

Non Compliance: Trends, Prevention, Root Cause

NPCC Mitigation and Enforcement Team

May 23, 2018

White Plains, NY

Scott Nied, Damase Hebert, Jenifer Wallace

- O&P Non Compliance Trends
- Leading O&P Non Compliance Factors
- Cycle of Mitigation
- CIP Non Compliance Trends
- Leading CIP Non Compliance Factors

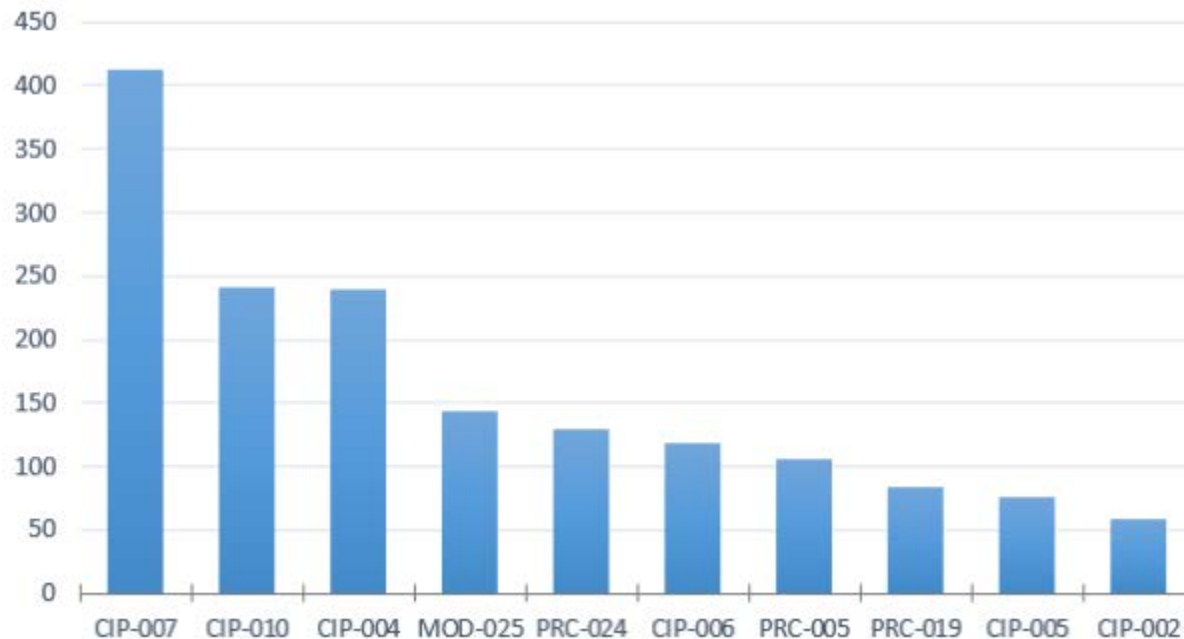
5 Year Total Number of Non Compliances Discovered Across ERO



Total Number of Non Compliances Discovered in NPCC



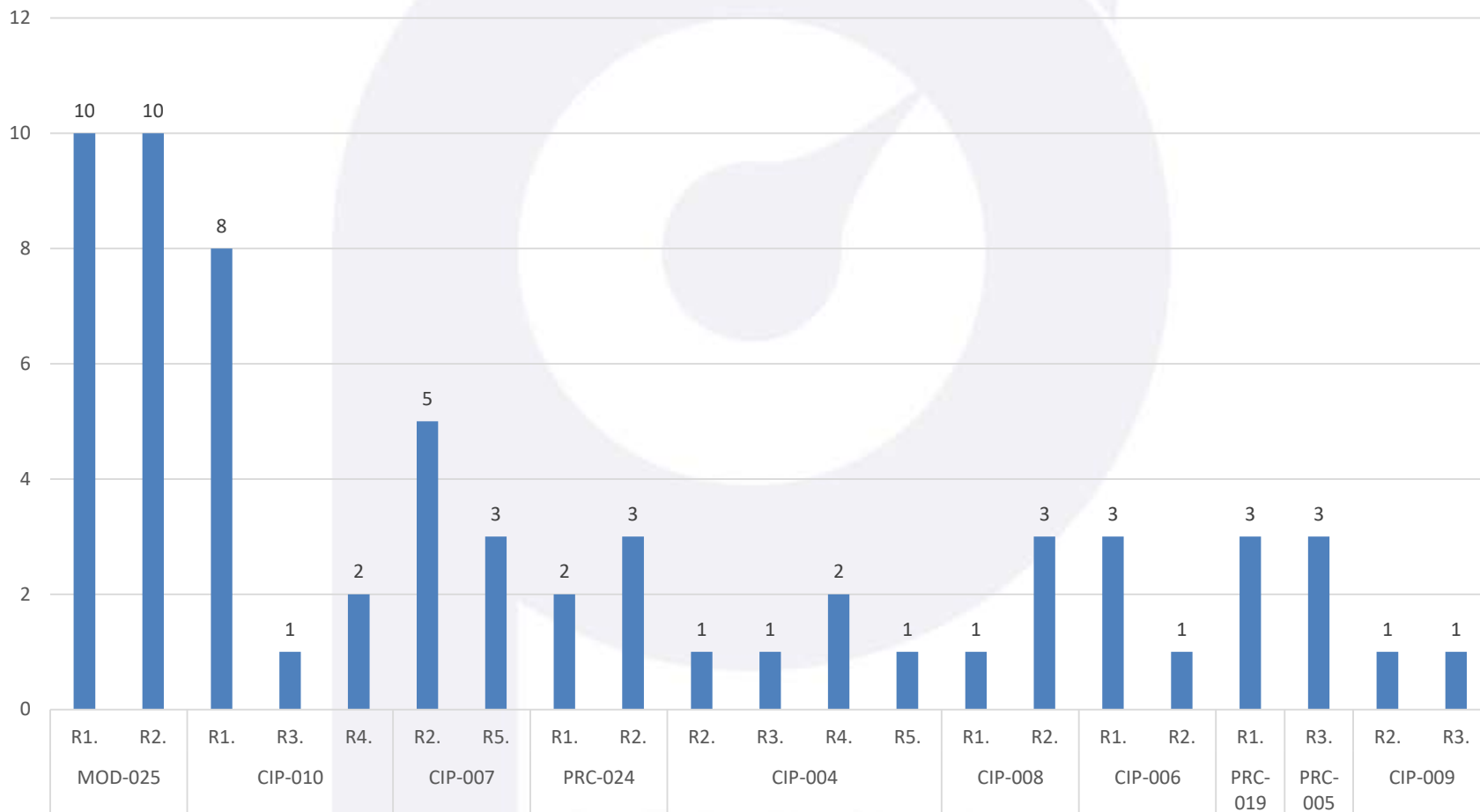
2017 Top 10 Most Violated Standards in ERO



