RELIABILITYFIRST

Human Performance Workshop

Why Are We Here?

Johnny Gest
Manager, Engineering & System Performance

August 5, 2021

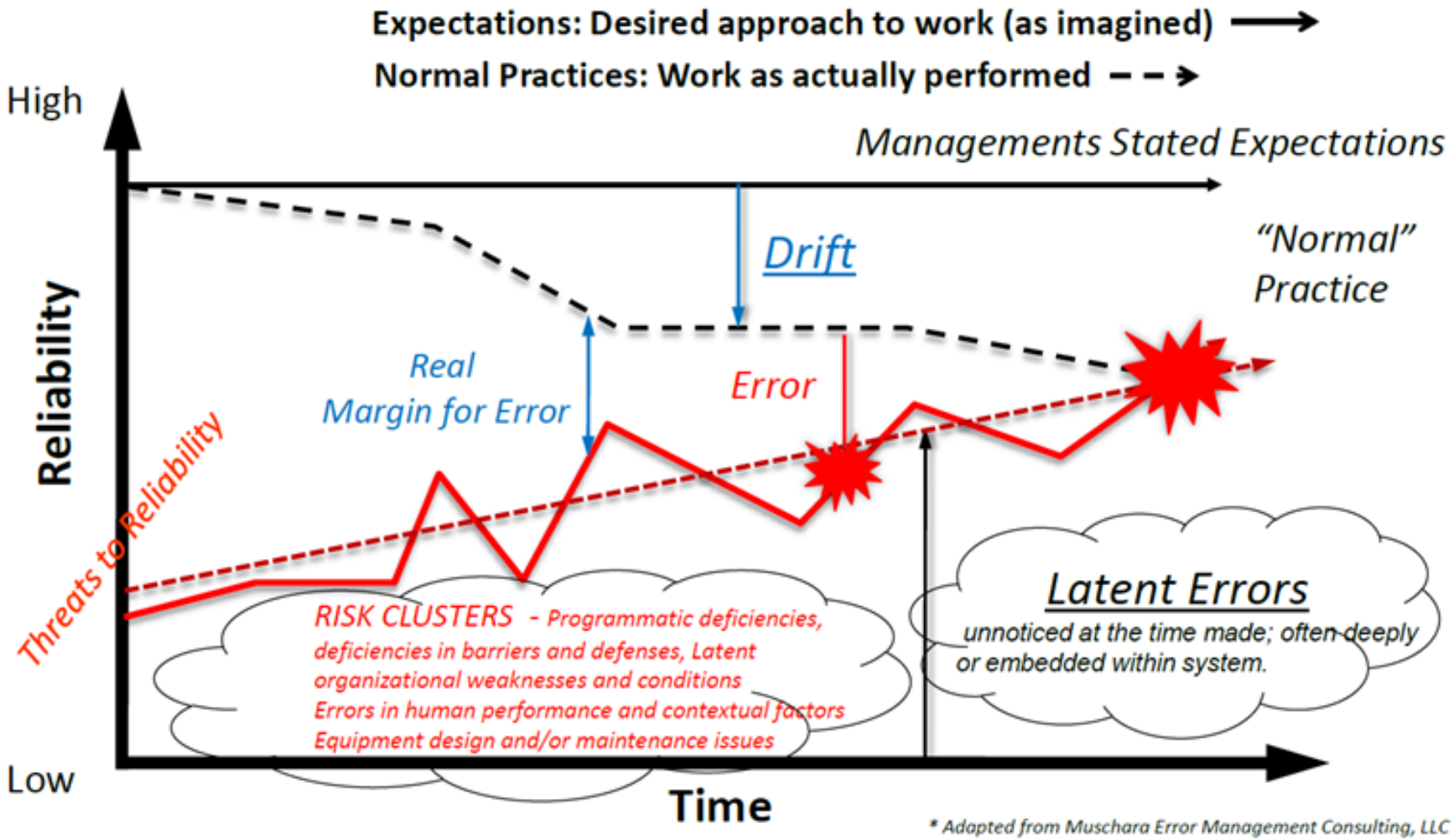
LIMITED DISCLOSURE






What is Human Performance?

Drifting to Failure Concept



* Adapted from Muschara Error Management Consulting, LLC

2016-2020 Outages per Circuit (100 kV+)

- **Number of transmission outages from ac circuits and transformers caused by human error is decreasing/stable**

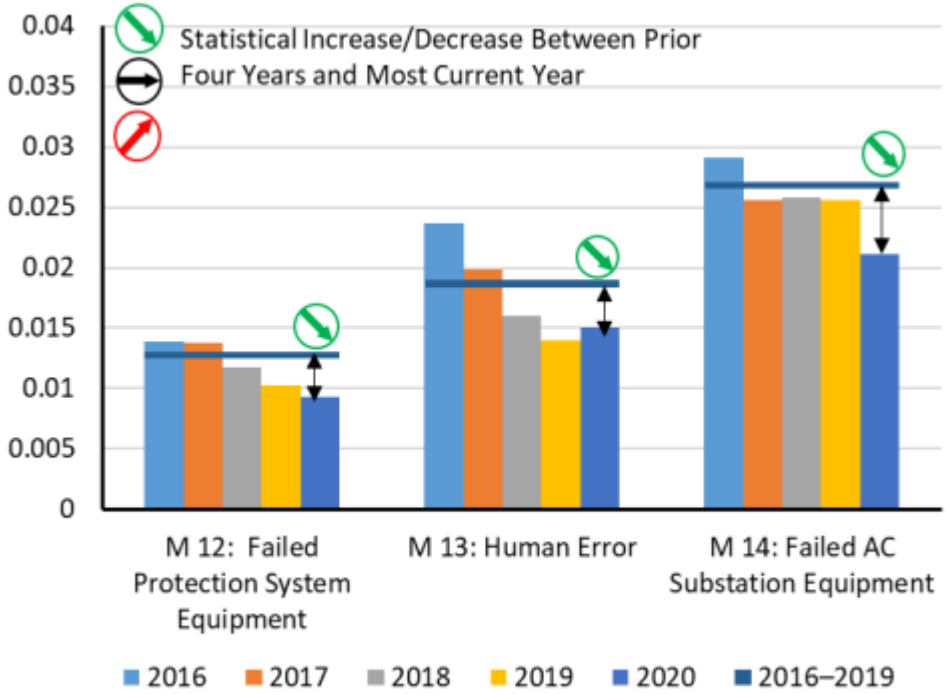


Figure 3.9: Number of Outages per AC Circuit due to Various Initiating Causes

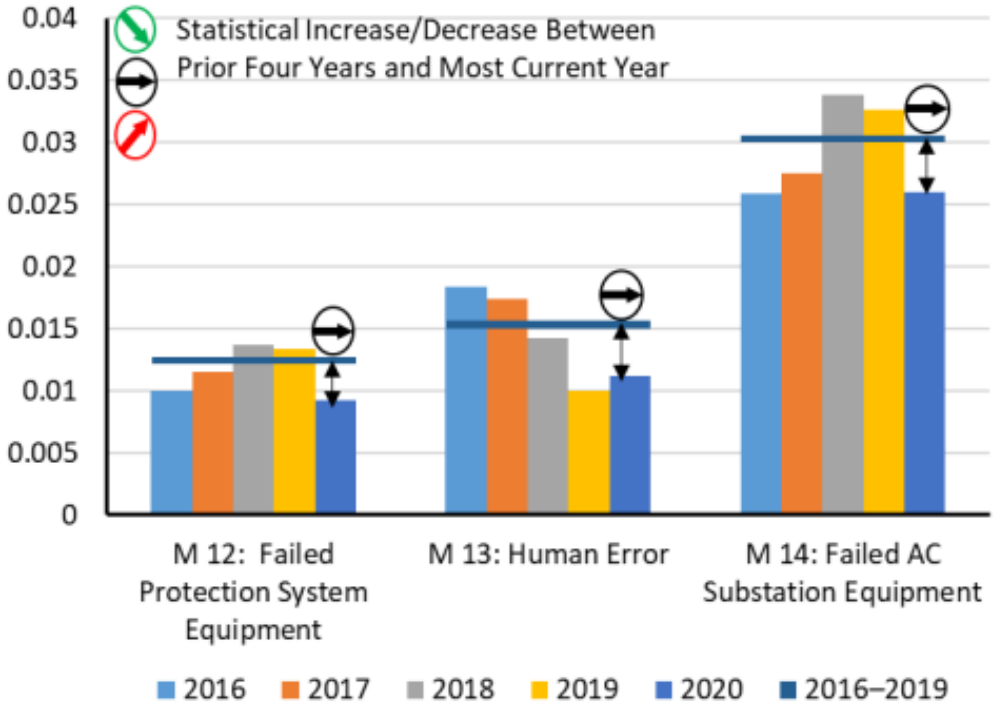
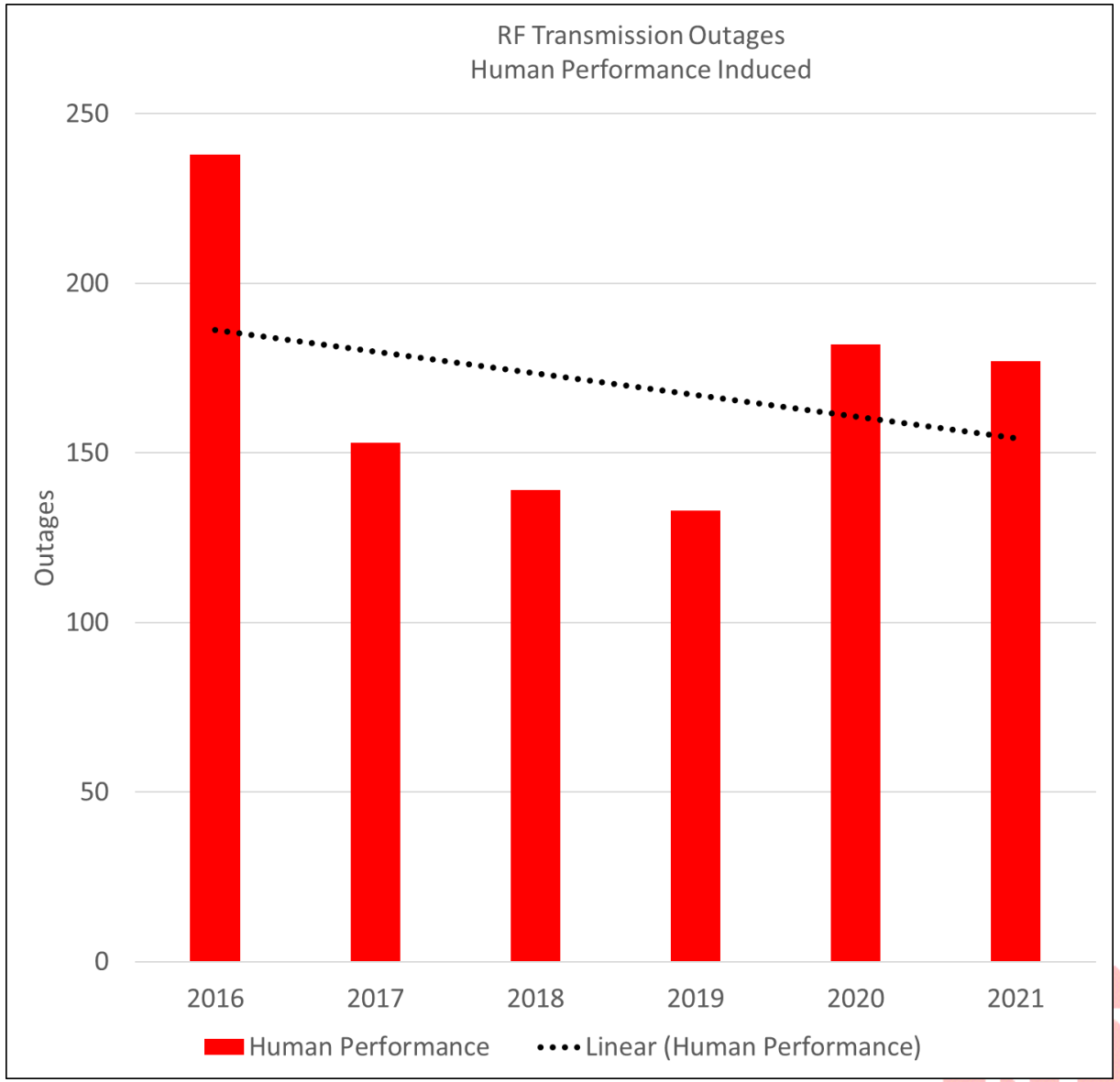


Figure 3.11: Number of Outages per Transformer Due to Various Initiating Causes

https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf

ReliabilityFirst HP Performance

- Number of outages from ac circuits and transformers caused by human error are ***decreasing***
- This trend is also reflected in generation outages and misoperations
- Events caused by human error are minimal



Maximizing Human Performance

We must understand that people will be people!

Make it easy for employees to do the right thing.

Make it hard for employees to do the wrong thing.

Make it so that when they do the wrong thing, it doesn't lead to a catastrophe!

Make the system conform to the people, not the other way around!

Create an environment that allows feedback and adaptation!

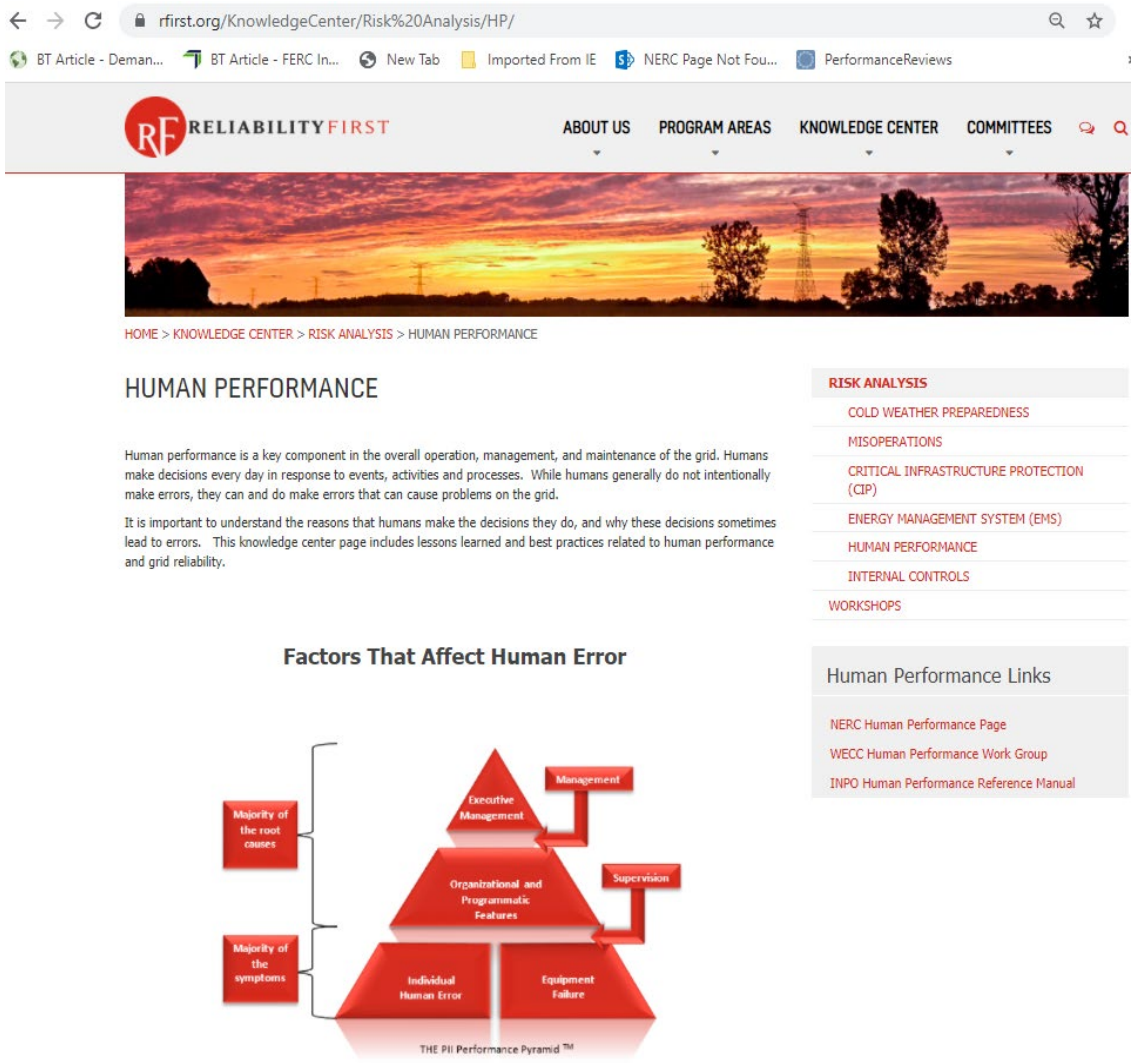
RF Human Performance Community of Excellence

A Community of Excellence (CoE) is a group of people who share an interest or passion for something they do, and learn how to do it better as they interact regularly with other colleagues in their field of expertise.

