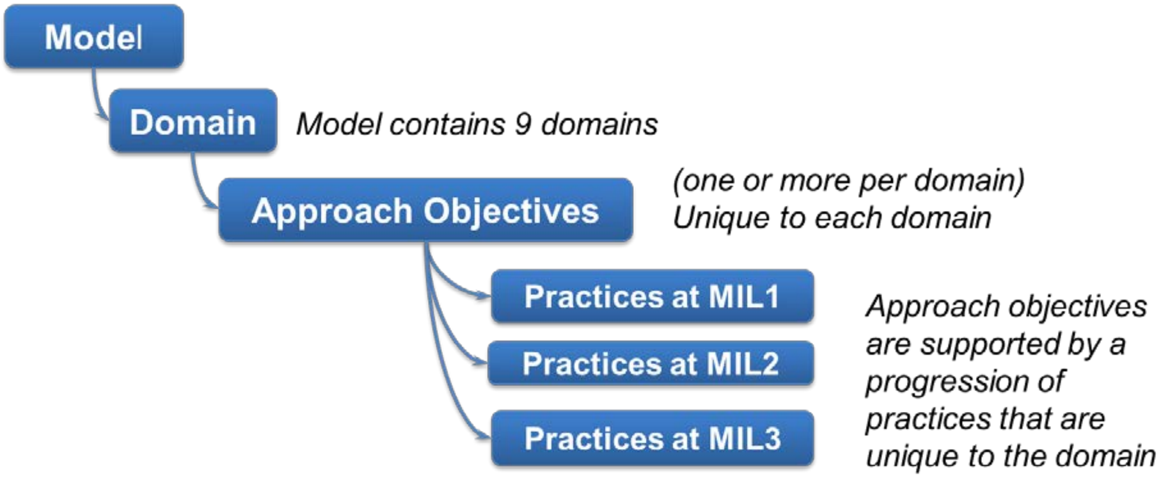

Figure 1. The Relationship Between TRMM Model Elements

For each TRMM domain, the model provides a purpose statement (a high-level summary of the concept of the domain) followed by introductory notes which provide the context for the domain and introduce its practices. The purpose statement and introductory notes offer context for interpreting the practices in the domain.

The practices within each domain are organized under objectives, which represent achievements that support the domain. Each of the objectives in a domain has a set of pertinent practices, which are ordered by MIL.

The following subsections provide a summary description of each domain.

Resilience Program Management (PM)

Purpose: Establish and maintain a transmission business unit (TBU) resilience program that provides governance, overall program strategy, direction and sponsorship for the TBU's resilience activities. The PM aligns resilience objectives with the TBU's and enterprise's strategic objectives and the risk to infrastructure.

A transmission resilience program is an integrated group of activities designed and managed to meet resilience objectives for the TBU.

The Transmission Resilience Program Management (PM) domain has four objectives:

1. Establish and maintain resilience governance structure
2. Establish and maintain the resilience program strategy
3. Sponsor resilience program activities
4. Incorporate resilience in rate making/cost recovery process

Risk Identification, Assessment, and Management (RM)

Purpose: Establish, operate, and maintain a resilience risk management program to identify, analyze, prioritize, select, develop, and implement actions to address resilience risks.

A resilience threat will adversely impact an organization's facilities and operations. These threats include actions by malicious actors (e.g., terrorist groups, criminal organizations), non-routine weather events (e.g., hurricanes, major ice storms), earthquakes, solar storms, and others.

A resilience vulnerability is a weakness or flaw in transmission infrastructure, site security, communications systems, IT systems, internal controls, etc. that could be exploited by a non-routine threat and result in a disruption of transmission capabilities that cannot be promptly restored (e.g., an outage lasting many days, weeks, or months). Vulnerability discovery may be performed using internal and external sources of information (e.g., announcements by industry associations or vendors, exercise findings, self-assessment results, and audits.)

Transmission resilience risk is determined by characterizing the potential consequences of adverse events and the likelihood or susceptibility to the events that could trigger those consequences. Consequences of concern for resilience programs are those that could impact transmission operations (including mission, goals, image, and reputation), resources, and other organizations over an extended period of time. Transmission resilience risk is one component of the overall business risk environment and it feeds into an organization's enterprise risk management program. Transmission resilience risk cannot be completely eliminated, but it can be managed and mitigated through informed decision-making processes.