2018 Top 10 Most Violated Standards in NPCC



2018 Top 10 Most Violated Standard By Requirement in NPCC

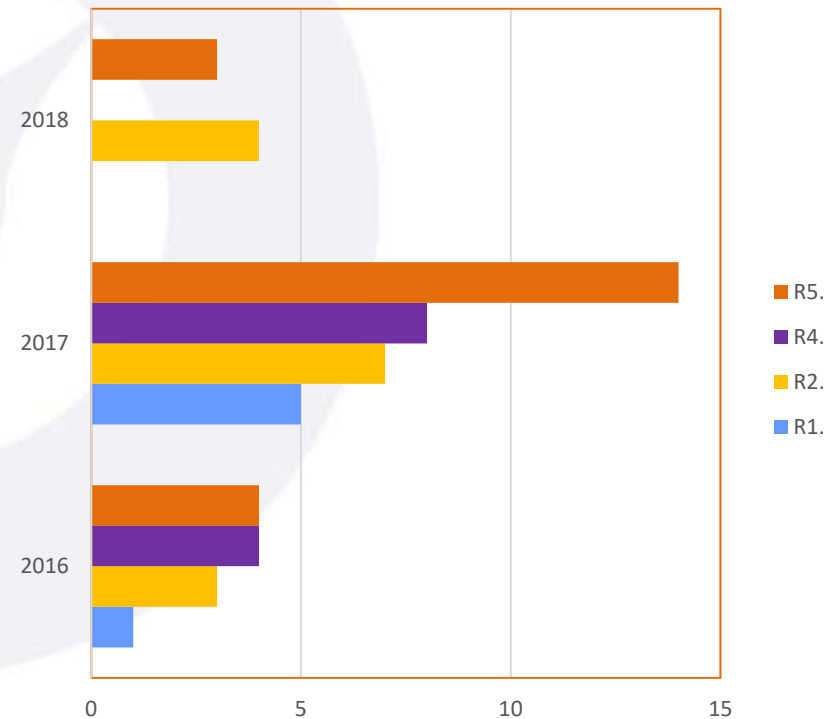


All Time CIP-007 by Requirement

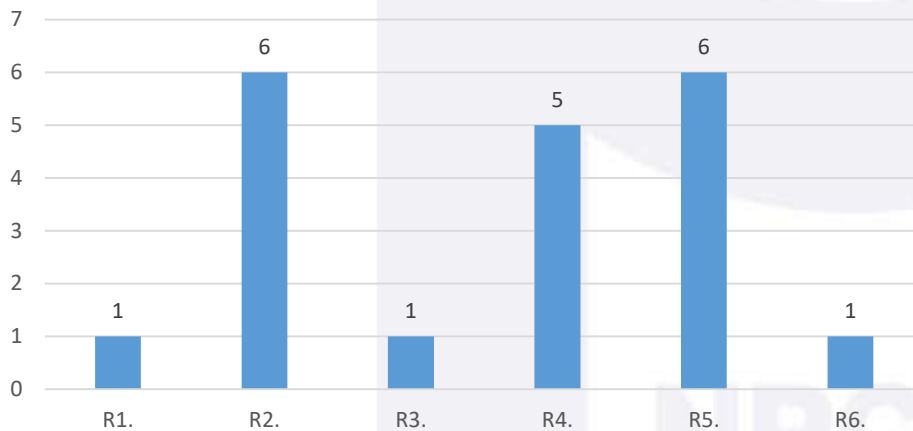


JV Slide

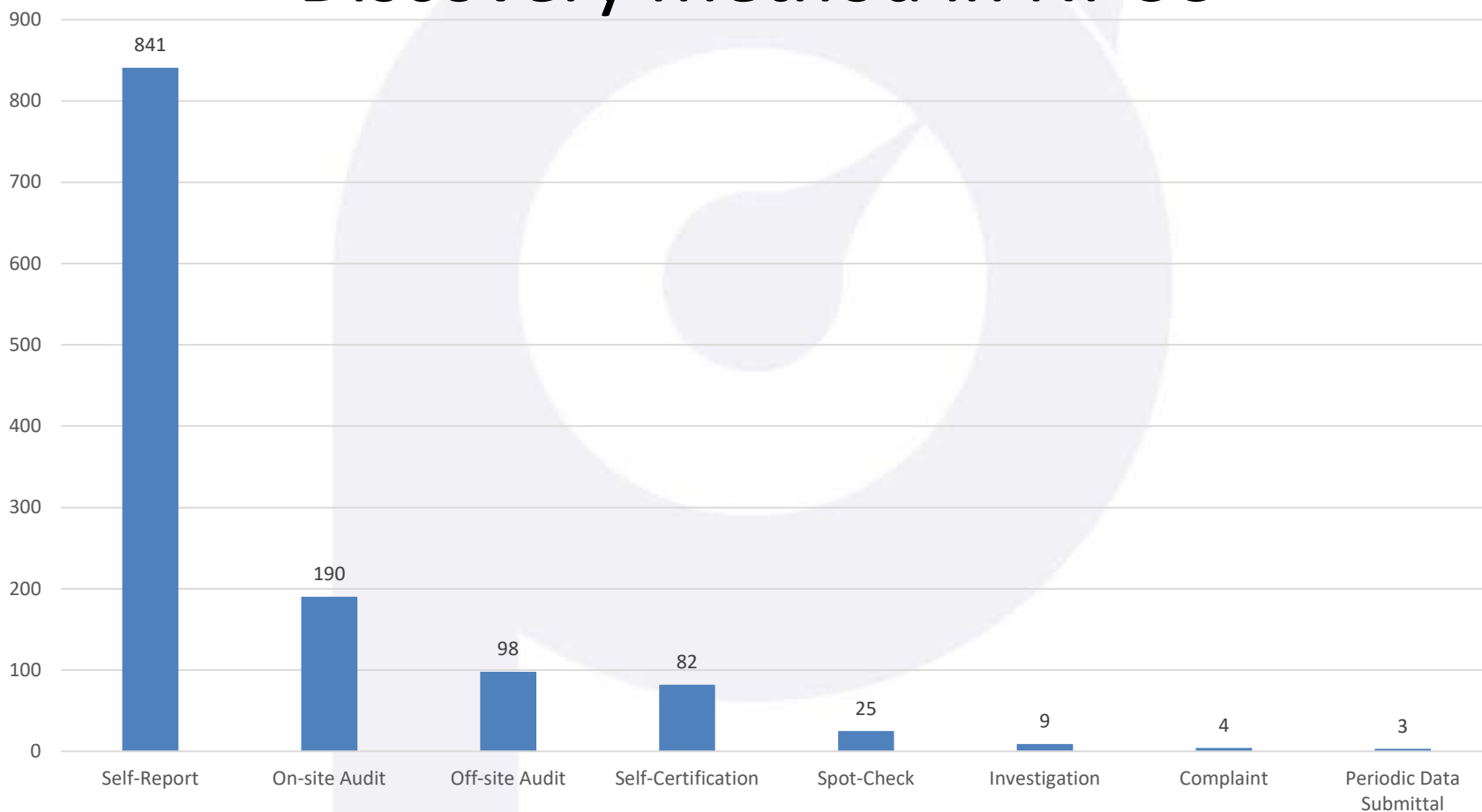
CIP-007



Past 12 Months (April-April) CIP-007 by Requirement



All Time Total Non Compliances by Discovery Method in NPCC



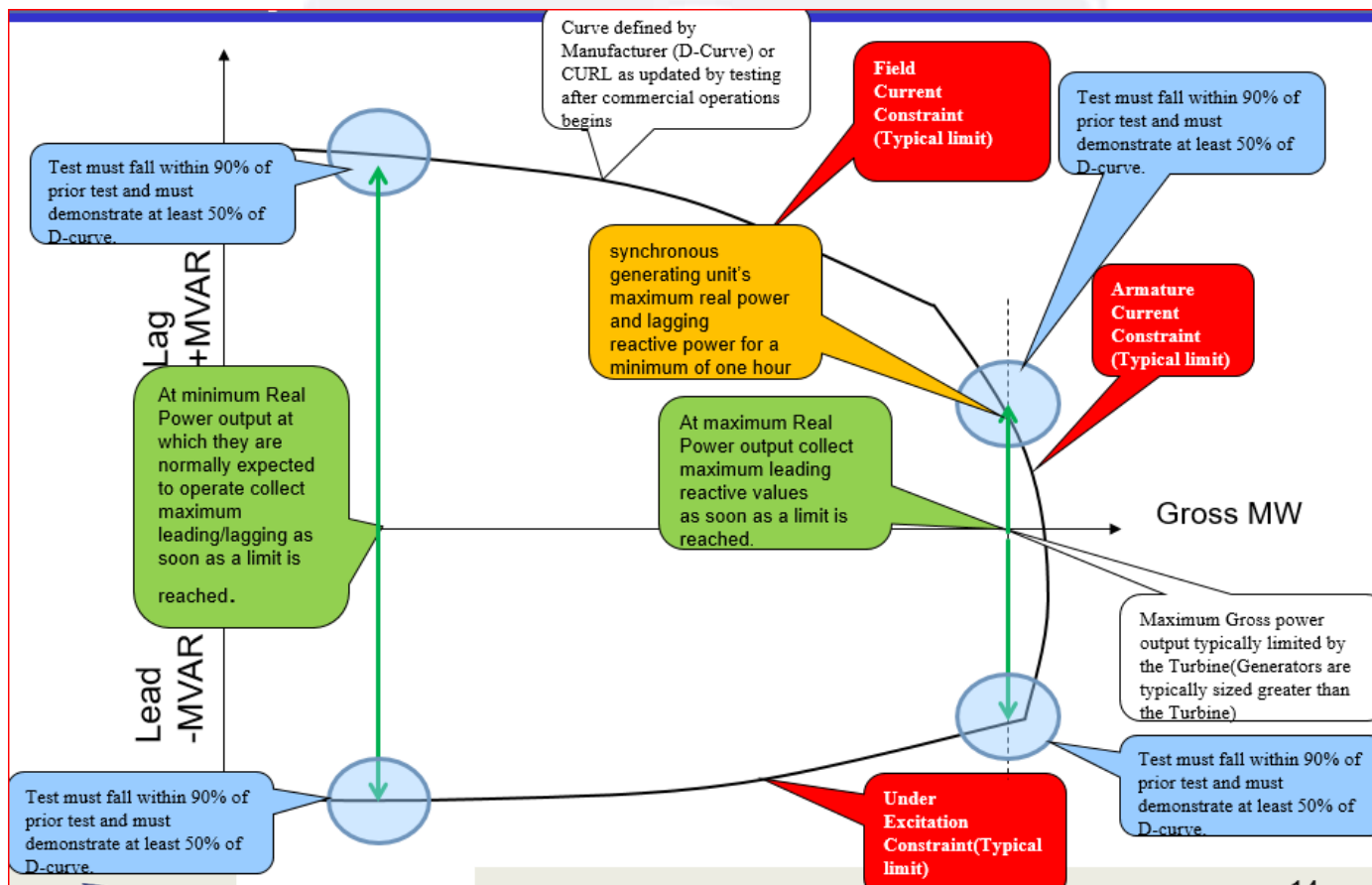