Intended Audience:

Human Performance Professionals from the ReliabilityFirst entities

RF Knowledge Center on Web Site



https://rfirst.org/KnowledgeCenter/Risk%20Analysis/HP/

Technical Talk with RF

Technical Talk with RF is typically scheduled the third Monday of each month 2:00-3:30 p.m.

Save the date for our next event,
Monday, August 15

The next *Tech Talk* will include guest presentations from **Talen Energy** and **DTE Energy** on their **Internal Control Programs**. Please invite not just compliance personnel, but also Internal Control Champions, and all those associated with designing, developing, implementing, and monitoring internal controls.

No Registration Required
- Calendar Reminder
- Webex Link

Follow us on:

ReliabilityFirst

Annual Reliability and Compliance Workshop

Tuesday, Sept. 27, 1:00 pm – 5:00 pm
Wednesday, Sept. 28, 8:00 am – 12:00 pm
Location: 3 Summit Park Drive, Suite 530 • Cleveland, OH 44131

The theme of this year's workshop is *Embracing the Transformation*. Our world and industry are evolving at a rapid pace, including the associated risks. The changing generation mix, inverter-based resources, virtualization, cloud computing, extreme weather, plus evolving cyber and physical security threats, all amid a pandemic, impact every aspect of how we perform our jobs to preserve and maintain reliability, resilience, and security. This workshop will help entities and stakeholders gain a deeper understanding of how we can collaboratively mitigate the known risks while anticipating emerging risks.

This event will be a hybrid workshop, meaning that we will host guests both i**n-person** and **virtually**. The in-person meeting will be limited to 125 RF Registered Entity guests at our newly renovated facility on the 5th floor of our offices. To accommodate as many Registered Entities as possible, we are limiting the **in-person** attendance to **eight persons** per NCR number. There are no limitations regarding **virtual** (Webex) registration. Please encourage your coworkers, staff, and stakeholders to sign-up to attend.

REGISTER TODAY -> Eventbrite Registration Link

Follow us on:

GRIDSECCON 2022
NERC • E-ISAC • RELIABILITYFIRST

GridSecCon Registration is Open

NERC, the E-ISAC, and ReliabilityFirst are co-hosting the 11th grid security conference on October 18–19, with training opportunities available October 17. Once again, GridSecCon will be held virtually. Registration can be found on the E-ISAC website here, and the agenda is located here.

At GridSecCon 2022 you can participate in:

- World-class training sessions
- Cutting-edge discussions, breakout sessions, and keynotes
- In-depth presentations on emerging cyber and physical threats
- Policy updates, lessons learned, and best practices

This year attendees can optimize their GridSecCon experience and chose breakout sessions from six conference tracks: cyber or physical security, supply chain issues, diversity and inclusion, human performance, and security policy matters.

Follow us on:

We Are All Connected!

These engagements are about building relationships with our stakeholders so we are all successful!

Tell Some Stories!

"STORIES ARE JUST DATA WITH A SOUL."

DR. BRENÉ BROWN – UNIVERSITYOF HOUSTON

National Standard of Canada for Psychological Health and Safety in the Workplace

Reliability First
5th Annual Human Performance Workshop

August 4 2022

Mental Health Commission of Canada
Commission de la santé mentale du Canada

Our Purpose

Inspiring hope:

Our *lives depend* on it.

Mental Health

What the data is telling us

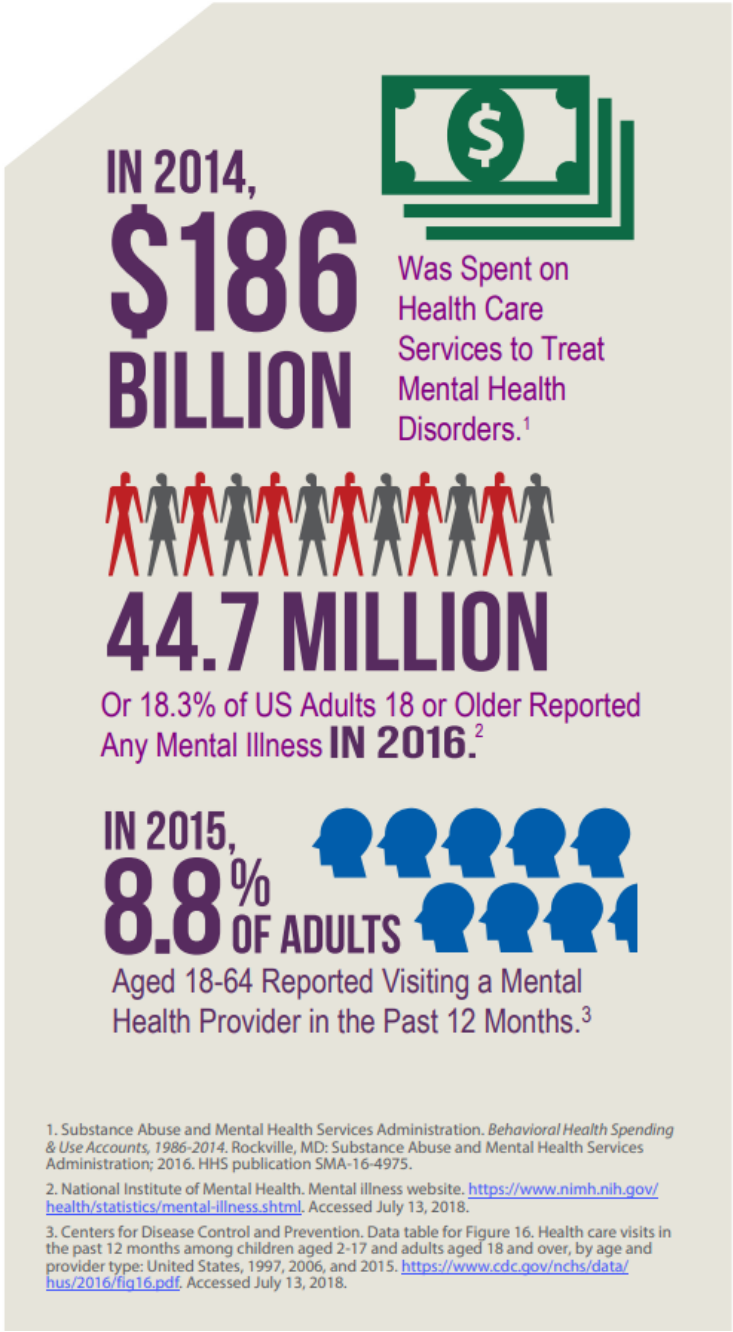
Mental Health

- A **state of well-being** in which the individual realizes his or her own **abilities**, can **cope** with the normal stresses of life, can **work** productively and fruitfully, and is able to make a **contribution** to his or her community.
- In this positive sense, mental health is the **foundation of well-being and effective functioning** for an individual and for a community.

Mental Health Commission of Canada
Commission de la santé mentale du Canada


1 in 3

Mental Health in the U.S.A.



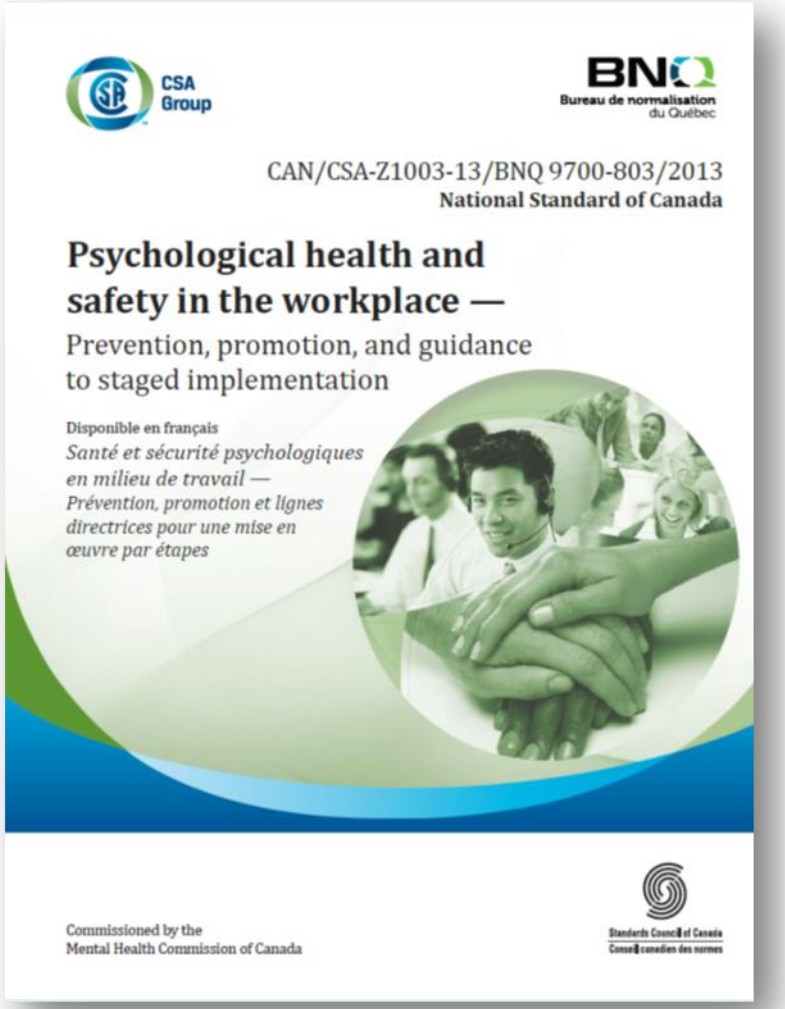
Mental Health System

Workplaces

Canada’s National Standard

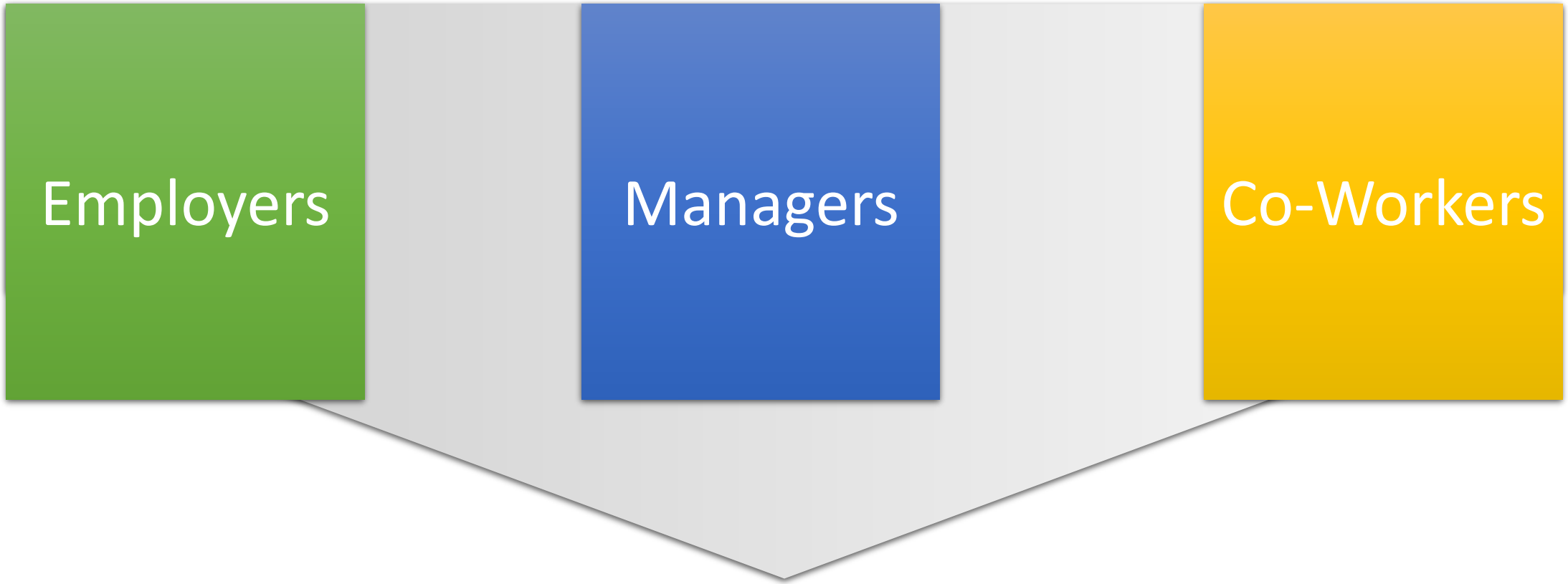
Voluntary Guidance for Psychological Health and Safety in the Workplace

A voluntary framework for creating and sustaining a psychological health and safety system.



A workplace that **promotes** worker's psychological well-being and actively works to **prevent** harm to worker psychological health including in negligent, reckless or intentional ways.

PHS in the WORKPLACE



All have a role to play!