The Risk Identification, Assessment, and Management (RM) domain comprises six objectives:

1. Identify threats to transmission resilience
2. Identify vulnerabilities to transmission resilience
3. Identify the consequences of transmission resilience threats and vulnerabilities
4. Assess transmission resilience risks
5. Perform risk mitigation activities
6. Management support activities

Situational Awareness (SA)

Purpose: Establish and maintain activities to monitor, analyze, and communicate information in a common operating picture, or COP (i.e., a single display of relevant information), commensurate with the resilience objectives and risks to the transmission infrastructure. The Time Horizon covered by this domain is Operations Planning and Real-time Operations (i.e., the timeframe where the transmission business unit (TBU) must be aware of threats in order to adjust and implement mitigating strategies, but not far enough in advance to build or harden). Those Long-term Planning actions are covered under the Risk Identification, Assessment, and Management domain.

Situational Awareness provides an understanding of the current resilience landscape, based on knowledge and analysis of both real-time and near real-time knowledge. This is accomplished, in part, through monitoring key aspects of potential threats, vulnerabilities, and risk. It also includes the monitoring the inventory and status of assets and equipment – including spare transmission assets and equipment needed to support resilience program activities (e.g., light vehicles, service vehicles, communication equipment). It further includes information on workforce resources (e.g., available primary response staff and backup staff, available contractor support).

It is important to note that events external to an enterprise can represent imminent or emerging operational threats to the enterprise. Therefore, a broad awareness of relevant external events is necessary to develop and maintain a robust COP. COP is defined as a single identical display of relevant information shared by all affected groups. A COP facilitates collaborative planning and assists all groups to achieve situational awareness. The COP aggregates information from multiple topical areas such as cyber, physical, telecommunications, and system operations. The COP leverages various technologies to collect, analyze, alarm, present, and use the aggregated information for timely, effective TBU decision-making and actions.

The COP serves as a key input to the Event Response and Recovery Domain activities.

The Situational Awareness (SA) Domain comprises three objectives.

1. Perform monitoring
2. Establish, maintain, and communicate a common operating picture (COP)
3. Management support activities

Event Response and Recovery (ERR)

Purpose: Establish, maintain, and exercise plans, procedures, and technologies to respond to and recover from events impacting transmission business unit (TBU) resilience, commensurate with the resilience objectives and risks to the transmission infrastructure.

A key element of resilience is the TBU's ability to respond to and recover from an actual resilience event. To achieve a good outcome the TBU must have defined plans and capabilities for restoration and recovery as well as be able to satisfactorily execute these capabilities. Integral to those capabilities is implementation of an incident command structure (e.g., based on Federal Emergency Management Agency (FEMA) Incident Command System (ICS)). Given that employees are integral to the restoration and recovery process, the TBU must pay special attention to addressing employee needs so that they can perform their defined tasks.

The Response and Recovery (ERR) domain comprises five objectives:

1. Develop and maintain response and recovery capabilities
2. Exercise/drill response and recovery capabilities
3. Communicate and share pertinent information during an event
4. Provide support for personnel participating in response and recovery
5. Management support activities

Transmission and Supporting Equipment Management (EqM)

Purpose: Identify and manage assets used to detect, identify, analyze, prepare for, respond to, and recover from resilience threats and events. For the purposes of this model, assets to be considered include things such as transmission equipment, tools, databases, software, computer hardware, vehicles

In order to effectively manage resilience challenges, the transmission business unit (TBU) needs a variety of assets to be able to detect, identify, analyze, respond to, and recover from resilience threats and events.

These assets include:

- transmission system equipment (e.g., transformers, poles, relays)
- transmission support equipment (e.g., tools for repairing transmission system equipment, vehicles for transporting materials and personnel, tools for system analyses, monitoring, and managing restoration processes).

The Transmission and Supporting Equipment Management (EqM) domain comprises four objectives:

1. Identify and manage transmission equipment

2. Develop and coordinate transmission equipment spare program
3. Identify and manage supporting equipment
4. Management support activities

Information Sharing and Communications (ISC)

Purpose: Establish and maintain relationships, procedures, and capabilities (both voice and data) with internal and external entities to collect and provide resilience information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with resilience objectives and risks to transmission infrastructure.