2018 Non Compliances by Discovery Method in NPCC



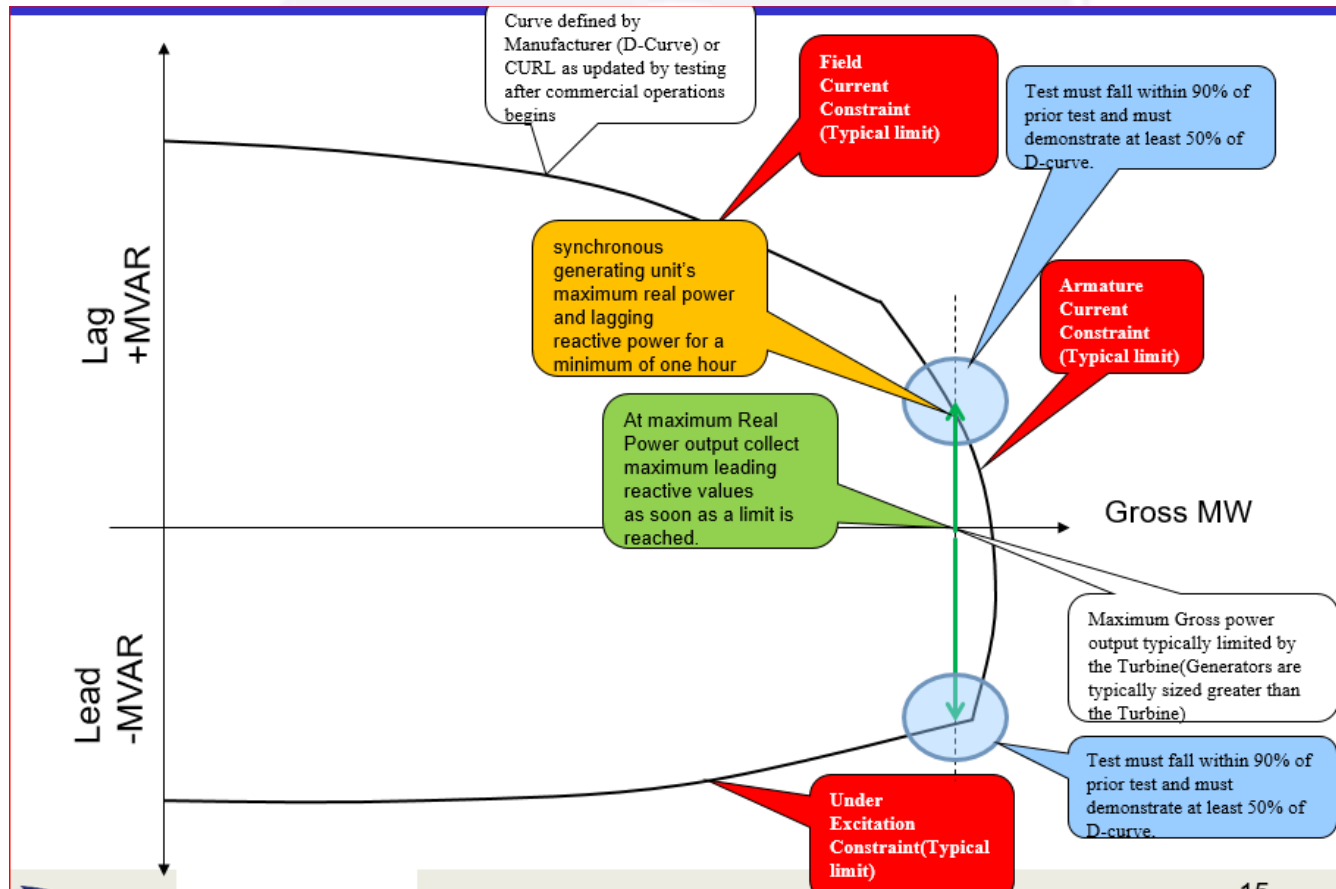
Leading O&P Non-Compliance Factor

- Implementation Plan dates
- Incorrect Assumptions
 - Facility, Component, Entity, NYISO D9 and D10 program
- Lack of Awareness/Obligation/Understanding
 - MOD-025 Real/Reactive
 - PRC-024 Freq and Voltage Operational Curves
 - PRC-019 Voltage Regulating System Control Verification
- Lack of proper controls