5 Pillars to Your Workplace Mental Health Strategy

Programs

- Workplace awareness campaigns
- Occupational health services department
- Integrated wellness program
- Peer support programs
- Self-help tools

Policies

- Accommodation policies
- Return to work plans
- Employee recognition
- Space for privacy (e.g. quite room)

Benefits

- EAP or EFAP
- STD & LTD leave
- Paid leave for medical appointments or family obligations
- Prescription drug coverage
- Coverage for psychological services

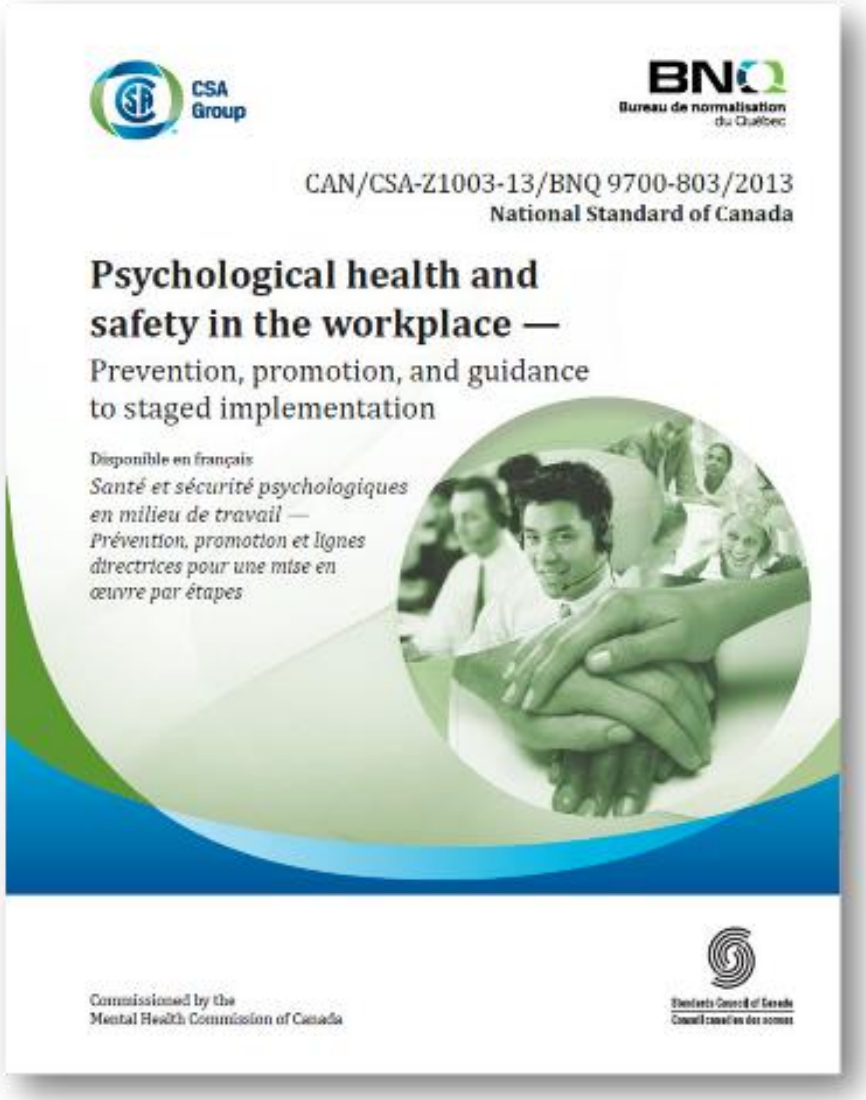
Training

- Resiliency
- Mental health training (e.g. MHFA)
- Anti-stigma training (e.g. The Working Mind)
- Respect in the workplace
- Management training

Assessment

- Employee surveys (Guarding Minds @ Work)
- Interactive Audit Tool
- Mental Health at Work (Excellence Canada)
- Health risk assessments


Commitment, Leadership and Participation
Planning
Implementation
Evaluation and Corrective Action
Management Review

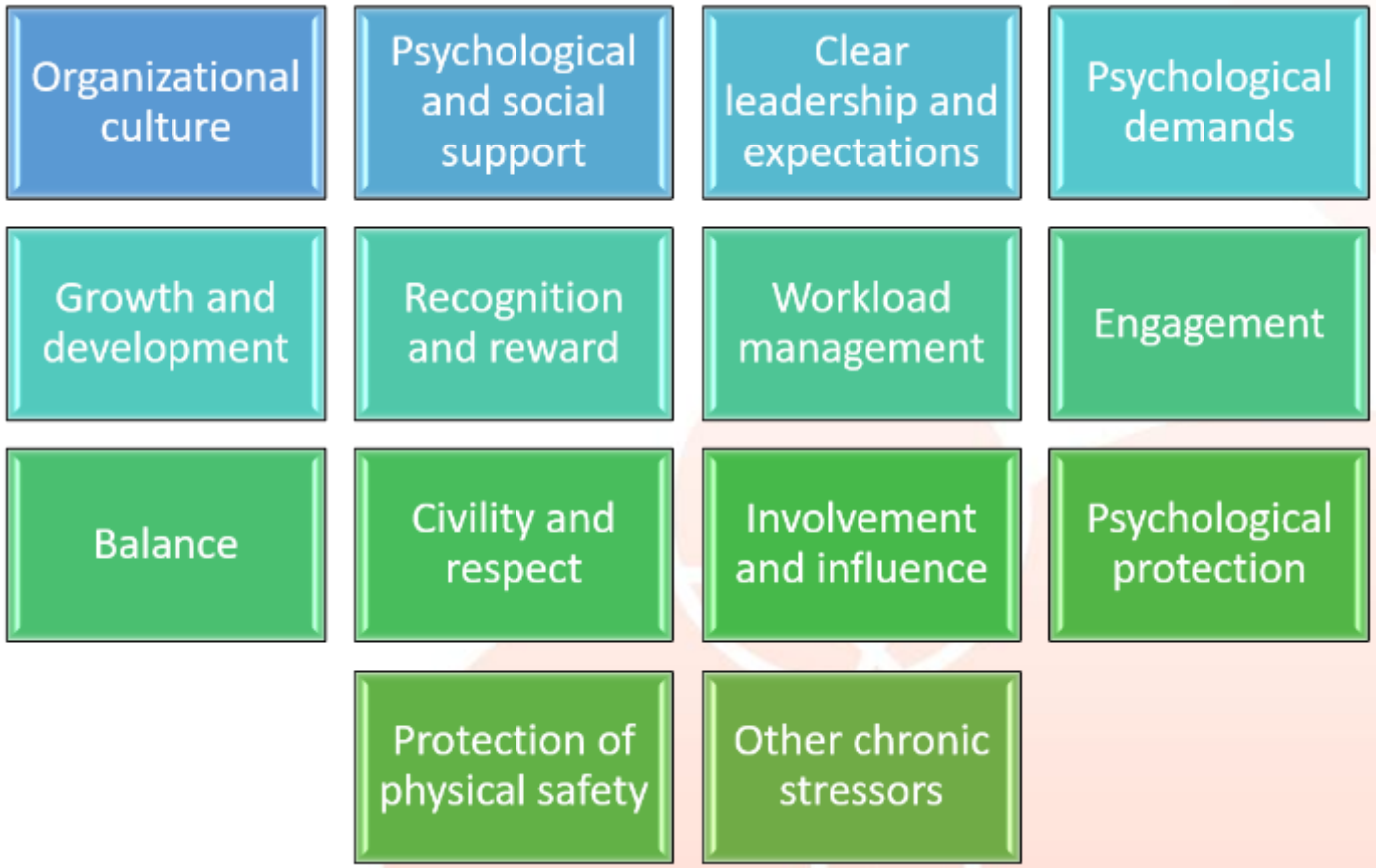

CSA Group
BNQ
Bureau de normalisation du Québec
CAN/CSA-Z1003-13/BNQ 9700-803/2013
National Standard of Canada
Psychological health and safety in the workplace —
Prevention, promotion, and guidance to staged implementation
Disponible en français
Santé et sécurité psychologiques en milieu de travail — Prévention, promotion et lignes directrices pour une mise en œuvre par étapes
Commissioned by the Mental Health Commission of Canada
Standards Council of Canada
Conseil canadien des normes

Risk Mitigation Process

- Hazard identification
- Hazard elimination
- Risk assessment
- Risk control
- Prioritization

Mental Health Commission of Canada
Commission de la santé mentale du Canada

Workplace Factors



Mental Health Commission of Canada
Commission de la santé mentale du Canada

Protection of Physical Safety

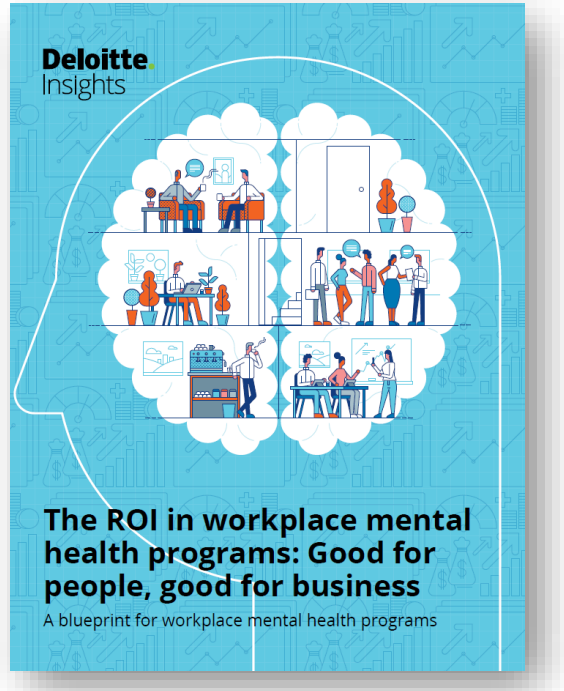
Psychological Protection

Psychological & Social Support

Management System

Evidence of ROI for WMH Strategy

"Mental health programs are more likely to achieve positive ROI **when they support employees along the whole spectrum of mental health,** from promotion of well-being to intervention and care, **as well as the elimination or reduction of workplace hazards** that could psychologically harm an employee."

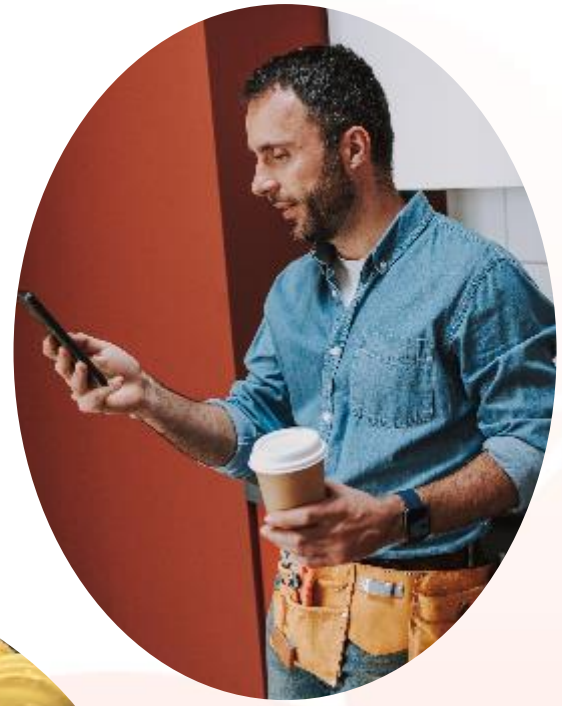


Source: The ROI in workplace mental health programs: Good for people, good for business, Deloitte, 2019

Call to Action

Take a step toward a psychologically healthy and safe workplace

Andriy Blokhin/Adobe Stock



Mental Health Commission of Canada
Commission de la santé mentale du Canada

Need More Help?

- Visit the MHCC website for more info and links to helpful resources
- Book a webinar or training for your workplace
- Contact us to discuss your support needs or to schedule an internal PHS audit

Thank you

Liz Horvath
Manager, Workplace Mental Health
lhorvath@mentalhealthcommission.ca

Mental Health Commission of Canada
Commission de la santé mentale du Canada

Inquire
Inspire
Improve

Human Performance– Emerging Threats to the BES (CIP)

David Sopata Principal Reliability Consultant

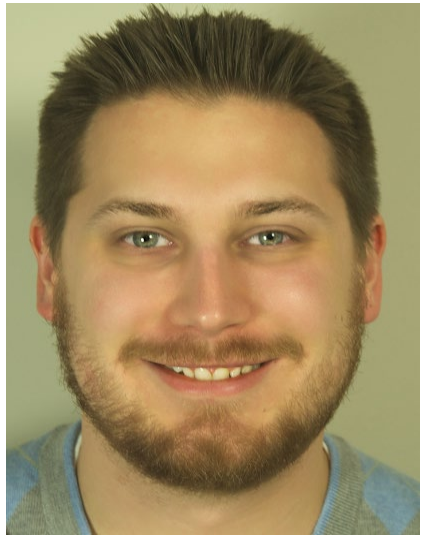
August 4, 2022

Limited Disclosure






A little bit about me



David Sopata, **CISA, CISSP, GIAC GRID**

Principal Reliability Consultant, Entity Engagement, ReliabilityFirst

David joined ReliabilityFirst in 2012, and has participated in appraisal engagements, leads and participates in certification reviews, participates in outreach efforts such as assist visits, and provides guidance to entities in CIP compliance, internal controls and helps in the development of maturity models and security assessment tools. David was a CIP Auditor until 2014, where he participated in and led multiple NERC CIP audits, helped in developing the appraisal model, and participated in the first early appraisal assessment pilots. David previously worked at a security consulting firm for 4 years and has several cybersecurity and auditing certifications. David holds a Bachelors degree in Information Security.

Agenda

- IEEE-NERC Security Integration Project
- How to define threat and how does it relate to risk and vulnerabilities?
- Current tools to help communicate threat and threat groups
- Discussion of different threats that are affecting common IT and OT/ICS systems
- Potential ways of operationalizing threat information to help with incident response

IEEE-NERC Security Integration Project Overview

- Integrating security and engineering practices
- Identified by both NERC and IEEE PES leaderships as a high priority topic
- Fast-track project sponsored by IEEE technical committees and NERC created to publish report by Q4 2022

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

IEEE PES
Power & Energy Society®

What is Threat?

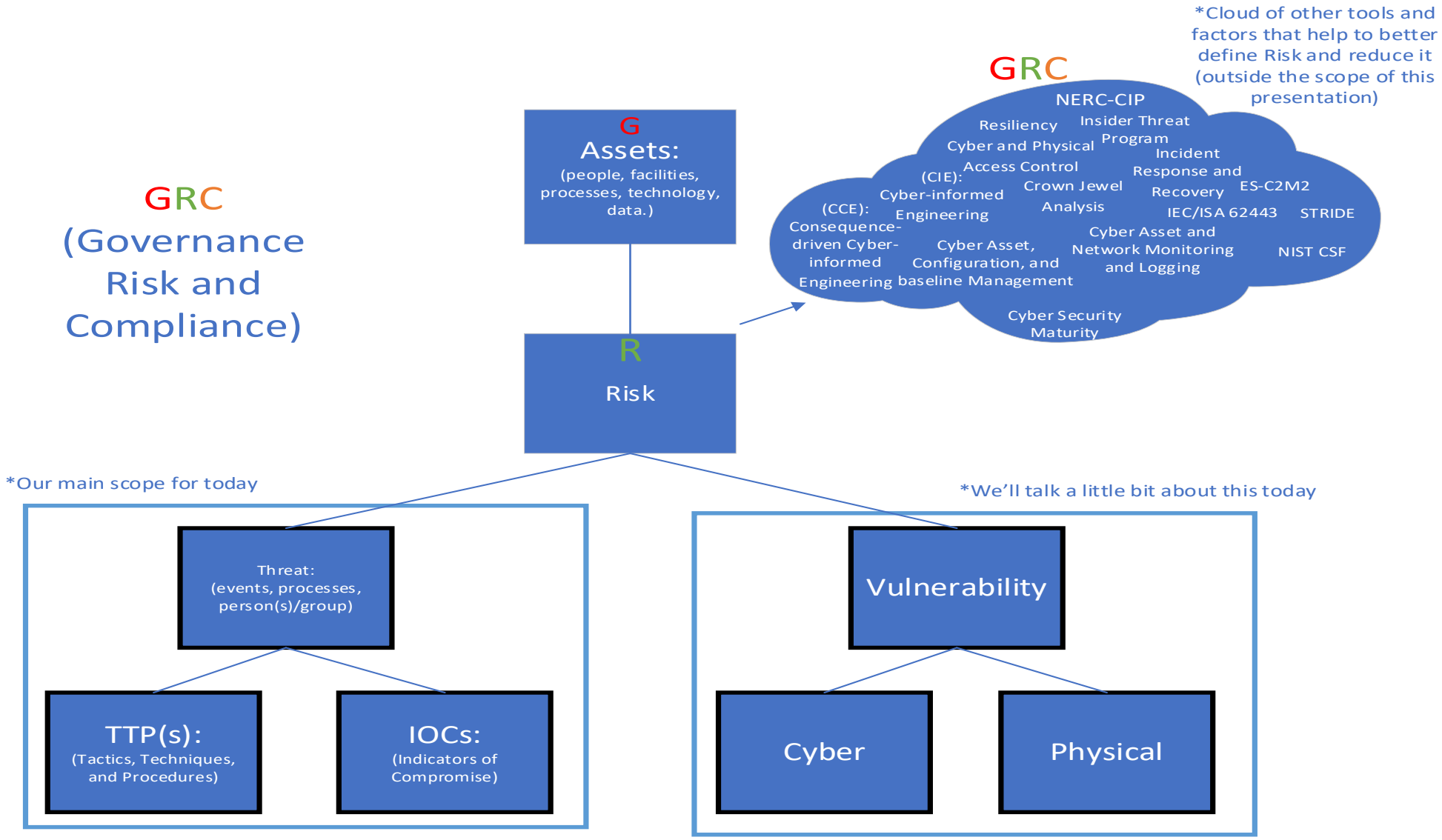
- **Knowing the difference between risk, threat, and vulnerability can be very challenging as people within industry and cybersecurity use these interchangeably.**
  - Risk
    - "is the potential for loss, damage or destruction of assets or data caused by a cyber threat."
  - Vulnerability
    - "a weakness in your infrastructure, networks or applications that potentially exposes you to threats."
  - Threat
    - "is a process that magnifies the likelihood of a negative event, such as the exploit of a vulnerability."