The objective of information sharing is to strengthen resilience that supports transmission capabilities and the interconnected critical infrastructure, by establishing and maintaining a framework for interaction, communication, and information sharing. This includes communication within an organization or enterprise, with external partners, and with government agencies.

The Information Sharing and Communications (ISC) domain comprises four objectives:

1. Identify internal and external communication partners
2. Build information sharing and communication relationships
3. Manage/maintain communications tools
4. Management support activities

Supply Chain and Critical Entities Management (SCE)

Purpose: Establish and maintain relationships with suppliers and other key resources needed to respond to a transmission resilience event commensurate with resilience objectives and the risk to the transmission infrastructure (e.g., establishing mutual aid agreements, managing key vendor relations, establishing spare equipment sharing arrangements.) Critical entities can support the TBU/enterprise, the electricity subsector, or society at large.

As the dependencies among infrastructures, operating partners, suppliers, service providers, and customers increase, establishing and maintaining a comprehensive understanding of key relationships and managing their associated resilience risks are essential for a secure, reliable, and resilient transmission system.

Supply chain risk is a noteworthy example of a supplier dependency. The characteristics of products and services vary widely. Without proper supply chain management, new threats can be introduced, including software of unknown provenance and counterfeit hardware. Requests for proposals often give suppliers of high-technology systems, devices, and services only rough specifications, which may lack adequate requirements for security and quality assurance. Therefore, it is important to consider transmission resilience requirements in managing procurement activities (e.g., via agreements, acceptance testing, mitigation strategies).

A key element in supply chain and critical entities management is the identification of the TBU's "critical entities." These critical entities can impact the TBU, the Bulk Electric System (BES), or society at large.

The Supply Chain and Critical Entities Management (SCE) domain comprises five objectives:

1. Identify critical entities
2. Manage the supply chain to support resilience
3. Manage the needs of electricity subsector critical entities to support resilience
4. Manage the needs of society critical entities to support resilience
5. Management support activities

Transportation Management (TM)

Purpose: Establish and maintain transportation plans and capabilities for the timely delivery of personnel, assets, and fuel to where they are needed to both prepare for and respond to a transmission resilience event.

During an event that challenges transmission resilience, a key resilience activity involves the transportation of physical assets (e.g., transformers, transmission tower equipment, cranes, power lines, portable generators), personnel (e.g., lineman, drivers, crane operators), fuel (e.g., diesel, gasoline) and other critical infrastructure (e.g., electric power, water, lighting, shelter, food) to the locations where personnel and physical assets are needed to support restoration activities for electric power transmission. Plans for the movement of assets and personnel are important as assets in storage yards and personnel at home or in their offices are not positioned to help address needs at remote locations.

The Transportation Management (TM) domain comprises two objectives:

1. Establish and maintain a transportation program
2. Management support activities

Workforce and Family Care Management (WFM)

Purpose: Raise resilience awareness in the workforce and prepare them to contribute during a resilience event by providing plans, training, tools, and peace of mind.

Workforce management for resilience events is critical to the successful restoration of the grid. Procedures should provide direction for workforce life cycle activities (e.g., hiring, security screening, transfer and termination practices), awareness and training, assignment of responsibilities, and family care plans.

Importantly, workforce plans for responding to resilience events should consider: 1) the full utilization of the workforce in roles that may be different from their traditional roles for potentially extended periods of time, and 2) recognition that events can have personal impacts to employees and their families.

The Workforce Management (WFM) domain comprises six objectives:

1. Increase Employee Resilience Awareness/Create a Culture of Resilience
2. Assign resilience event responsibilities
3. Provide training to response and recovery personnel
4. Control the workforce life cycle
5. Develop, maintain, and execute family care plan
6. Management support activities

3. Scoring Practice Implementation Levels

The implementation of individual practices is evaluated using a 4-point scale:

4-point answer scale	**The organization's performance of the practice described in the model is …**
Fully implemented (FI)	Complete -- the practice is performed as described in the model
Largely implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially implemented (PI)	Incomplete -- there are multiple opportunities for improvement
Not implemented (NI)	Absent -- the practice is not performed in the organization

This four-point scoring system is referred to using the acronym "FILIPINI." This is shorthand for "fully implemented, largely implemented, partially implemented, and not implemented."[1]

[1] The authors and developers of other C2M2-based maturity models pronounce this acronym as "fill-uh-PEE-nee."