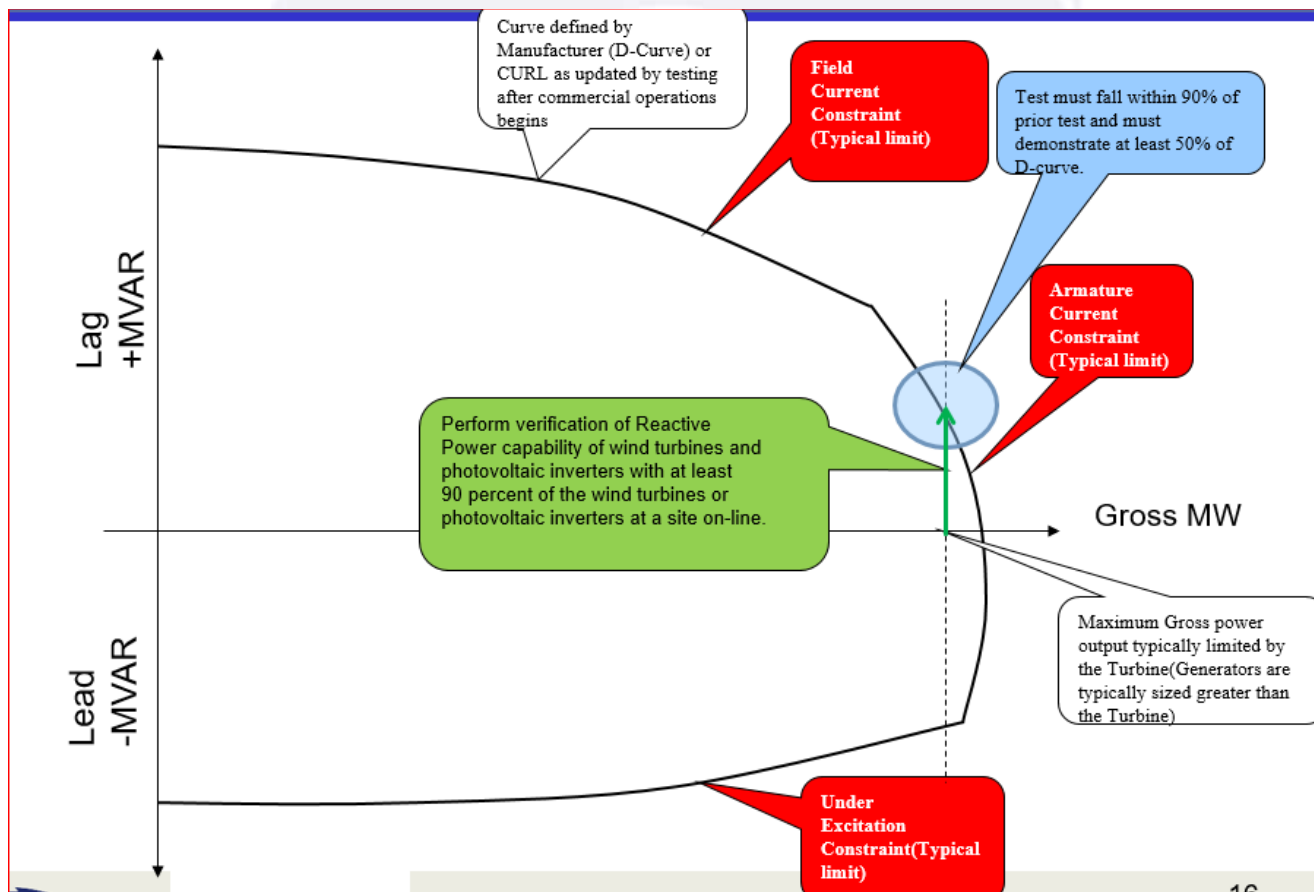
MOD-025 Thermal (except Nuclear)



MOD-025 Nuclear



MOD-025 Variable



MOD-025

- Use the NERC form
- Or provide the same data as on the NERC form
- For NERC Compliance, your ISO cannot dictate to you to use their form. If you provide them the data fields on the NERC form in some fashion, you are compliant.
- ISO Market Rules are a different story

MOD-025 nuances of your TOP's Process

- ISONE OP-12...AVR must stay in auto controlling voltage. The TOP is adjusting the system voltage so you can send provide/absorb VARS for your test.
- NYISO...AVR can come out of automatic

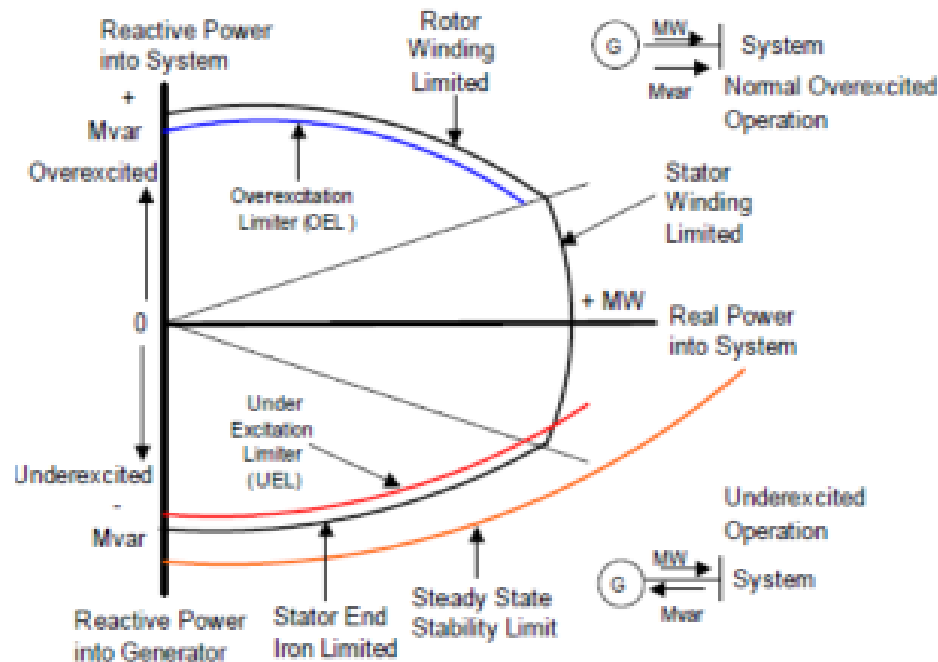
PRC-024 Misconceptions

- Facility – What is a Facility in this Standard?
- 2 curves: Freq and Voltage
- UF is trumped by PRC-006-NPCC-01
- Voltage Protection Systems and POI
- Solar Invertors – WECC Events
 - Current from invertors to grid cannot stop while within either curve.
 - “Trip” is not a defined term

PRC-019 Voltage Regulating Control Verification

- Need some sort of analysis
- Show your lines on the D Curve
- Need documentation that it was verified before the due date. Still a PNC if no changes are needed without proper documentation.