https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/

Limited Disclosure

Relationship of Threat in GRC

GRC (Governance Risk and Compliance)



**Note - Using the generic definition of asset, cyber asset, and facilities not the NERC Glossary definitions.

Preparing for the Future through the Past

- **Threat Analysis and Threat Intelligence is based off information from the past to help us prepare for a future potential incident**

- **Threat Information sharing through organizations like the E-ISAC and other sources helps the industry work on fresh, applicable, and actionable information**

- **Organizations prepare for an incident by having good incident response plans, collection capabilities, tools, and playbooks to analyze and act upon this information during and after an incident**

MODELS FOR COMMUNICATING THREAT

Value, Maturity Scale and Pyramid of Pain

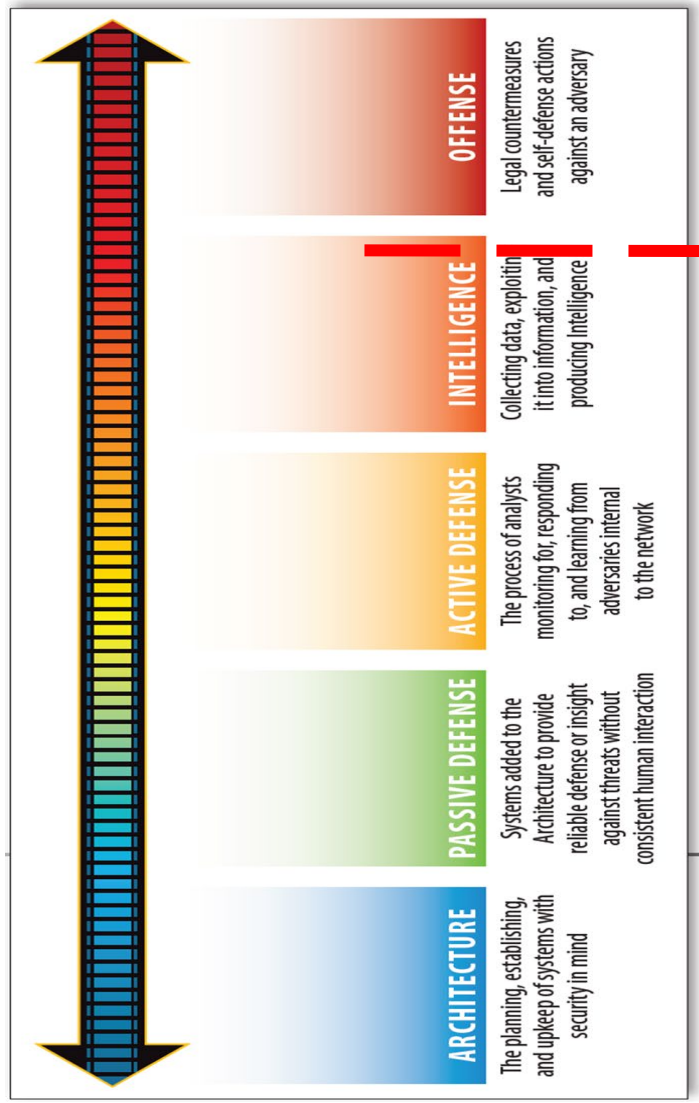
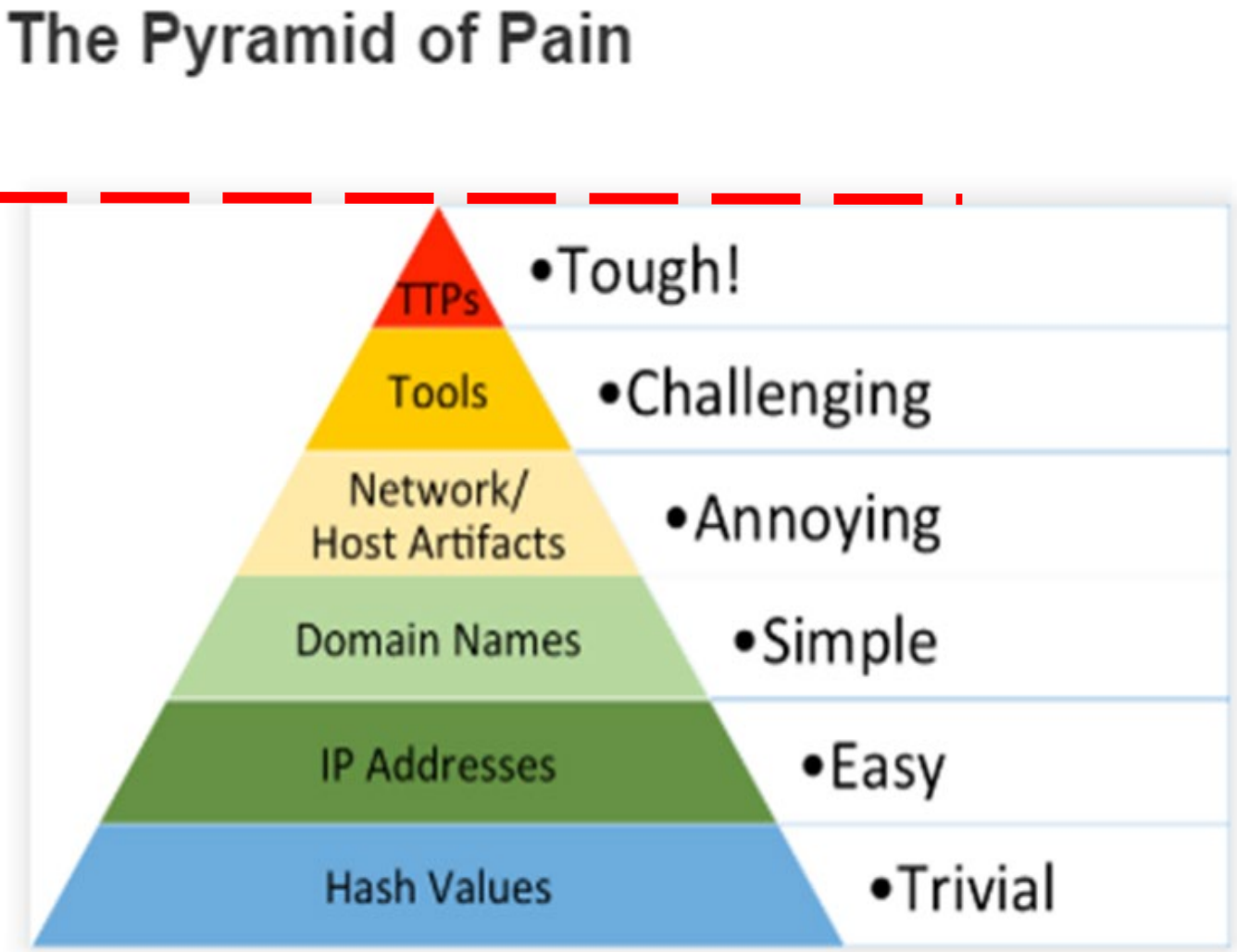


Figure 1. The Sliding Scale of Cyber Security



https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

* TTPs are Tactics, Techniques and Procedures

Limited Disclosure

ICS Cyber Kill Chain

- The original Cyber Kill Chain was developed by Lockheed Martin to be able to better communicate the stages an advisory would take during an attack campaign.
- In 2015, SANS came out with an updated version specific for ICS environments creating a stage 1 (this follows the original would equate compromising the Entity's Corporate Environment) and stage 2 where material attacks on the ICS environment actually take place (this would equate to compromising the EMS/GMS, Substation, generation plant, etc.).

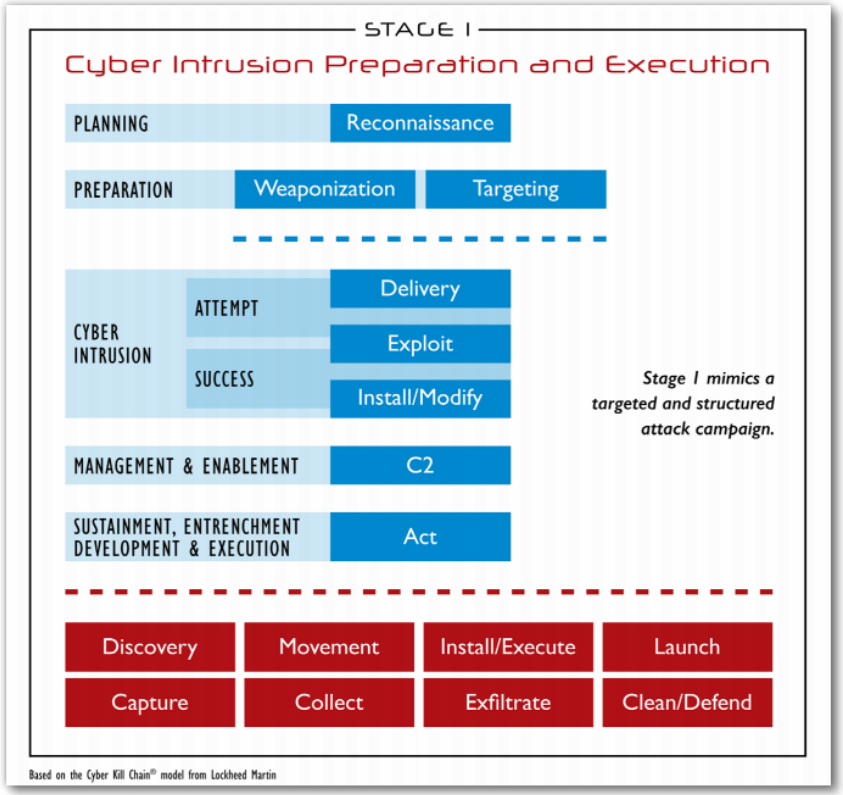


Figure 1. Stage 1: Cyber Intrusion Preparation and Execution

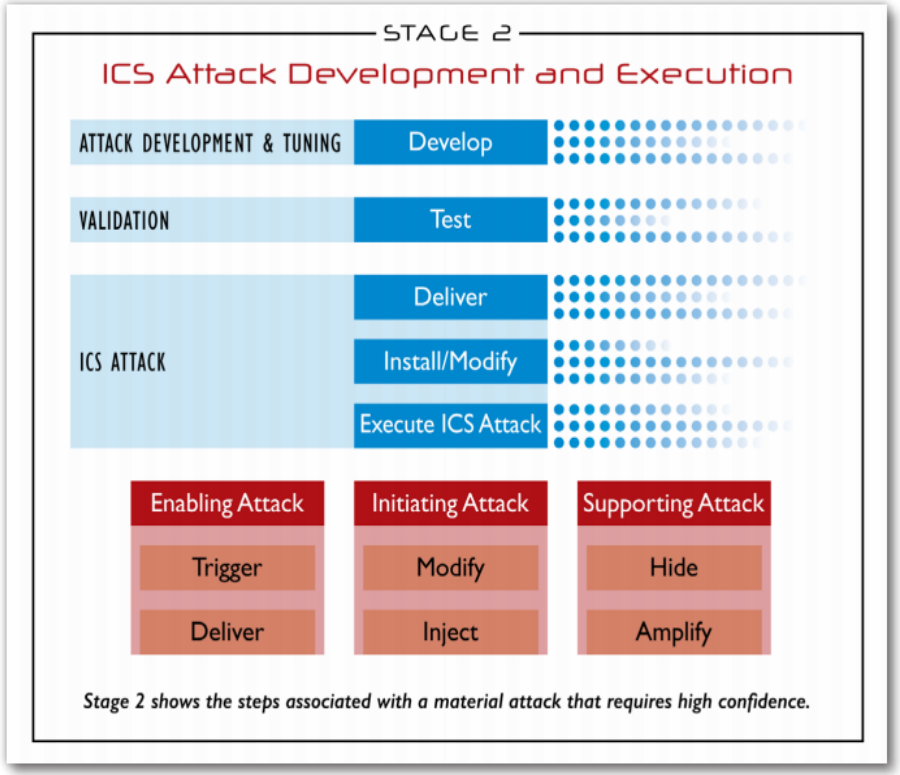


Figure 2. Stage 2: ICS Attack Development and Execution

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Enterprise and ICS MITRE ATT&CK®

SANDWORM Stage 1 Capability (Enterprise MITRE ATT&CK® Framework)

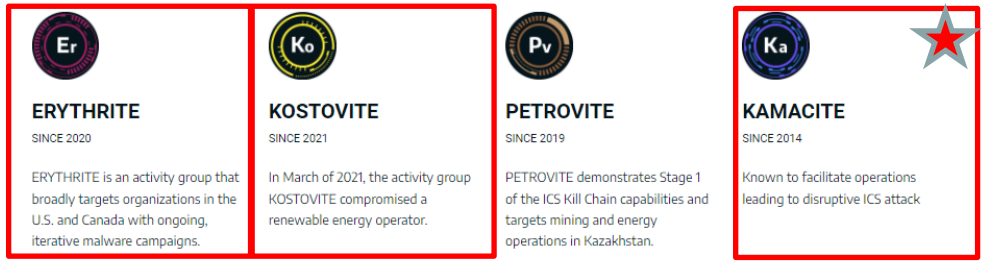
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					

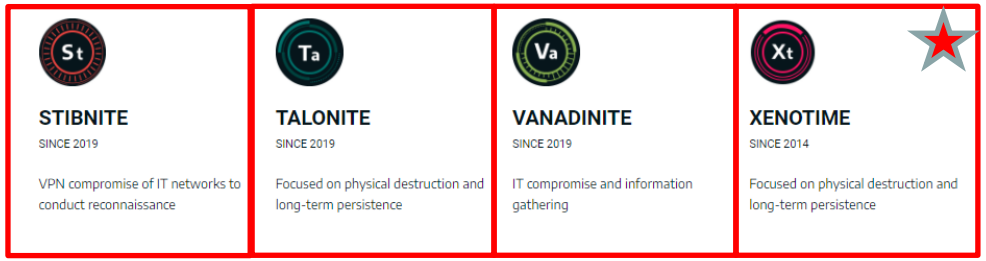
ELECTRUM Stage 2 Capability (ICS MITRE ATT&CK® Framework)

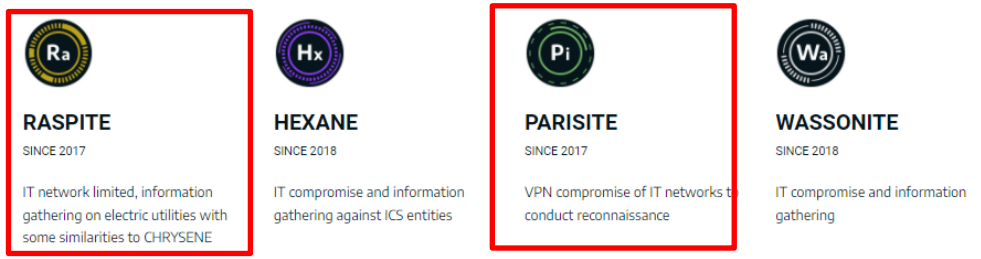
ICS Initial Access	ICS Execution	ICS Persistence	ICS Evasion	ICS Discovery	ICS Lateral Movement	ICS Collection	ICS Command and Control	ICS Inhibit Response Function	ICS Impair Process Control	ICS Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		

