



MIDWEST  
RELIABILITY  
ORGANIZATION

# MRO 2021 Regional Risk Assessment

John Seidel, Principal Technical Advisor

Steen Fjalstad, Director of Security

Lee Felter, Principal Risk Assessment & Mitigation Engineer, CIP

CLARITY

ASSURANCE

RESULTS

John Seidel, Principal Technical Advisor

# MRO 2021 Regional Risk Assessment



CLARITY

ASSURANCE

RESULTS

# Assessing Bulk Power System Risk

- **Similar to the 2020 Regional Risk Assessment (RRA), the 2021 RRA references multiple ERO-wide reports that assess North American bulk power system risk:**
  - 2019 ERO Reliability Risk Priorities report (RISC report)
  - 2021 ERO Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP report)
  - 2020 NERC State of Reliability Report (SOR report)
  - 2020 NERC Long-Term Reliability Assessment (LTRA)
  - 2020 NERC/WECC Inverter-based Resource Modeling Report



# Assessing Regional Risk

- **MRO regional risk:**
  - MRO staff and advisory council members collaborated to identify risks that may have a higher probability of occurrence and/or impact within the region
- **MRO staff also reviewed the regional risk assessments of several other ERO regions to capture additional risks identified**



# Assessing Regional Risk

- **Operations and planning risks**

- Largely identified from Planning Coordinator (PC) assessments and data collection and trending, such as:

- Event Analysis, Misoperations reporting, Energy Emergency Alerts, NERC alerts, NERC lessons learned

- **Physical and cyber security risks**

- Captured annually in the MRO Regional Security Risk Assessment



# Assessing Regional Risk

- **CMEP activities to help reduce risk**
  - Development of Compliance Oversight Plans (COPs)
  - Summary of high risk requirements
  - Identification of new and existing high risk standards



# 2021 Risk Rankings

- **New in the 2021 RRA is the ranking of operational, planning, cyber security, and physical security risks**
  - A team of MRO staff assessed 2021 risks in terms of impact and likelihood using the Regional Risk Matrix that was developed by the Reliability Advisory Council
- **Also included are evolving industry trends that should provide operating flexibility and help mitigate some of the operational risks identified**



## MRO Reliability Risk Matrix- Operations and Planning Risks

| Consequence/<br>Impact (C) to<br>the BPS |            | Likelihood of Occurring (L) |          |          |             |                |
|--|------------|-----------------------------|----------|----------|-------------|----------------|
|  |            | L1                          | L2       | L3       | L4          | L5             |
|  |            | Very Unlikely               | Unlikely | Possible | Likely      | Almost Certain |
| C5                                       | Severe     |                             |          |          |             |                |
| C4                                       | Major      |                             |          | 6        |             |                |
| C3                                       | Moderate   |                             | 2        | 3, 4, 9  | 11          |                |
| C2                                       | Minor      |                             |          | 1        | 5, 7, 8, 10 |                |
| C1                                       | Negligible |                             |          |          |             |                |

| Operations and Planning Risks |   |
|-------------------------------|---|
| 1                             | Overhead Transmission Line Ratings During Cold Weather          |
| 2                             | Voltage Stability and Reactive Management of the BPS            |
| 3                             | Reactive Capability of Inverter Based Resources                 |
| 4                             | BPS Modelling Accuracy  |
| 5                             | Sunset of Telecommunication Circuits                            |
| 6                             | Uncertainty of Planning Reserve Margins                         |
| 7                             | Vegetation Management of 100-200 kV Circuits                    |
| 8                             | Cold Weather Operation of SF6 Gas Insulated Circuit Breakers    |
| 9                             | Wind Plant Modelling and Ride-Through Capability During Faults  |
| 10                            | Misoperations Involving Directional Comparison Blocking Schemes |
| 11                            | Misoperations Due to Errors Occurring During Commissioning      |





# Top Operational and Planning Risks

## ● Uncertainty of Planning Reserve Margins

- In 2020, three of the four PCs/Balancing Authorities (BAs) within MRO experienced a shortage of generation capacity that resulted in either energy emergency alerts or BA resource alerts
- This occurred during load conditions below forecast peak levels
- Wind generation was at times below the anticipated output level assumed in capacity planning and reserve margins



# Top Operational and Planning Risks

- **Uncertainty of Planning Reserve Margins**

- The 2020 summer anticipated planning reserve margins for the same three BAs were well above target reserve margin levels
- The deployment of accurate and timely Demand Side Management (DSM) of sufficient MW amount can help PCs/Reliability Coordinators reconcile the uncertainty associated with seasonal planning reserve margins and help manage real-time energy shortages



# Top Operational and Planning Risks

## ● BPS Modeling Accuracy

- The integrity of the Eastern Interconnection models must be maintained as many model builders participate to ultimately generate an Eastern Interconnection model
- The following attributes of bulk power models must all fit together accurately to have reliable set of models:
  - Renewable generation
  - The changing characteristics of load
  - Distributed energy resources netting with load
  - Interchange assumptions between each modeling area
  - Market flow assumptions
  - As well as short circuit modeling and inverter connected generation



# Top Operational and Planning Risks

- **Reactive Capability of Inverter Based Resources**
  - Inverter Connected Resources
  - These types of essential reliability services will need accurate planning models to assure the bulk power system remains secure



# Top Operational and Planning Risks

- **Wind Plant Modeling and Ride-Through During Faults**
  - Increasing percentage of inverter based generation across North America
  - MRO region has ~ 44 GW of wind generation, about 40% of the US total, with much of it inverter connected
  - Bulk power models need to have wind generation accurately represented



# Top Operational and Planning Risks

- **Misoperations Due to Commissioning Errors**
  - Misoperations reported through MIDAS and TADs database
  - Human error during commissioning of protection systems
  - No Reliability Standards covering commissioning