D Curve



"Typical Generator Capability Curve and Operating Limits for a cylindrical rotor generator"
 from IEEE PES/SMC Paper
 "COORDINATION OF GENERATOR PROTECTION WITH GENERATOR EXCITATION CONTROL AND GENERATOR CAPABILITY"

New and Old: Industry Focus

- 7/1/18, R2: MOD-026-1 and MOD-027-1
 - Verification of Gen Excitation Control System
 - Verification of Turbine/Governor and Load Control
 - Implementation Plan: 30% of NCR applicable gross MVA by Interconnection completed and the data supplied to TP
- FAC-003-4
 - 2003 Blackout, not looked upon lightly, keep up your guard
- FAC-008-3
 - Issues uncovered in ERO
 - Field verification visits will start during TO, GO audits
 - Will check for most limiting series element that makes up the Facility Rating

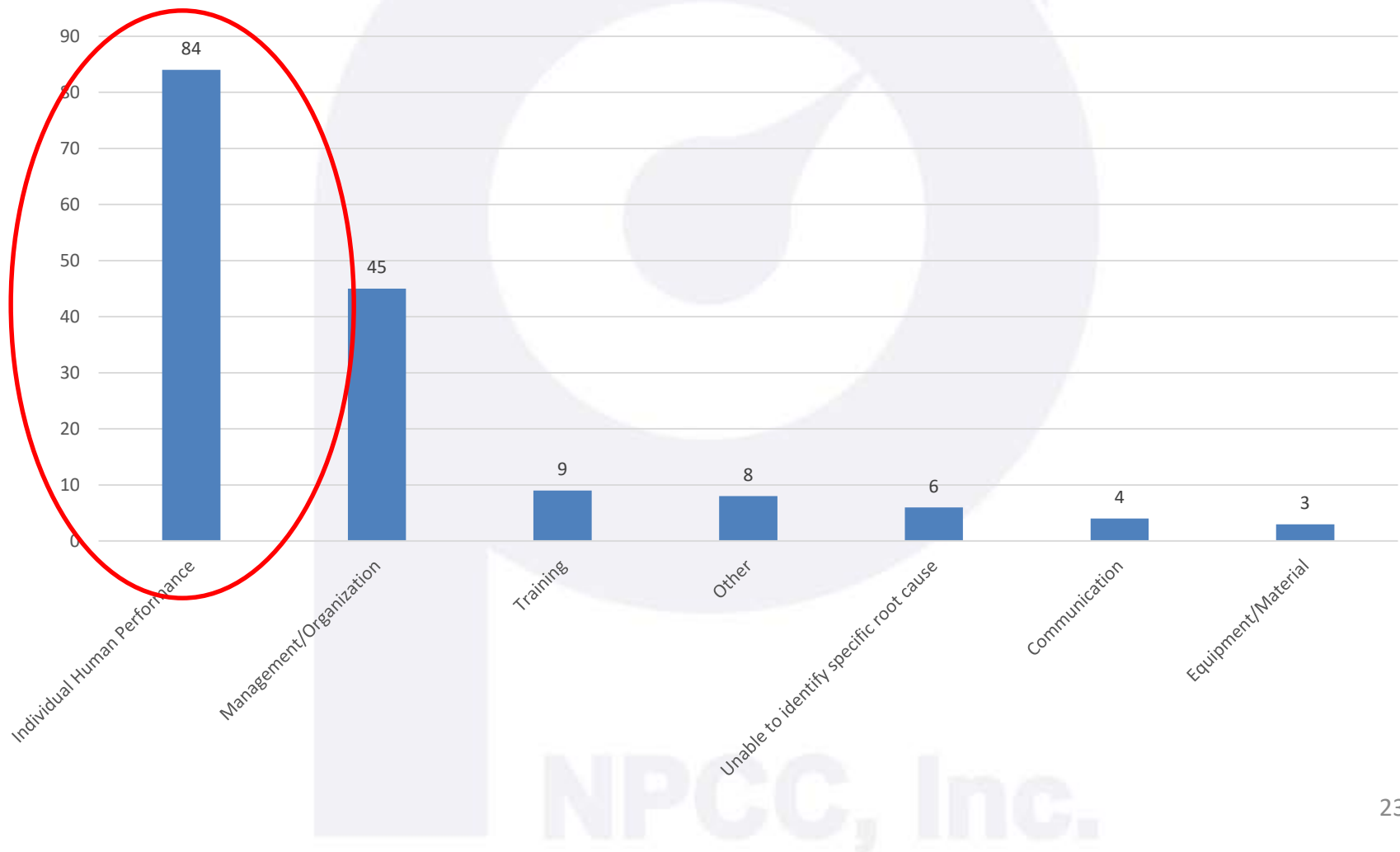
Cycle of Mitigation

- Identify the full scope/extent of the Non Compliance issue
- Identify the root cause of the issue
- Evaluate/Harden internal controls
 - Preventative, Detective, Corrective
 - Determine effectiveness of mitigation activities over time
- Feedback and Communication

Understanding the Full Scope of Issue

- 5 W's, 1 H
- Other facilities across its corporate structure
- Other departments
- Procedures, assets, facilities, or personnel that are directly affected or could be affected as part of noncompliance
- Other Reliability Standards

Root Causes of Violations of Repeats from November 2017 NPCC Review



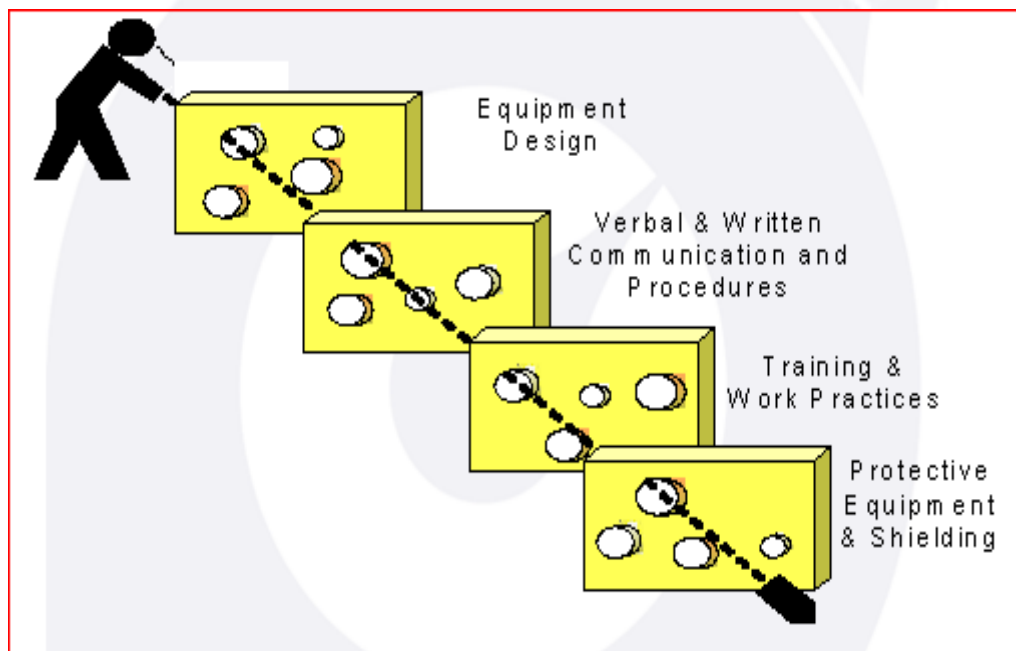
Controls Relate to Root Cause

- Dig deeper than just Human Error/Awareness/Training
- Human error is predictable, therefore preventable
- An effective cause analysis is made up of six steps
 - Clear definition of the problem
 - Collection of data surrounding the problem
 - Identification of contributing factors
 - Identification of the true root cause
 - Identifying and implementing mitigation solutions
 - Evaluating those solutions for continuous improvement
- Which controls worked? Which didn't?