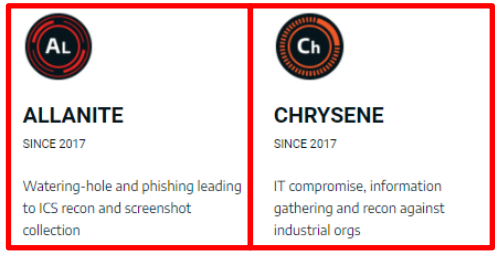
https://mitre-attack.github.io/attack-navigator/enterprise/
https://www.dragos.com/mitre-attack-for-ics/
https://www.dragos.com/resource/mapping-industrial-cybersecurity-threats-to-mitre-attack-for-ics/

ICS Threat Groups from Dragos and ICS MITRE ATT&CK®









Legend:

- Targeted Energy industry and USA/North America
- Have shown high TTP capability in stage 2

*Note, All of these groups have bridged the knowledge/technical gap from Stage 1 (Enterprise IT) to Stage 2 (ICS)
*There are a total of **129 known threat groups** for the Stage 1 tracked on Enterprise MITRE ATT&CK® site.

https://collaborate.mitre.org/attackics/index.php/Groups
https://www.dragos.com/threat-activity-groups/

Limited Disclosure

Common Threat Group/Actor Categories

- Insider
- General Hacker
- Organized Crime/Ransomware
- Spammers/Phishers/Scammers
- Terrorists/Activists
- Foreign Intelligence Services/Nation State
- Industrial Espionage/Sabotage

Limited Disclosure

Threat Categories

- **Ransomware**
  - Ransomware vs. wipers
  - Multiple threat actors with different goals
- **Software Supply Chain**
- **Insider Threat**
  - Malicious vs. Unwitting Insider
    - *Could be the catalyst for initial compromise for other threats or threat actors
- **Emerging/Disruptive Technology**
  - Cloud Computing
  - Drones
- **Physical Attacks**
  - Metcalf

Limited Disclosure

TRISIS/TRITON/Triconex Attack

Threat Group: XENOTIME/TEMP.Veles

- Attacked a specialized Safety Integrated System (SIS) that are specialized systems that intervein at the process level to protect people, processes, and equipment
- Attack **reached Stage 2 (OT)** at an oil refinery environment
- **Highly targeted, requiring**
  - deep understanding of the technology and process being impacted
  - Large amount of time and resources likely with nation-state backing
- **Was a near miss in accomplishing their perceived goal of damaging equipment and causing harm to people.**
  - Showed this type of attack is possible

https://www.dragos.com/wp-content/uploads/relocated/t/Threat_Group_Trading_Cards_XENOTIME_XENOTIME-731x1024.png

https://attack.mitre.org/groups/G0088/
https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

Limited Disclosure

SIS and PS similarities

- **Safety Instrumented Systems (SIS) and Protection Systems (PS) are similar in that They both have:**
  - A goal of ensuring that equipment fails in a fail-safe mode to protect the overall system or process.
  - Work at level 1 and 0 of the Purdue Model
  - Serial and network-based communication and management ports for:
    - Configuration and Calibration Management
    - Logging, alerting, and monitoring
    - Access Control
  - Requires another workstation (permanent or transient) to interact with it or can potentially be accessed remotely through the network (Purdue Model Level 2)
  - Guidance on designing, testing, and maintenance programs

https://collaborate.mitre.org/attackics/index.php/Safety_Instrumented_System/Protection_Relay
WG I-25 Commissioning _Testing of Protection Systems 5-10-2017.pdf (pes-psrc.org)
What is a Safety Instrumented System? - English | AIChE

Mapping the TRISIS Attack and 11/2/2021 Joint Review of Protection System Commissioning Programs

TRISIS Best Practices

- Start with advice from the vendor
- SIS should be deployed on isolated networks
- Controls to prevent physical unauthorized physical and logical access. Safety controls, equipment, or safety network
- Workstation, and software used to connect to the SIS systems should be secured
- Removable and transient cyber assets should be controlled and sanitized for potential malware prior to connecting to the SIS
- For SIS that have a programming and running mode it should be changed to running to prevent malicious or accidental modifications to configurations

https://attack.mitre.org/groups/G0088/
https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

PSC Program Observed Best Practices for Consideration

- **Included the cyber security experts as participants in the commissioning process.**
- As part of the commissioning process on tie lines, some participants employed back-to-back relay testing (i.e., testing in a laboratory environment) and end-to-end testing onsite.
- Required the commissioning group to review the settings and logic issued by the design engineering group.
- Ensured that the engineering drawings package identified all equipment that needed to be isolated or shorted to ensure adequate in-service protection throughout all stages of the project.
- Reported that when using a third-party contractor, it requires a company subject matter expert to review the commission test results before placing the equipment in-service.

Limited Disclosure

Protection System Commissioning Program Review Project.pdf (ferc.gov)

Recap

- Know the difference between risk, threat, and vulnerabilities and how threat fits into Governance, Risk, and Compliance (GRC)
- Understand what Tactics, Techniques and Procedures (TTPs) are and how easy/hard those are to change for the attacker
- Difference between Stage 1 and Stage 2 of the ICS Cyber Kill Chain
- High-level understanding of the known ICS threat landscape
- High-level understanding of some of the threat categories

Now I can talk about threats, how do I operationalize it to improve my cybersecurity program?

https://mitre-attack.github.io/attack-navigator/enterprise/
https://www.dragos.com/mitre-attack-for-ics/
https://www.dragos.com/resource/2021-year-in-review/
https://www.dragos.com/resource/mapping-industrial-cybersecurity-threats-to-mitre-attack-for-ics/

Operationalizing Threat Management

➢ Asset and Configuration Management

- Understand what assets are critical to your BES operations, mission, and business (Business Impact/Crown Jewel Analysis)
- Configuration baselines of cyber systems and cyber assets that are critical
- Network traffic baselines (what cyber assets should be talking to whom?)
- Increased collection capability of logging and monitoring of cyber systems, assets, and network traffic (Alerts, logs, Network Packet Captures/Netflow) i.e. **Increasing IT Situational Awareness**

Operationalizing Threat Management Cont.

➢ Tabletop Exercises

- Based on current threat groups and threat categories by operationalizing real or simulated incidents (The ICS and Enterprise MITRE ATT&CK framework can help)
- Using the DHS/FEMA Homeland Security Exercise and Evaluation Program (HSEEP) and the CISA version for Cybersecurity (CTEP) frameworks
- Tool examples
  - RF has developed an Incident Response Assessment Tool (IRPAT). Please visit the https://www.rfirst.org Contact Us page and choose Resilience from the list of Areas.
  - Dragos Tabletop Exercise https://www.dragos.com/tabletop-exercise/
  - Backdoors & Breaches from Black Hills Security https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/
  - NUARI DECIDE Platform https://nuari.net/decide/

Note: This is not an endorsement of these tools or companies.

https://www.cisa.gov/sites/default/files/publications/2%20-%20CTEP%20Exercise%20Planner%20Handbook%20%282020%29%20FINAL_508.pdf

Operationalizing Threat Management Cont.

➢ Threat Reporting

- The more we share as an industry, the more we can help each other with being able to detect, respond, and contain potential threats effectively and quicker.
  - This was a hard lesson learned from the Financial Industry with the FS-ISAC back in 2009-2012 timeframe with a rampant up-tick in account takeovers and DDoS attacks
- Some reporting is required through CIP-008, EOP-004, and DOE OE-417 standards.
- The Electric Information Sharing and Analysis Center (E-ISAC) https://www.eisac.com/
  - Provides resources and services for members to share and communicate threat intelligence information with peers within the Industry

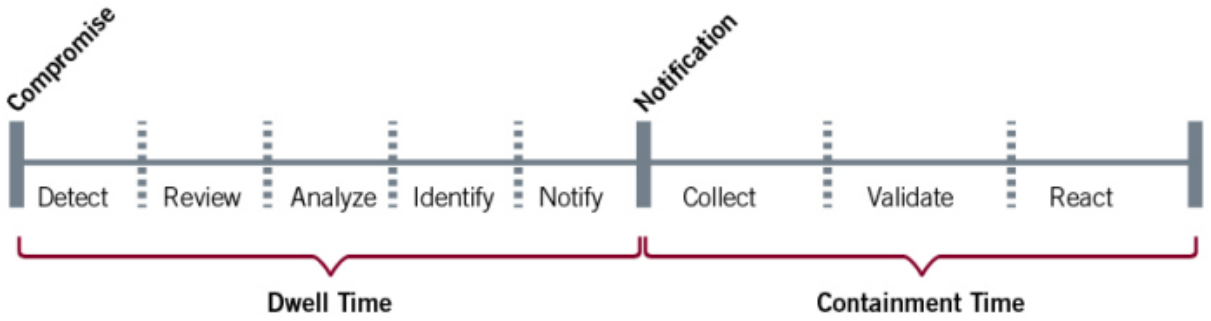
https://www.bankinfosecurity.com/interviews/bill-nelson-i-1758

Operationalizing Threat Management Cont.

➢ Improving Incident Response Metrics from Mandiant

Time	Category	Measurement	Benefit
Dwell	**Detect**	Time from initial entry into the system/network to detection	Measures the effectiveness of detection systems and capabilities
	Review	Time from detection of the incident to analyst for review	Determines if staffing level is properly sized
	Analyze	Time to analyze the incident	Determines if the organization has the right expertise and tools and if the right escalation occurs
	Identify	Time to identify the affected assets, location, and owner	Measures the effectiveness of asset inventory
	Notify	Time to successfully notify appropriate contacts	Measures the effectiveness of contact database and communication plan
Containment	**Collect**	Time to collect live response data	Determines if the right tools are deployed to assist in collection
	Validate	Time to validate intrusion based on collected data	Determines if the right skill sets are in place at each level
	React	Time to react (contain, remove, etc.)	Determines if the right definition of remediation exists and if it is applied consistently

Table 1: DRAIN CVR Definitions



$$f((D + R + A + I + N) + (C + V + R))$$

* Can use these metrics during tabletop exercises and attack simulations

https://www.nist.gov/system/files/documents/2016/09/16/mandiant_rfi_response.pdf

Questions & Answers

Forward Together ReliabilityFirst

Limited Disclosure

WHEN GOOD IS TOO GOOD

Brian Hattery, Planning & Engineering Supervisor

Transmission Field Services, AEP

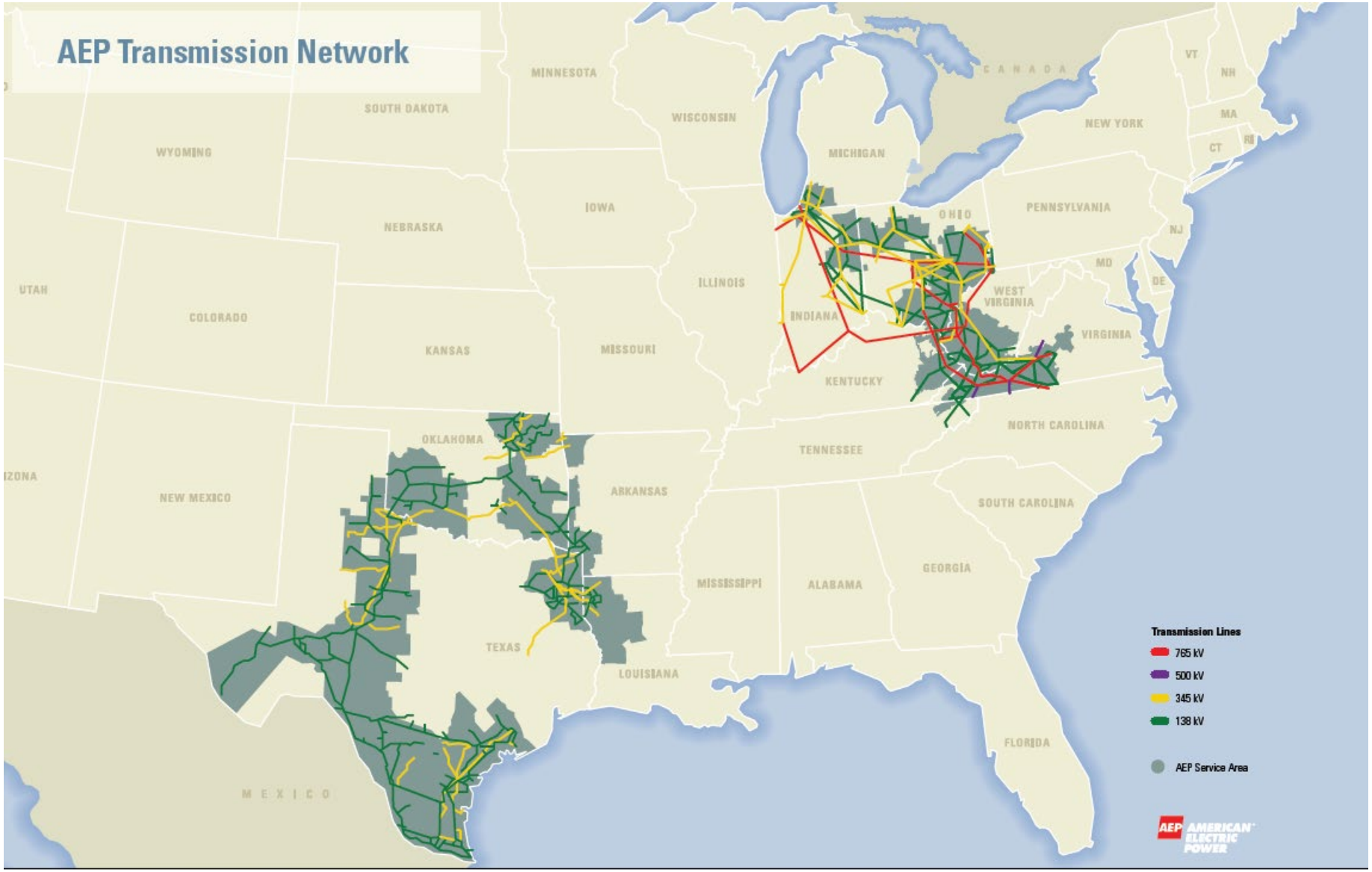
AEP Background Info

- American Electric Power has
  - Nearly 5.5 million regulated customers in 11 states
  - 40,000 miles transmission line and 223,000 miles of distribution lines
  - More 765 kV line than all other US systems combines

- Concerning batteries, AEP Transmission has
  - More than 3,000 substations
  - Over 3,800 stationary battery systems
  - Of those battery systems, over 60% are NERC applicable
  - Approximately 300 VRLA type on the system
  - All remaining are VLA