Steen Fjalstad, Director of Security

# Highest Cyber and Physical Security Risks



CLARITY

ASSURANCE

RESULTS

## MRO Reliability Risk Matrix - Physical and Cyber Security Risks

| Consequence/<br>Impact (C) to<br>the BPS |            | Likelihood of Occurring (L) |          |          |        |                |
|--|------------|-----------------------------|----------|----------|--------|----------------|
|  |            | L1                          | L2       | L3       | L4     | L5             |
|  |            | Very Unlikely               | Unlikely | Possible | Likely | Almost Certain |
| C5                                       | Severe     |                             |          |          |        |                |
| C4                                       | Major      |                             | 3        | 8        |        |                |
| C3                                       | Moderate   |                             | 10       | 6, 4, 7  |        |                |
| C2                                       | Minor      |                             |          | 1, 2, 9  |        |                |
| C1                                       | Negligible |                             |          |          | 5      |                |

|    | Physical and Cyber Security Risks      |
|----|--|
| 1  | Adequate Security Staffing & Funding   |
| 2  | CIP Standard Compliance Fatigue        |
| 3  | Combined Cyber and Physical Attack     |
| 4  | Communication Network (Backhaul)       |
| 5  | Drones / Unmanned Aerial Systems (UAS) |
| 6  | Insider Threat                         |
| 7  | Sabotage                               |
| 8  | Supply Chain                           |
| 9  | Unsupported/Legacy Devices             |
| 10 | Vulnerability Management               |

*The four risks in the orange section of the security risk heat chart have been identified as having the highest relative risk and are:*

- *Supply Chain*
- *Insider Threat*
- *Communication Network Backhaul*
- *Sabotage*





# Top Cyber and Physical Security Risks

- **Supply Chain**
  - Technology (equipment, hardware, and software)
  - Access (OEM, vendors) along with sub-components
  - Pandemic and lead time impact



# Top Cyber and Physical Security Risks

## ● Insider Threat

- Sensitive access with company specific insight
- Economic and political motivational factors
- Remote access & work from home element
- Behavioral indicators



# Top Cyber and Physical Security Risks

## ● Communication Network (Backhaul)

- Backhaul refers to the communication network that supplies connectivity to remote systems
- Risk is increased as a result of:
  - Lack of path diversity and redundancy for critical communications
  - Unknown or unacceptable third party communication backhaul provider availability and security
  - The use of shared infrastructure
  - Lack of security controls and incident response plans



# Top Cyber and Physical Security Risks

## ● Sabotage

- Saboteurs may cause disruption to operations, damage to assets, safety risks, and adverse financial and reputational impacts
- Risk is increased as a result of:
  - Insufficient situational awareness of saboteur groups and corresponding response plans and training
  - Inadequate physical access controls
  - Remote locations with long incident response times
  - When undertaking new facility construction or building new transmission lines



| MRO Reliability Risk Matrix – Operations and Planning Risks + Physical and Cyber Security Risks |            |                             |          |                 |             |                |
|---|------------|-----------------------------|----------|-----------------|-------------|----------------|
| Consequence/<br>Impact (C) to<br>the BPS  |            | Likelihood of Occurring (L) |          |                 |             |                |
|   |            | L1                          | L2       | L3              | L4          | L5             |
|   |            | Very Unlikely               | Unlikely | Possible        | Likely      | Almost Certain |
| C5  | Severe     |                             |          |                 |             |                |
| C4  | Major      |                             | 3        | 6 8             |             |                |
| C3  | Moderate   |                             | 2 10     | 3, 4, 9 6, 4, 7 | 11          |                |
| C2  | Minor      |                             |          | 1 1, 2, 9       | 5, 7, 8, 10 |                |
| C1  | Negligible |                             |          |                 | 5           |                |

- A combined total of nine risks fall into the moderate/higher (orange) area of the heat chart
- These nine have been identified as areas to focus on and develop action plans to help reduce impact/likelihood

Lee Felter, Principal Risk Assessment & Mitigation Engineer, CIP

# **CMEP Activities to Help Reduce Risk**



CLARITY

ASSURANCE

RESULTS

# Forward Looking CIP Risk Concerns

- **Physical Security and COVID-19**
- **Coordinated Cyber Attack Vulnerability on Geographically Distributed Targets**
- **Data Security**
- **Anomalies and Events, and Mitigation**



# CMEP Activities

- **Regional reliability considerations for CMEP activities**
  - Risk in aggregate
    - Identify Reliability Standards in COPs for entities with low inherent risk when considered individually, but have a substantial impact to the BES when aggregated (ie. inverter based generation).
    - Examples include Reliability Standards addressing:
      - Cyber Security for Low Impact BES Cyber Systems
      - Protection System Maintenance
      - Generator Frequency and Voltage Relay Settings (Voltage control ride through)
      - Response to Directives
  - CMEP Implementation Plan





# Contemporary Standards Changes

- **Regional Reliability considerations for CMEP activities**
  - New and upcoming standards include:
    - CIP-005-6: Electronic Security Perimeter(s)
    - CIP-008-6: Incident Reporting and Response Planning
    - CIP-010-3: Configuration Change Management and Vulnerability Assessments (patch verification)
    - CIP-013-1: Supply chain Risk Management



# MRO CIP Most Violated Standards

- **Manual Process, Automated Process**
  - CIP-007-6 R2 – Patch Management
  - CIP-010-2 R1 – Configuration Change Management
  - CIP-004-6 R4 – Access Management Program
- **System Complexity, Inadequate Process**
  - CIP-004-6 R4 - Access Management Program





CLARITY

ASSURANCE

RESULTS