Proactive and Preventative

- Majority of issue is due to preventative controls
- Humans will make mistakes
- Change/adjust the conditions that humans work
- Majority issues: Management failures and/or failures in the program/process

Opportunities to Defend



- Line Sag into tree
- State Estimator not working
- Operator Situational Awareness Lacking
- Lack of Communication to Neighbor System



CIP Enforcement

Jenifer Wallace

CIP Self Report / Self Log

- Violation description
 - # of devices / facilities / personnel in scope
 - Names/IDs of devices/facilities/personnel
 - Where are the devices located (e.g. ESP, PSP, facility)
 - What are the devices used for
 - What type of access do the personnel have (e.g. cyber, physical, both)

CIP Self Report / Self Log

- Violation description continued
 - How was the noncompliance discovered?
 - Root Cause
 - What control failed or was lacking (can no longer use “Human Error”)
 - Compensating measures
 - Preventative
 - Detective
 - Corrective

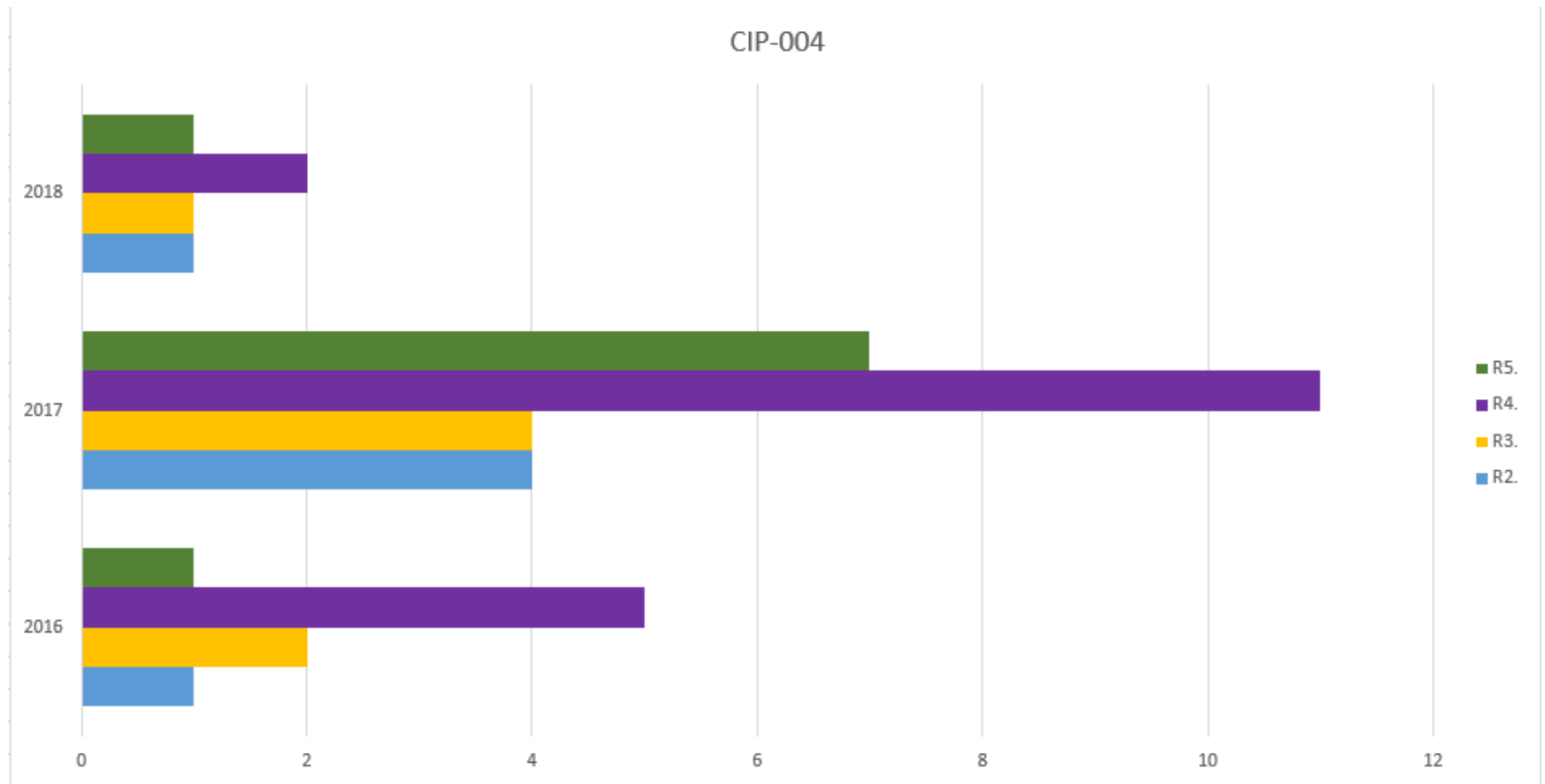
CIP Mitigation Plan

- Is the root cause addressed?
- Future Prevention
 - Identify preventative measures
 - Identify detection measures
 - Training

Violation Trends

- CIP-004 R4, R5, R3, R2
- CIP-006 R1, R2
- CIP-007 R5, R4, R2, R2
- CIP-010 R1, R2, R4, R3

CIP-004



CIP-004

- Common Root Causes
 - R2
 - Out of date procedure
 - Misunderstanding of requirement
 - Tracking system failed to alert
 - R3
 - Miscommunication
 - Tracking system not up to date / gaps for expiring soon