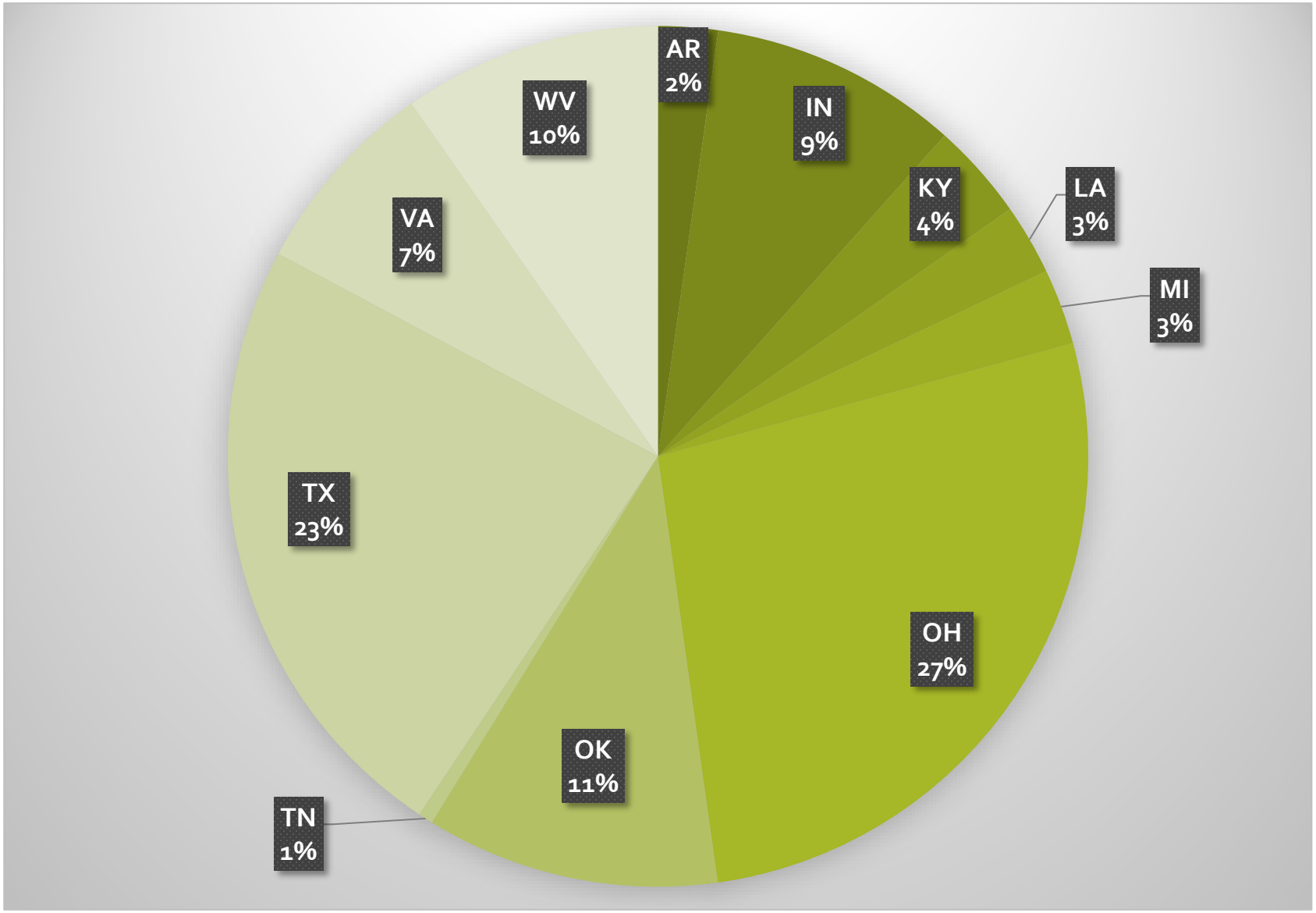
AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

AEP Transmission



AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

AEP Substations by State



AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

DC Supply & AEP-T

- Field oversite -
  - DC Supply commissioning and maintenance practices are overseen by Transmission Field Services – Station Policies and Procedures team and the DC Supply working group
  - The Station P&P team establishes commissioning and maintenance policies and acts as a go-between for the field and the equipment standards groups
  - The working group is lead by P&P and consists of field and standards personnel and meets regularly
  - Discussions include problems, maintenance practices, updates, and policy changes

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

DC SUPPLY MAINTENANCE PRACTICES

Maintenance Practices

- Prior NERC PRC-005…

Good

- Internal ohmic testing was happening in all regions
- Testing regularly, annually or bi-annually

Bad

- Each area had it's own standards
- Different test sets used
- Different test results
- Testing jars only
- No intercell connection tests

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

Response to PRC-005 - Standardization

- AEP transmission focused on standardization across all regions
  - A test set for all areas was chosen
    - Funds were secured to provide all areas with the test set
  - New testing standards and maintenance practices were written
    - Now testing individual cells and intercell connections
    - Expected test values were developed as a guide (using conductance)
  - All areas personally received the test sets and training in 2012.

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

Response to PRC-005 - Test Criteria

- Testing criteria was developed as part of the standardization
  - Cell conductance
    - 70% of expected conductance – Warning
    - 60% of expected conductance – Failed
  - Intercell connectors
    - Greater than 100 uOhms – Warning
    - Greater than 500 uOhms – Failed
  - Response actions and time-frames are dictated by the degree of failure

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

Response to PRC-005

- To ensure NERC compliance, AEP transmission…
  - Uses an accelerated maintenance schedule
    - Bi-monthly checks to cover 4 calendar month tasks
    - Annually maintenance to cover the 18 months tasks
  - Uses a layered approach to analyzing test results
    - Test personnel reviews results before leaving the station
    - An internally created software analyzes the results and flags concerns
    - A local field engineer reviews the analysis and raw test results and takes action from there
    - The local field engineer is ultimately responsible for NERC compliance of batteries in their area

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

HOW GOOD BECAME TOO GOOD

New Employee, Fresh Eyes

- At the end of 2018, a new field engineer was hired within an area of AEP
- As part of his new duties, he was trained on how to test batteries and review the results
- During his first review of battery test results in spring of 2019, he noticed certain batteries in his area had abnormally low test results for the intercell connections
- He asked his supervisor, who had trained him, why the results were so low on some batteries, which triggered an investigation

Cell #	Strap
CELL01	1
CELL02	3
CELL03	1
CELL04	3
CELL05	3
CELL06	1
CELL07	3
CELL08	1
CELL09	3
CELL10	2
CELL11	1
CELL12	1
CELL13	1
CELL14	2
CELL15	4
CELL16	4
CELL17	3
CELL18	3
CELL19	3
CELL20	1

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

The Investigation

- The field supervisor initiated an investigation which determined:
  - In his region, a number of batteries had intercell connectors test abnormally low
    - <10 uOhms, when the expected range was 20-80 uOhms
  - All tests were performed by the same individual (who we'll call "Steve")
  - Steve had been performing annual battery tests since 2012 (and earlier), when the new standards were established
  - Steve was asked to demonstrate his testing procedures

Typical Test Process

The test begins with an internal cell test

- Then an intercell connection test is performed
- The connection resistance is determined by finding the difference between the tests

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

The Problem

Steve performed the internal cell test correctly

- However, when the Steve performed his intercell connection test, he placed his test lead on top of the connector
- This essentially left out the resistance of this connection point

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

The Results

- The investigation result
  - Steve believed he had been performing the tests correctly since 2012
  - He was genuinely surprised to learn he had been performing the tests incorrectly
  - Internal meetings were held with different compliance groups
    - It was determined that for every NERC applicable battery that Steve tested, potentially multiple violations had occurred
    - AEP self-reported to NERC

The Violation

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Protection System Station dc supply using Vented Lead-Acid (VLA) batteries not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

Why was this Missed?

- The new field engineer started reviewing test data in 2018 – Why wasn't this caught earlier?
- The previous test reviewer was interviewed
- He had noticed the low test results, but did not think they were a problem
- The testing criteria only discussed high resistance values being a problem
- There was no protocol for test results being "too good"

	Test Day	Test Day	Test Day
	02-21-2017	01-15-2018	03-28-2019
Cell #	Strap (uOhms)	Strap (uOhms)	Strap (uOhms)
CELL01	26	1	25
CELL02	29	3	32
CELL03	25	1	21
CELL04	30	3	27
CELL05	26	3	39
CELL06	32	1	34
CELL07	22	3	42
CELL08	32	1	31
CELL09	27	3	36
CELL10	24	2	32
CELL11	26	1	37
CELL12	28	1	35
CELL13	30	1	27
CELL14	21	2	34
CELL15	24	4	44
CELL16	24	4	36
CELL17	34	3	36
CELL18	40	3	39
CELL19	25	3	35
CELL20	28	1	32
CELL21	37	2	37
CELL22	30	1	25
CELL23	29	2	40
CELL24	33	4	30
CELL25	28	4	37
CELL26	35	4	25
CELL27	28	3	27
CELL28	22	4	17
CELL29	24	2	37

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

The Mitigation

- Starting with Steve
  - Immediately, every battery Steve had tested that year was reexamined
    - Those with questionably low intercell connection resistances were retested and confirmed good
- How far had this spread locally?
  - Test results for all batteries in the region were examined
    - Since Steve had been testing batteries for over 20 years, and was around in 2012 when the new standards were established, he was considered "experienced"
    - He had been asked to train newer employees on battery testing for a number of years
    - However, it looked to be confined to Steve
    - Any other batteries with questionable test results were retested as a precaution

The Mitigation

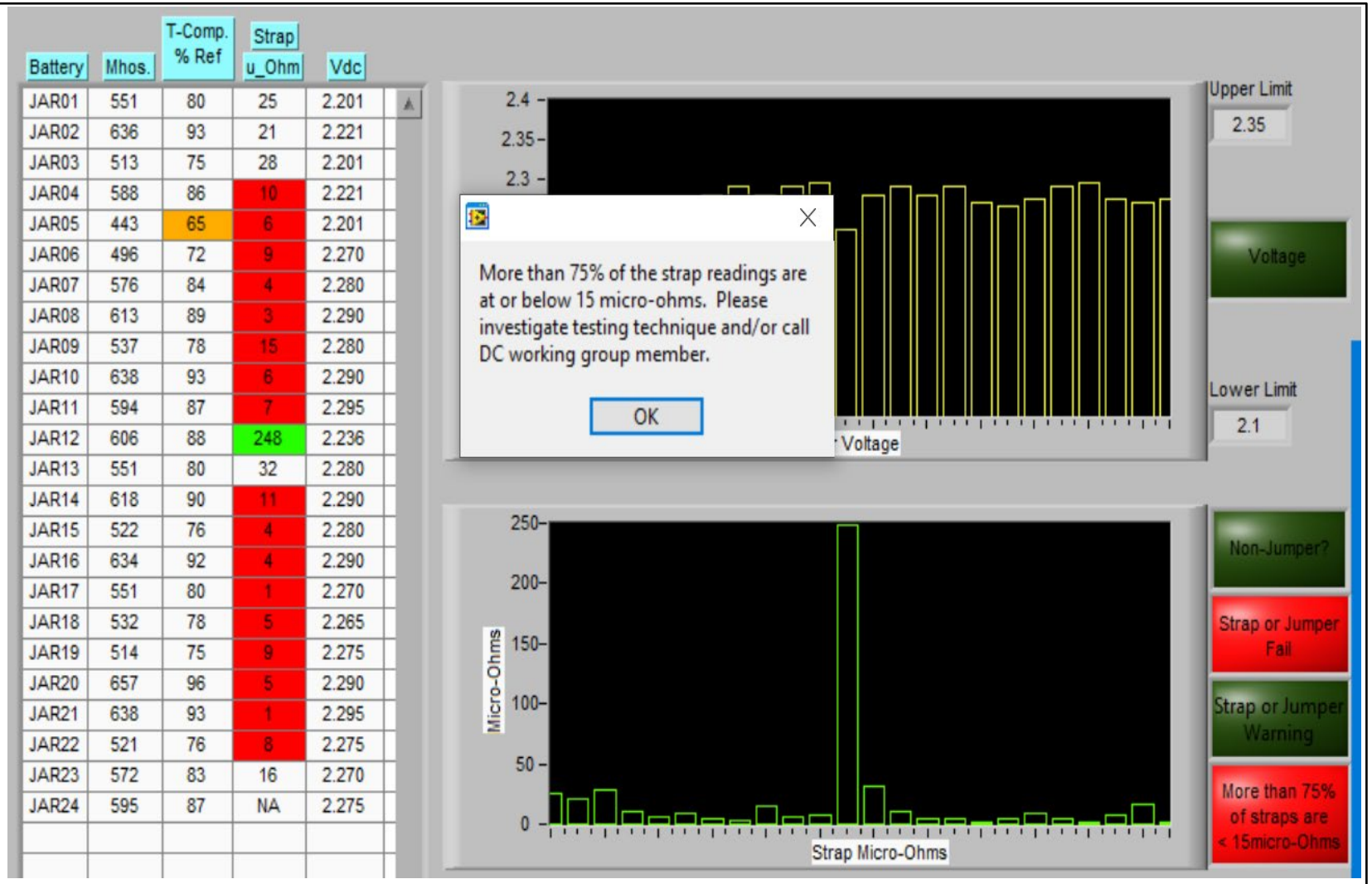
- Did this problem exist anywhere else?
  - Who else may be testing incorrectly in other regions of AEP?
  - A specialized report was created to look through AEP's database of test files to look for low strap values
  - Anything suspicious was investigated by local field engineers, including requesting a demonstration of testing methods
  - The report was then set up to run quarterly. So far, no additional problems have been found.

TFS Are	Battery Location	Asset Name	SSC	Serial Nr	PRC 005 Applicable Version	Test Date	Strap Data
		BATTERY1	APP	10204859	Version 2	1/14/2019	1
		BATTERY#1	RWH	10000	None	3/11/2019	1
		BATTERY	APP	10204590X	None	4/4/2019	1
		BATTERY	APP	1021223	Version 2	2/20/2019	1
		BATTERY1	APP	60V70GI175LA	Version 2	2/11/2019	1
		BATTERY 1	APP	1022506204B	None	2/13/2019	1
		STATION BATTERY	BUC	0204480	None	5/2/2019	1
		BATTERY BANK		10250167/008	ERCOT-T	5/28/2019	1
		BATTERY	APP	P125	None	2/12/2019	1
		BATTERY	HUN	10259110001	Version 2	1/7/2019	8
		BATTERY 1	APP	CB125	None	4/3/2019	1
		BATTERY BANK	RDK	T01275478232012	None	8/28/2019	1
		DICM BATTERY1	APP	DICM1	Version 2	1/16/2019	1
		DICM BATTERY2	APP	DICM2	Version 2	1/17/2019	1
		BATTERY BANK STA_1	AAA	T014100720131106	None	7/24/2019	3
		BATTERY #1	RWH	IND5714	None	4/4/2019	1
		BATTERY	RWH	10289910050	Version 2	1/29/2019	1
		BATTERY 1	APP	R98413	Version 2	3/25/2019	1
		BATTERY1	APP	SP93014	Version 2	2/11/2019	1
		BATTERY BATT	STE	0291581_026	Version 2	1/8/2019	5
		138KV BATTERY 1	APP	JF138252015	Version 2	1/17/2019	1
		STATION BATT	EC1	BATT3028_1	None	3/21/2019	1
		CANYON ROCK BATTERY	AB1	10298011/025	Version 2	6/11/2019	4
		BATTERY	APP	S54452	Version 2	2/27/2019	1
		BATTERY 1	APP	RAD06172015	None	2/7/2019	2
		BATTERY 1	APP	AUST6302015	None	1/24/2019	1

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

The Mitigation

- Additional Mitigation
  - The software that evaluates test results had added programming
  - Any batteries where greater than 75% of the intercell connections were less than 15 uOhms were flagged
  - The test reviewer is required to enter a comment on the flagged results