4. Maturity Indicator Levels (MIL)

The model defines four maturity indicator levels, MIL0 through MIL3, which apply independently to each domain in the model.

Five aspects of the MILs are important for understanding and applying the model:

1. The MIL score is independent for each objective and domain. That is, an organization using the model is likely to score at different MILs in different objectives and different domains. For example, an organization could be operating at MIL1 in one objective, MIL2 in another objective, and MIL3 in a third objective. Similarly, the organizations may operate at different MILs across the nine domains. Some domains may be at MIL1, MIL2, or MIL3 levels. Note, there are no practices assigned for MIL0; therefore, if an organization is not operating at least at MIL1 for all practices at the objective or domain level, they would score at a MIL0 for that respective objective or domain.

2. The MIL scores are cumulative within each objective and domain. To earn a specified MIL for a given objective, an organization must largely or fully implement all of the objective's practices at that MIL and any lower MIL. For example, an organization must perform all of the objective's MIL1 and MIL2 practices to achieve MIL2 in the objective. The organization would have to largely or fully implement all of the practices in MIL1, MIL2, and MIL3 to achieve MIL3 for an objective. Just a single partially or not implemented practice can keep a MIL from being achieved. Similarly, to earn a specified MIL for a given domain, an organization must largely or fully implement all of the domain's practices at that MIL and each lower MIL. This scoring approach aligns with the concept that a chain is only as strong as the weakest link. Even one practice that is partially or not implemented, will keep an organization from achieving a MIL level.

3. Given the above rules for achieving MIL, an organization can, for example, have the same MIL for:

   - an objective or domain if only one practice is partially or not implemented, and all the other practices are largely of fully implemented.

   - an objective or domain where all the practices are partially or not implemented.

   This might accurately reflect the resilience capabilities of the organization in that objective or domain, but it does not indicate how close the organization may be to achieving that MIL. To capture that information, the TRMM provides a bar chart that offers a "MIL Progression Rating." This rating indicates the MIL level achieved and progress toward the next MIL. For example, an organization with a MIL1 rating and half of the additional MIL2 practices being largely or fully implemented, would have a MIL Progression Rating of 1.5.

The integer value indicates the MIL level achieved and the decimal value indicates the fraction of practices at the next level that are largely or fully implemented. The decimal value can range from 0 to a value just under 1.

4. Establishing a target MIL for each domain is an effective strategy for entities using the model to guide transmission resilience program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.

5. Resilience practice performance and MIL achievement goals need to align with business objectives and the organization's transmission resilience strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the model was developed with the intent that all companies, regardless of size, should be able to achieve MIL1 across all domains.

The general performance characteristics for each MIL are provided below.

Maturity Indicator Level 0 (MIL0)

Performance at MIL0 simply means that the practice has not achieved MIL1.

Maturity Indicator Level 1 (MIL1)

To achieve MIL1 performance, MIL1 activities are performed in at least in an informal or ad hoc manner. "Ad hoc" refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. Documentation is not required. A more formalized implementation that covers the scope of the practice immediately qualifies as largely or fully implemented at MIL1 and may jump to MIL2 or MIL3 depending on the performance of practices that evaluate those higher levels of maturity.

The level of implementation of a practice may vary significantly depending on who performs the practice, when it is performed, how it is performed, and the context of the problem being addressed. With experienced and talented personnel, resilience activities may be effectively implemented even if the practices are performed in an ad hoc manner. However, without documentation (e.g., policies, procedures, lessons learned), it is difficult to sustain an effective program as personnel and individual's priorities change.

If an organization were just starting work in a particular area, it should focus initially on implementing the MIL1 practices.

Maturity Indicator Level 2 (MIL2)

MIL2 performance is the result of formal processes and procedures that are kept current. A MIL2 organization is no longer performing activities irregularly or in an ad hoc manner. As a result, the organization's performance of the practices is more stable. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time.

Maturity Indicator Level 3 (MIL3)

MIL3 is the highest achievable MIL in the TRMM. Organizations performing at MIL3 are actively managing resilience activities. MIL3 performance is further stabilized and guided by high-level organizational directives, such as policy. Where applicable, performance at MIL3 includes coordination across the enterprise and not just within the TBU. Overall, a MIL3 organization should have additional confidence in its ability to sustain the performance of the TRMM practices over time and across the organization.