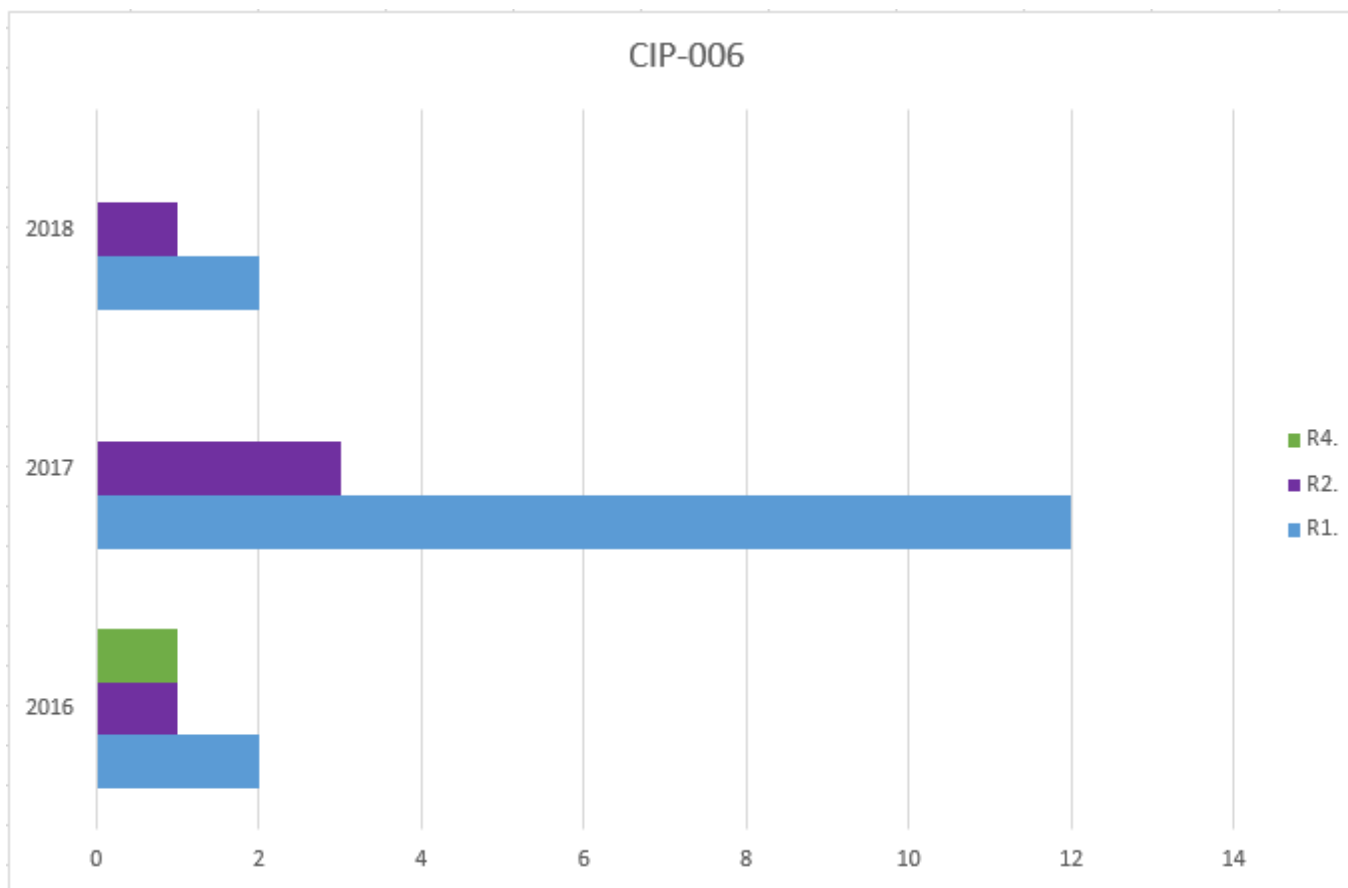
CIP-004

- Common Root Causes
- R4
 - Failure to follow process when granting
 - Automated Access – system bug
- R5
 - Management not aware of CIP Procedures
 - Failure to follow documented process
 - Use of outdated lists

CIP-004

- Things to look for
 - Does your procedure reflect what you do?
 - Do individuals with access understand who is allowed to use the mouse/keyboard and why?
 - Do you have clear communication between departments?
 - Do you test your tracking tool?
 - How often do you check for expiring Training/PRA's?
 - Do personnel know how to respond when they are under pressure to grant access?

CIP-006



CIP-006

- Common Root Causes

- R1

- Door latch malfunction
 - Authorized personnel propping doors / disabling locks
 - Asset list discrepancy
 - Lack of a process to review PSP to PSP connections
 - Failure to follow process / communicate process

- R2

- Misunderstanding of responsibilities
 - Failure to follow process
 - Lack of awareness

CIP-006

- Things to look for
 - Survey employees
 - Do they know they shouldn't prop open doors?
 - Do they know they shouldn't tape over locks?
 - Do they confirm PSP Doors, Racks and other access points are securely closed when they finish work/leave?
 - Do they know what to do if a door must be propped?
 - Do they know there is a visitor process?

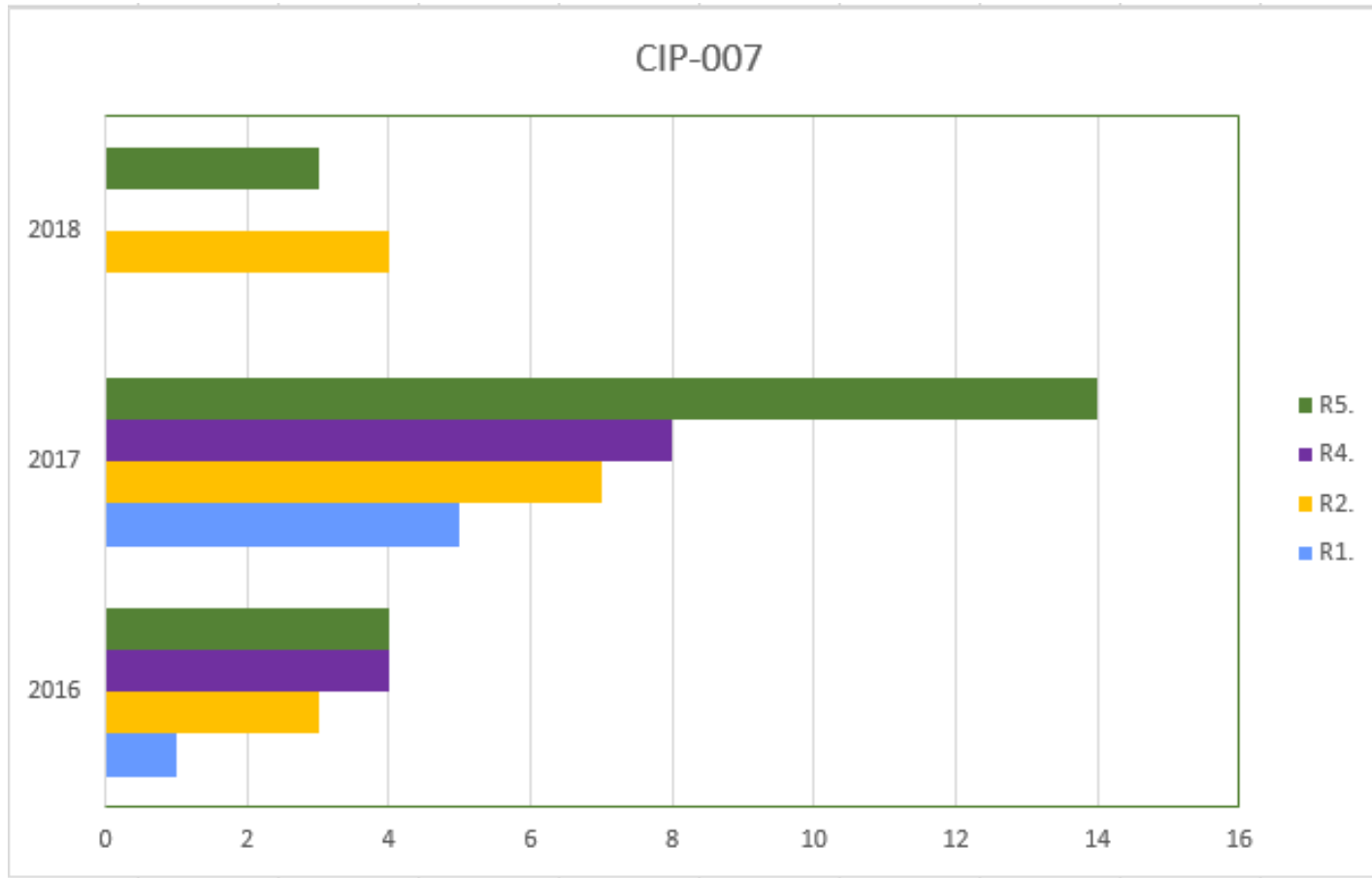
CIP-006

- Things to look for
 - How often are door latches tested?
 - Do door locking mechanisms have a delay?
- Visitors
 - How do personnel know the visitor process applies?
 - What should personnel do if they don't know how to bring a visitor into a facility?