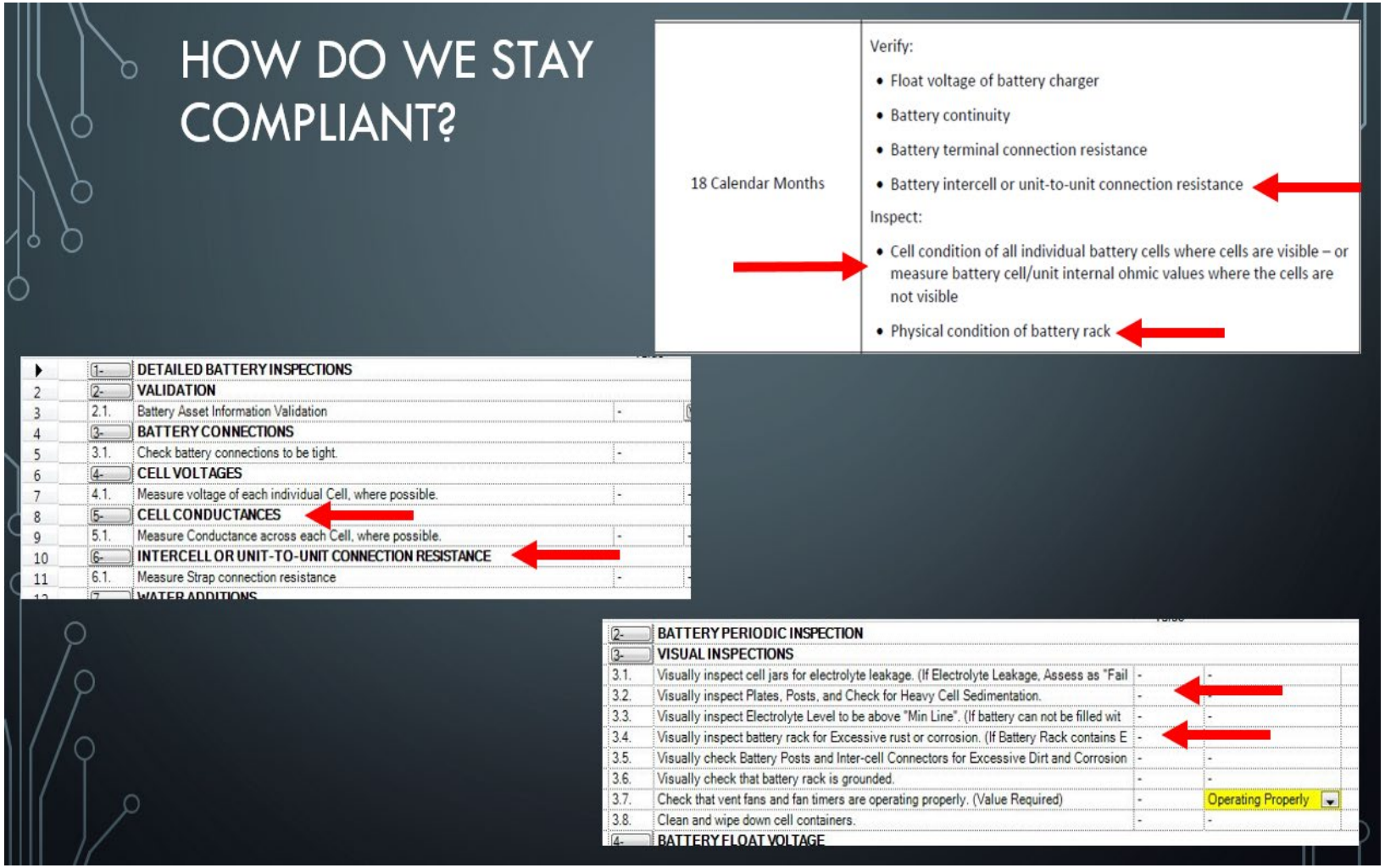


Battery	Mhos.	T-Comp. % Ref	Strap u_Ohm	Vdc
JAR01	551	80	25	2.201
JAR02	636	93	21	2.221
JAR03	513	75	28	2.201
JAR04	588	86	10	2.221
JAR05	443	65	6	2.201
JAR06	496	72	9	2.270
JAR07	576	84	4	2.280
JAR08	613	89	3	2.290
JAR09	537	78	15	2.280
JAR10	638	93	6	2.290
JAR11	594	87	7	2.295
JAR12	606	88	248	2.236
JAR13	551	80	32	2.280
JAR14	618	90	11	2.290
JAR15	522	76	4	2.280
JAR16	634	92	4	2.290
JAR17	551	80	1	2.270
JAR18	532	78	5	2.265
JAR19	514	75	9	2.275
JAR20	657	96	5	2.290
JAR21	638	93	1	2.295
JAR22	521	76	8	2.275
JAR23	572	83	16	2.270
JAR24	595	87	NA	2.275

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

The Mitigation

- Additional Mitigation
  - During 2019, every battery tester and all field engineers were trained on this event and the proper testing techniques
  - All testers were trained on how their actions kept AEP compliant with NERC standards
  - All appropriate battery policy documents were also updated



AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY™

Lessons Learned

- A number of lessons were learned from this experience
  - Do not be too narrowly focused
    - Standards created looked only in one direction – Too High!
    - The question should have at least been discussed if results were too low
    - A conversation and a little imagination could have caught this problem years ago
  - Do not undervalue the importance of a fresh perspective
    - For nearly 6 years this problem was missed!
    - One pair of new eyes easily caught a problem that now can be clearly seen
    - All testing standards have been and are currently being reexamined by a compliance group for any potential deficiencies

Lessons Learned

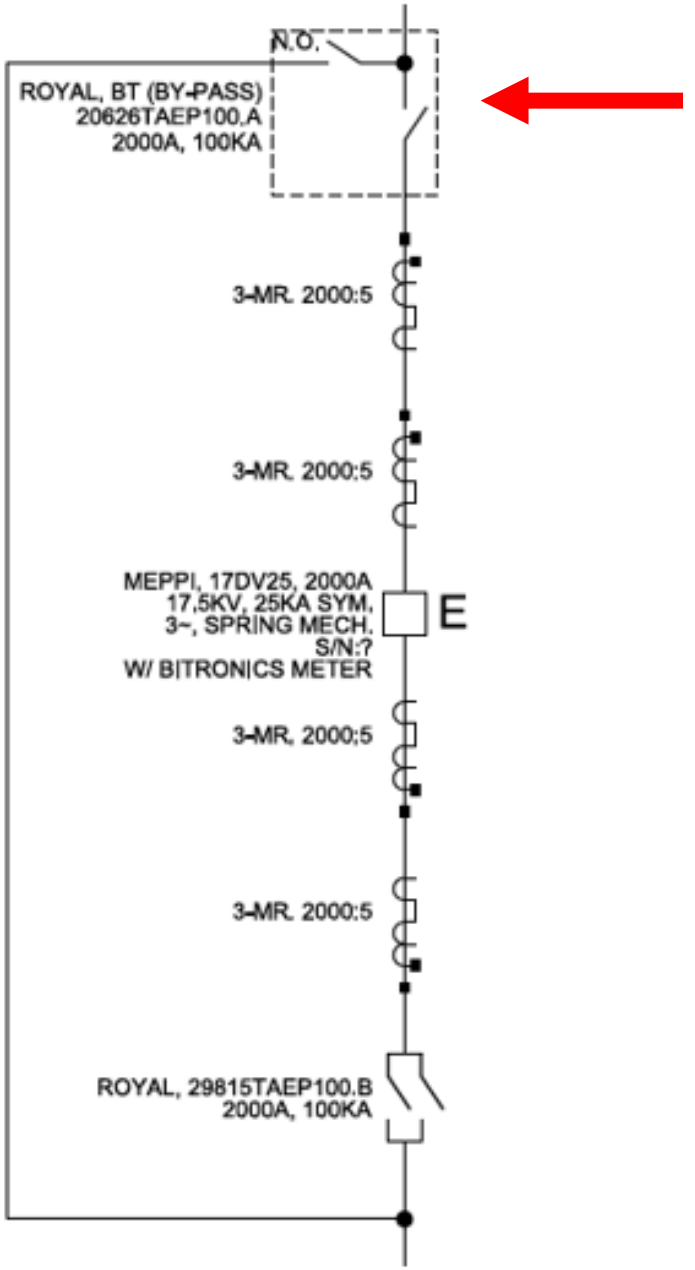
- A number of lessons were learned from this experience
  - You know what they say about assuming…
    - It was assumed for years that because Steve had been taught how to test, and was given a detailed testing guide (with pictures), he knew how to test correctly
    - And he was testing correctly, in every way but one
    - Assumptions are not safe

ROYAL 12 AND 34KV BYPASS/DISCONNECT SWITCH COMBO UNITS

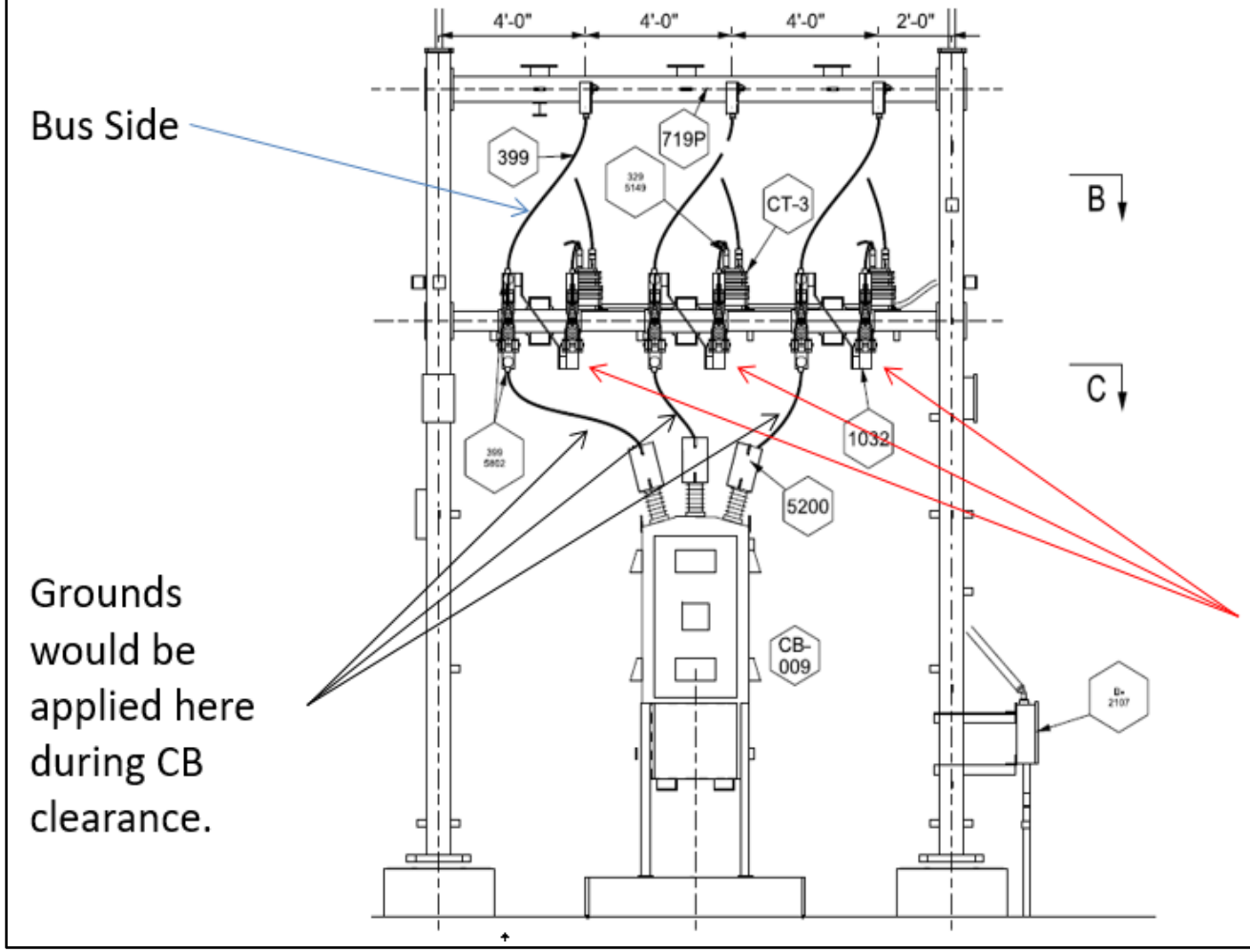
Bonus Content

Disconnect/Bypass Switches

- Beginning around 2017, low voltage construction has utilized a Royal combination switch that encompasses both a breaker disconnect and a bypass switch.
- Depending on the application, the bypass switch may have fuses instead of a solid blade.