CIP-006

- Visitors continued...
 - Do your personnel know there is a process but choose not to follow it? Why? Is your process too complex?
 - Do personnel know what to do if they can't follow the regular process (off hours – not enough badges, they don't know where to go to get badges)

CIP-007



CIP-007

- Common Root Causes
 - R1
 - Lack of oversight and miscommunication
 - R2
 - Workload constraints / Lack of resources
 - Lack of training on patch tracking system
 - Patch evaluation reminder failure
 - Failure to request a Mitigation Plan extension
 - Failure to assign responsibility upon transfer of personnel

CIP-007

- Common Root Causes

- R4

- Lack of understanding of the requirement
 - lack of process/failure to verify and test logging/alerts
 - Workload constraints / Lack of resources

- R5

- Workload constraints / Lack of resources
 - Password tracking sheet out of date
 - Lack of a process to inventory and track passwords
 - No process to document password changes
 - No method for identifying passwords had been enforced new deployment / upgraded

CIP-007

- Things to look for
 - When deploying new projects / multiple assets have responsibilities been assigned?
 - Are personnel trained on the use of tools?
 - Do you test your reminder tools to ensure alerts are working?
 - Is your process clear on what to do if a Mitigation Plan date cannot be met?
 - Do you track individual responsibilities and have a method to assign responsibilities to another individual (sick, vacation, transfer)

CIP-007

- Things to look for
 - During times of heavy workload, do personnel have a process for managing workload, setting priorities and escalating issues (Daily/weekly scrum)?
 - Do you have a clear process for identifying what devices need CIP-007 controls?
 - Do you have a method for verifying and testing that logging and alerting are functional (initial deployments and after baseline changes)?

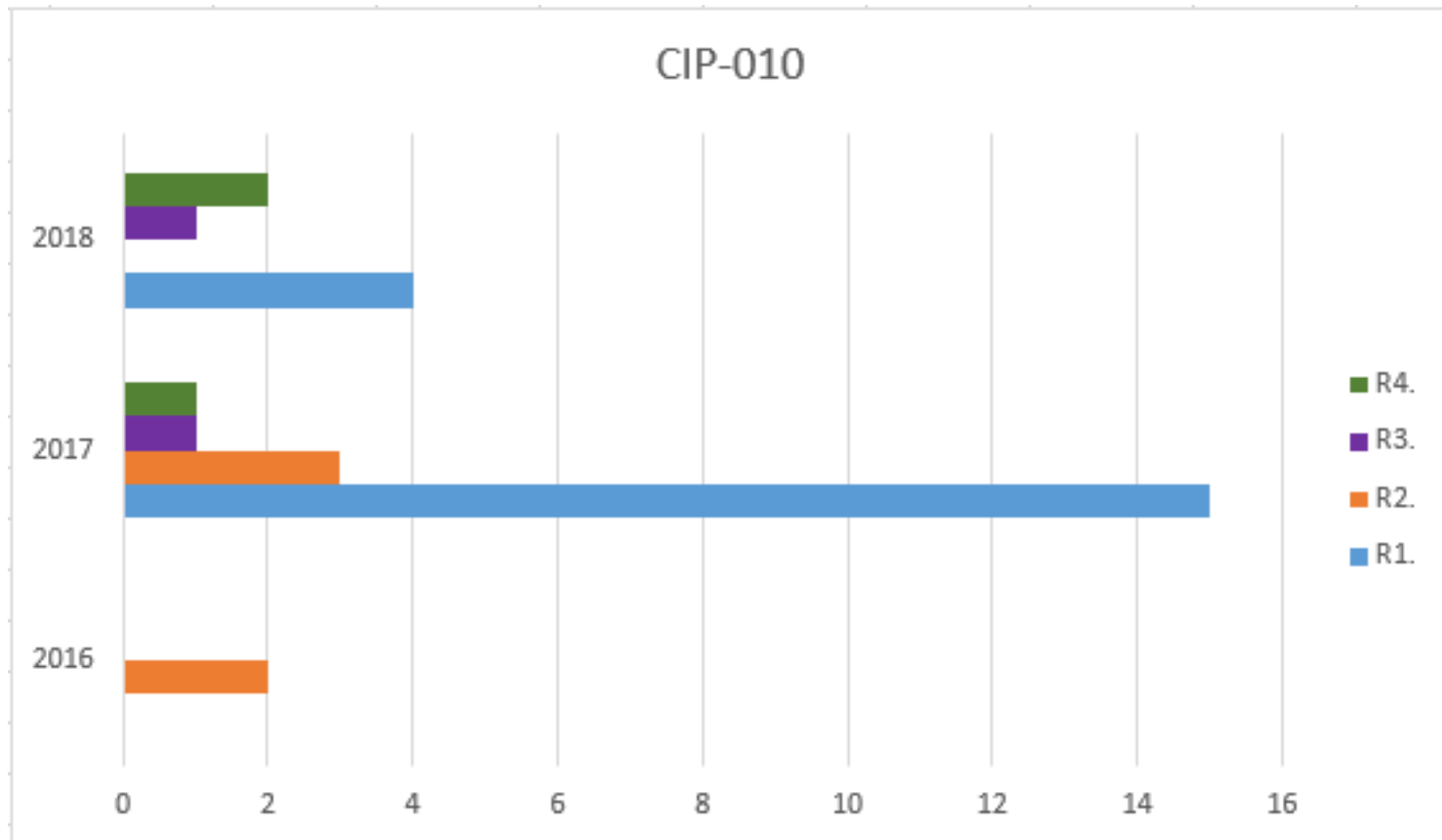
CIP-007

- Things to look for
 - Do you have a job aid for all applicable device types that describes how to enable logging / adjust settings?
 - Do you have a method to alert for detected failure of event logging?
 - Do you have a method to identify all application accounts and default shared accounts within applications?

CIP-007

- Things to look for
 - Do you have a method for checking the timeframes for password changes that are enforced procedurally?
 - Do personnel know what requirements need to be implemented when installing new/replacement devices (What if the replacement device has more functionality than the prior TFE'd device)?

CIP-010



CIP-010

- Common Root Causes

- R1

- Lack of understanding what should be a PACS, EACMS, PCA
 - Insufficient training on new technology
 - Lack of awareness, communication and oversight
 - Lack of a process for requiring CIP compliance evaluations prior to performing system restoration or troubleshooting tasks.
 - Failure to follow documented procedures
 - Workload constraints / Lack of resources

CIP-010

- Common Root Causes

- R2

- Individuals responsible for monitoring forgot
 - Failure to follow documented procedures
 - Lack of a process for identifying communication failures

- R3

- Lack of a process and controls to ensure vulnerability scans and mitigation plans were coordinated and completed.

- R4

- Lack of a control to identify patch failures
 - Lack of awareness and contractor training

CIP-010

- Things to look for
 - 36 calendar month active vulnerability assessment due by 07/01/2018
 - Do your personnel have a clear understanding or have job aid or process for identifying PACS, EACMS, and PCAs?
 - Does someone have assigned responsibility for completing a baseline for new/updated assets?
 - Do you have a process to identify new substation projects?

CIP-010

- Things to look for
 - For manual baseline collection, do personnel have a clear understanding or job aid for what they should be collecting and documenting?
 - Have personnel been trained on how to use new technology and how to identify errors?
 - Have personnel been trained on what job tasks require authorization?
 - Do personnel have a job aid for identifying changes that deviate from the baseline?

CIP-010

- Things to look for
 - Raise awareness that system restoration and troubleshooting tasks can lead to baseline changes
 - Do personnel know what adequate evidence is when it comes to demonstrating testing?
 - During times of heavy workload, do personnel have a process for managing workload, setting priorities and escalating issues (Daily/weekly scrum)?

CIP-010

- Things to look for
 - Do you have methods for reminding and escalating incomplete work tasks before you are in noncompliance?
 - Do you have a process for identifying device communication failures before you are in noncompliance with the 35 calendar days monitoring?
 - Do you have a process to ensure vulnerability scans and mitigations plans are coordinated and completed?

CIP-010

- Things to look for
 - Do you have a method for identifying control failures on TCA's?
 - Have contractors been trained on your TCA and Removable media processes?
 - Do personnel have a way to identify who is authorized to use a TCA?

Questions?

Jenifer Wallace, CISSP, CISA

Senior CIP Analyst

jvallace@npcc.org