On the Physical Prints

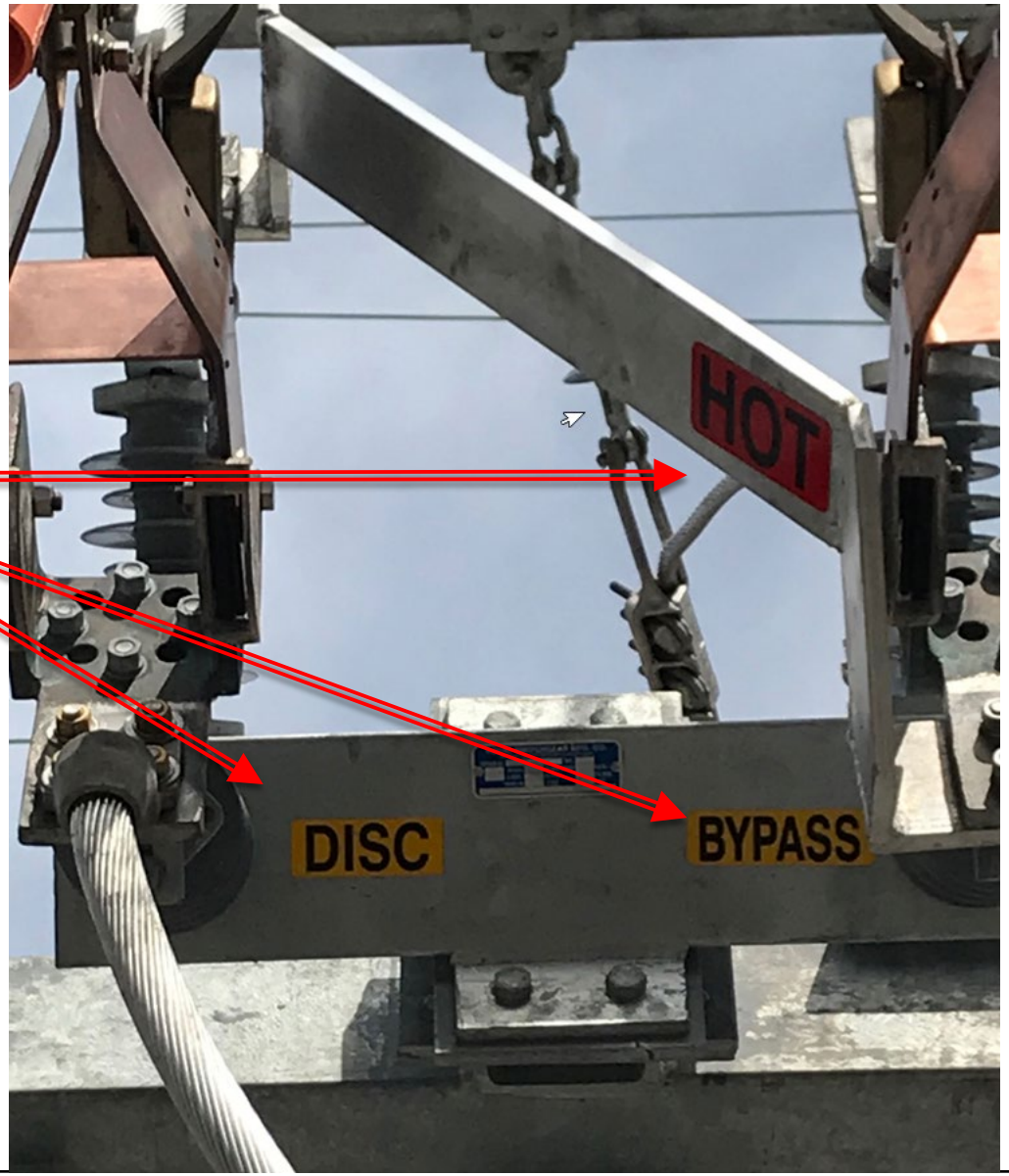


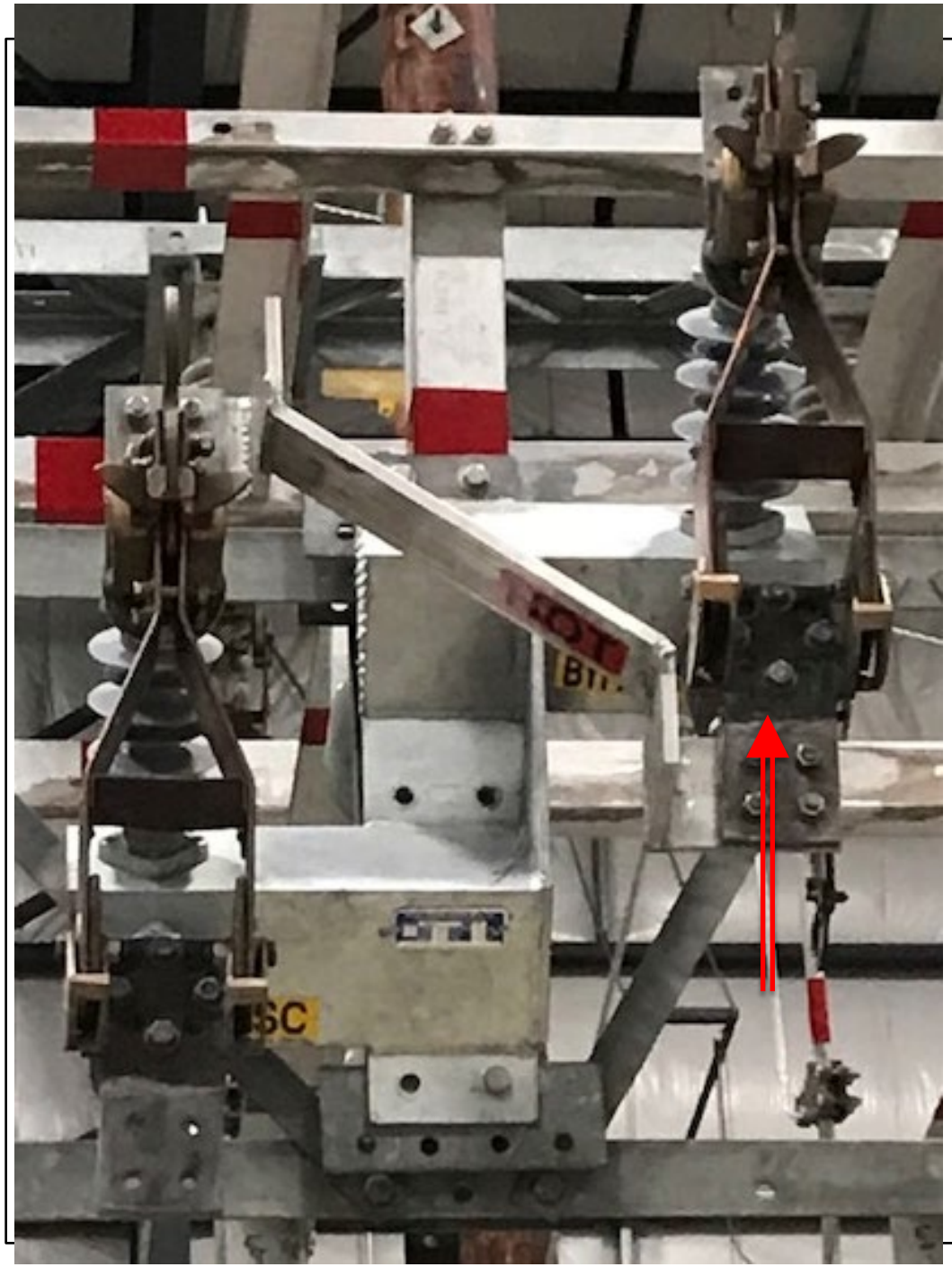
Concerns

- Proximity between ground and energized 12kV requires awareness and planning. Even so, a moments inattention can be very serious.
- Hazard at the time of placing safety grounds, with energized equipment so close.
- Another hazard if working near the top of the VCB such as doing a bushing replacement.
- AND, horizontally adjacent switches have led to switching errors.

12 and 34kV Royal Bypass/Disconnect Switches-Signage

- Mainly installed on Transformer LS totalizer breaker applications.
- The addition of three signs will make the switch functions clearer and aid in hazard recognition for those working in proximity.
- With care, the signs can be placed while the equipment remains in service.





Also, a Re-design

- The disconnect switch is offset lower than the bypass.
- This creates a visible difference meant to minimize switching errors as well as reduce safety hazards on equipment under clearance.
- The switches are on a common frame and mounted as one unit.

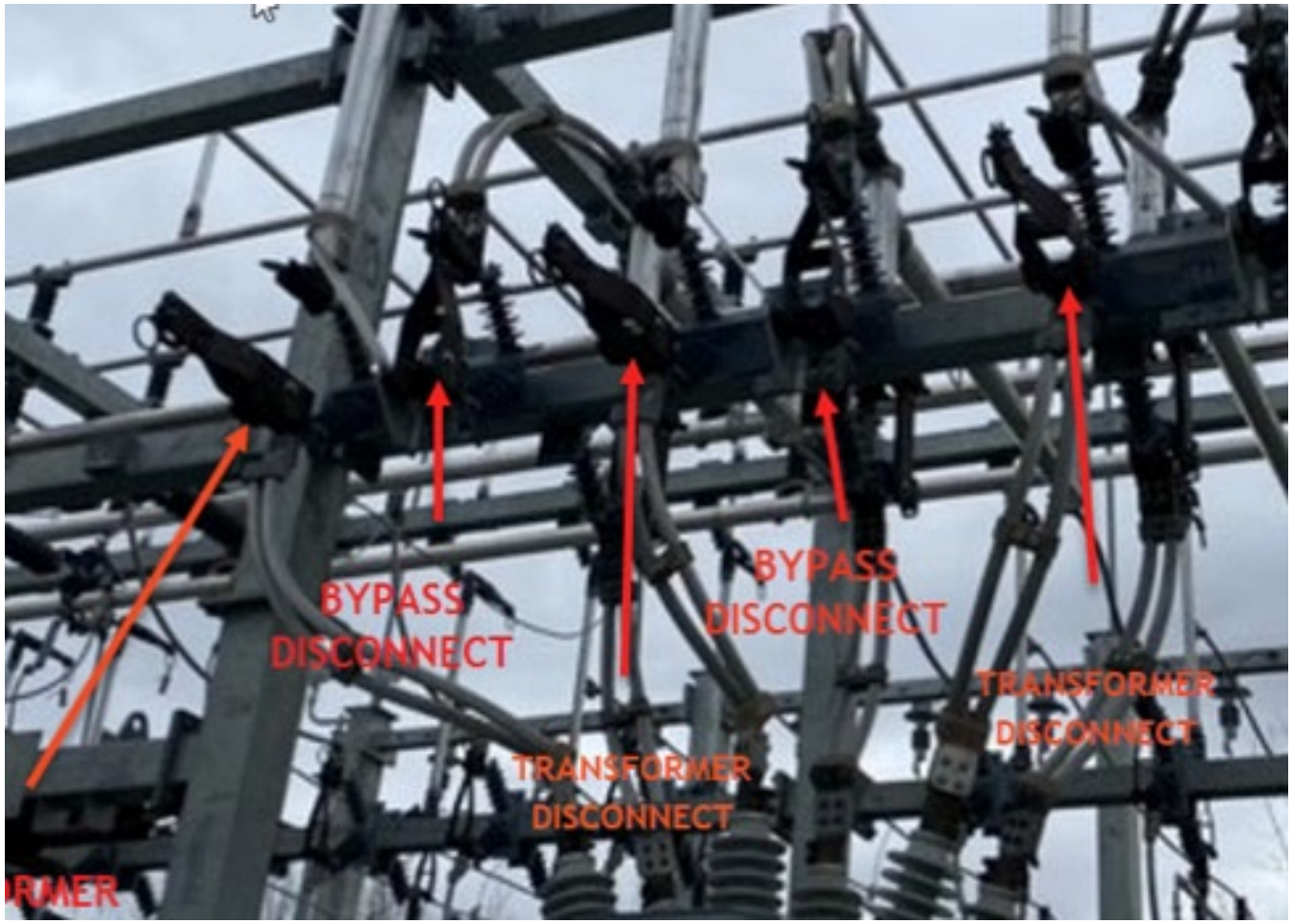
To Sum Up

- Labeling kits were provided for the old switch design in the summer of 2019. However, incomplete records may have inadvertently left off switch units so some may be missed.
- The offset switch design came out in fall of 2019 and was probably first used in construction in 2020(?). The offset switch design was supposed to have the labels affixed at the factory.
- However, due to delays in ordering the new design, and delays in field construction, there may be old units that have been in-serviced recently. Thus, this topic is still relevant.

A Recent Switching Error

- This occurred in AEP East.
- Switching on 6/23/21 requested the breaker disconnects to be closed and the bypass switches to be checked.
- This step was reported complete on that date.

The Discovery-A Questioning Attitude!!



- Found on 3/15/22 during routine station inspection.
- CB disconnects were open and the bypass switches were closed.
- Corrected the same day after discussion with dispatch.

Thoughts

- Switch was an old style without any offset between disconnect and bypass. Further, there were no labels in place.
- A relatively new servicer made the discovery (a fresh perspective).
- Complacency-the situation existed for nine months!
- Distraction-servicer making the error was helping to train a new dispatcher and may have lost focus.
- The breaker CTs fed a set of Bitronics ammeters. They would have read zero during the error period.

Follow-Up

- The area found three other stations with these switches. They weren't labeled either.
- Currently being rectified.
- Others??
- We have had another recent switching error involving this same switch design. It is currently being investigated.

Contact Info

- Brian Hattery
  Planning and Engineering Supervisor
  AEP Transmission Field Services
  Email: bfhattery@aep.com
  Phone: 419-675-5614

AEP TRANSMISSION
An AEP Company
BOUNDLESS ENERGY

RELIABILITY FIRST

NERC Lessons Learned

Dwayne Fewless
Principle Analyst, Operational Analysis & Awareness
ReliabilityFirst






Agenda

- What are Lessons Learned for?
- Example 1: Human error leads to evacuation of primary control room
- Example 2: Unmanned forklift contact with energized bus
- Where can you find written Lessons Learned?
- How do I get more information about a specific Lesson Learned?
- How can I submit a Lesson Learned?

HUMAN ERROR LEADS TO EVACUATION OF PRIMARY CONTROL ROOM

Problem Statement

Primary Interest Groups

- Balancing Authorities (BAs)
- Transmission Operators (TOPs)
- Generation Operators (GOPs)

Problem – Maintenance worker failed to follow hot work procedures; control center had to be evacuated

Event Details

- Fire occurred in the powerhouse adjacent to control center; extensive smoke required evacuation
- Smoke traveled up a utility tunnel and elevator, reaching the energy control center
- Primary control center was partially evacuated
  - Operators utilized the back-up control center
- Once relief crew reached the backup center, the system operators at the primary control center were able to leave their posts and report to the back-up control center

Cause of Event

- **Investigation determined that the maintenance workers incorrectly assessed the tank**
  - Workers were tasked with removing a potable water tank
  - A spark from a torch ignited the plastic lining of the tank
  - Prior to the removal, the workers viewed the side of the tank which had no lining or combustible materials
  - Fire occurred in the center of the tank which had flammable lining
- **Workers did not fully inspect the area for combustible materials**
  - Thus, a fire watch was not established and a hot work permit was not issued

Corrective Actions

- **All personnel have been retrained on the hot work permit system**

- **Specific measures will be implemented to prevent smoke from travelling to the control center**
  - Fire stops
  - Ventilation changes

Lessons Learned

- **Workers should evaluate work conditions before beginning any maintenance activities and follow established hot work safety guidelines**
- **Periodic training on hot work procedures should be given to all maintenance employees**
- **Control center ventilation equipment and fire stops should be evaluated regularly**
  - This will ensure that proper precautions have been taken to ensure that smoke from internal/external fires cannot reach the control center
- **When control centers are not separate i.e., they are adjacent to other active facilities, consideration should be given to the impact of these facilities on control centers**

UNMANNED FORKLIFT CONTACT WITH ENERGIZED BUS

Problem Statement

➢ Primary Interest Groups

- Transmission Owner (TO)
- Transmission Operator (TOP)

Problem – unmanned forklift came into contact with energized bus

- **Caused breakers connected to a 345-kV bus to open**
- **Transfer trip occurred on 115-kV and 2-345-kV lines**
- **Electrical service to a coal mine was interrupted**

Event Details

- **Unmanned forklift made contact with 345-kV bus, causing a fault and clearing the bus**
- **Forklift rose due to faulty controls and/or by drift elicited by an electromagnetic field of the bus**
- **115-kV & 2-345-kV lines were tripped**
- **Line servicing coal mine was de-energized**
- **Mine personnel were not notified of the work taking place**
  - No preparations were made for a potential outage
- **All lines were returned to service**
  - Forklift was removed
  - Faulted bus was confirmed to be suitable for re-energization and continued use
- **No injuries, generation outages or other customer service outages occurred as a result of the event**

Corrective Actions (Pt. 1)

- **At the end of a shift, all equipment shall be moved to a designated parking area away from energized or potentially energized equipment**
- **At the end of a shift, equipment should be checked to make sure it is not running and all keys to equipment shall be removed and locked in a secure place**
- **When heavy equipment is not in use, it will be turned off with the keys removed and locked in a secure place**
- **Machines used in tight space working environments may be left in place at the end of the shift**
  - Keys shall be removed and secured in a safe place

Corrective Actions (Pt. 2)

- **Job site shall be inspected at the end of the shift to check equipment**
  - Ensure that equipment is not running
  - Ensure that keys have been removed and locked in designated area
  - Check fencing and gates to ensure that the site is secure
- **Perform a Failure Mode and Effects Analysis (FMEA) for the switchyard and other critical locations to identify hazards and how to mitigate them**
  - Communicate with all possible affected entities to inform them when work is being performed that might impact them
    - Include Power System Operators & Generator owners/Operators

Lesson Learned (Pt. 1)

- **Construction equipment in a switchyard should never be left running unmanned**
  - Keys to the equipment should always be removed and stored in a secure area
- **Construction work sites in energized switchyards shall be inspected at the beginning of and end of each shift**
  - Ensure all barriers are identified and in place for potential hazards of accidental electrical contact of construction equipment

Lesson Learned (Pt. 2)

- **All heavy equipment (including forklifts) should be moved to a designated parking area away from energized or potentially energized equipment when not in use**
  - If the equipment cannot be moved, it should be put into a lockdown position and inspected to ensure it could not make contact with other equipment in the substation
- **Before starting work in the switchyards, notify and coordinate with all possible affected entities**

Where to find Lessons Learned

- **Lessons Learned can be found on the NERC website at the following link:**

https://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

To get additional information

- **Reach out to Region EA contact**
- **Contacts at ReliabilityFirst:**
  - Dwayne Fewless
  - Danielle Daugherty
  - Kellen Phillips
  - Bill Crossland
- **Send questions**
  - Contact will be made with entity
  - Either questions will be answered, or a meeting will be set up for discussion

To Submit a Lesson Learned

- **Contact RF EA**
- **Identify Lesson Learned**
- **Work with RF EA to create Lesson Learned**
- **Submit Lesson Learned**
  - You will have the option to either be on the review team or look over the submission after review team is complete

Questions & Answers

Forward Together ReliabilityFirst