



Big Data & Analytics for Security and Resilience of Power Systems

IEEE PES AMPS-BDAS
Task Force Meeting



2024 IEEE PES General Meeting
July 23, Seattle, WA, USA

Agenda

- Welcome
- Introduction of the Task Force
- Past and Planned Activities
- Discussions
- Adjournment



Welcome

Welcome to the TF Meeting

Task Force on Big Data & Analytics for Security and Resilience of Power Systems

Please

- Introduce yourself in a few sentence to everyone
- Register via the link or QR below:

<https://forms.office.com/r/D2k6gkmZkL>





Task Force Introduction

The Cybersecurity Landscape

For the Power & Energy Sector

Fast and steady growth of

- Threats, attack surfaces, and incidents
 - <https://www.shodan.io/search?query=port%3A502>
 - <http://threatmap.fortiguard.com>
- Awareness, discussions, and investments
 - <https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response>
- Technologies, innovations, and talents
 - <https://attack.mitre.org/software/S0604/>

Existing Efforts

Cybersecurity-related standards, guidelines, and regulations

	Focus
IEC 62351	IE 61850
ISA/IEC 62443	Industrial control systems
NERC CIP	Bulk electric systems
NIST SP 800-82r3	Operational technology security
NIST SP 1800-7	Situational Awareness for Electric Utilities
IEEE 2030.5	Smart energy application protocols
IEEE 1547.3	Distributed energy resources
...	

Existing Efforts

@ IEEE PES

Committees

**Power System
Communications &
Cybersecurity (PSCC)**

**Analytical Methods for
Power Systems (AMPS)**

Subcommittees

**Computing & Analytical
Methods**

Big Data & Analytics

WGs & TFs

**WG on Cyber Security in
Power Systems**

**TF on BDA for Security &
Resilience of Power
Systems**



Gaps & Challenges

For Big Data and Analytics (BDA)

- The richness of IT security have not been fully translated into OT solutions
- The context of OT systems have not been fully addressed by IT security

Opportunities for BDA

Big Data

Real (internal)

- Telemetries, configs, historian records, event logs, system alerts, ...

Real (external)

- Threat intelligence, knowledge bases, malware repositories, ICS advisories, ...

Synthetic

- Testbeds & digital twins, pen-tests, red-blue-yellow teaming, ...

Opportunities for BDA

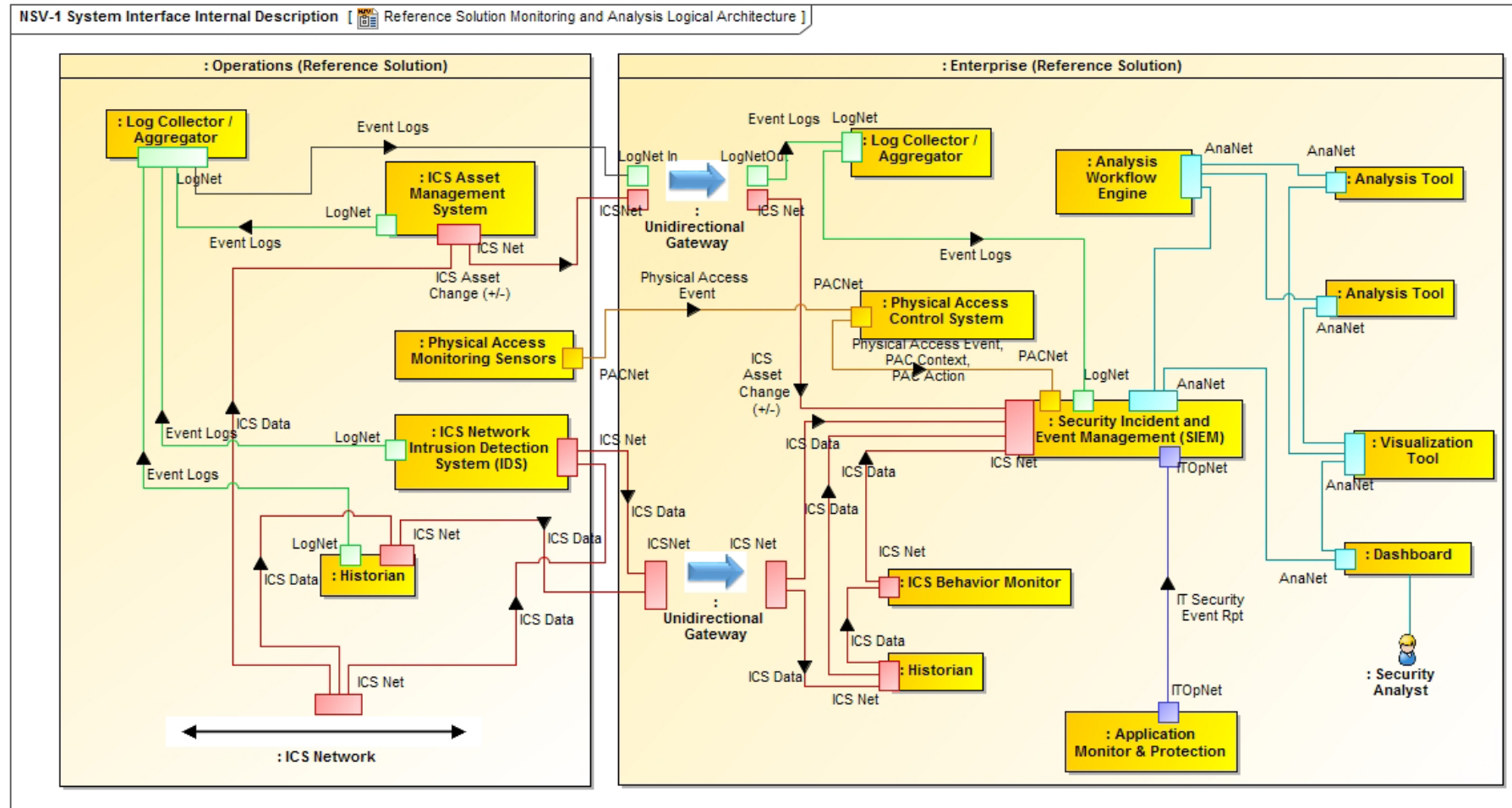
Analytics

- Characterize OT behaviour patterns
- Measure OT security postures and risks
- Determine cyber-secure OT boundaries
- Triage and enrich OT alerts
- Hunt and share OT cyber threats
- Enable long-term OT security hardening

...

Opportunities for BDA

Example Architecture from NIST 1800-7 ([link](#))



Scope and Objectives

1. **Identify** existing sources and emerging needs of big data for OT security in power systems
2. **Map** available tools and innovation gaps for analytics toward OT security in power systems
3. **Disseminate** the findings for cyber-informed power engineering in grid modernization with BDA

Potential Topics

BDA for OT Threat Intelligence for Power Systems

Collect, generate, validate, and share intelligence of OT cyber threats

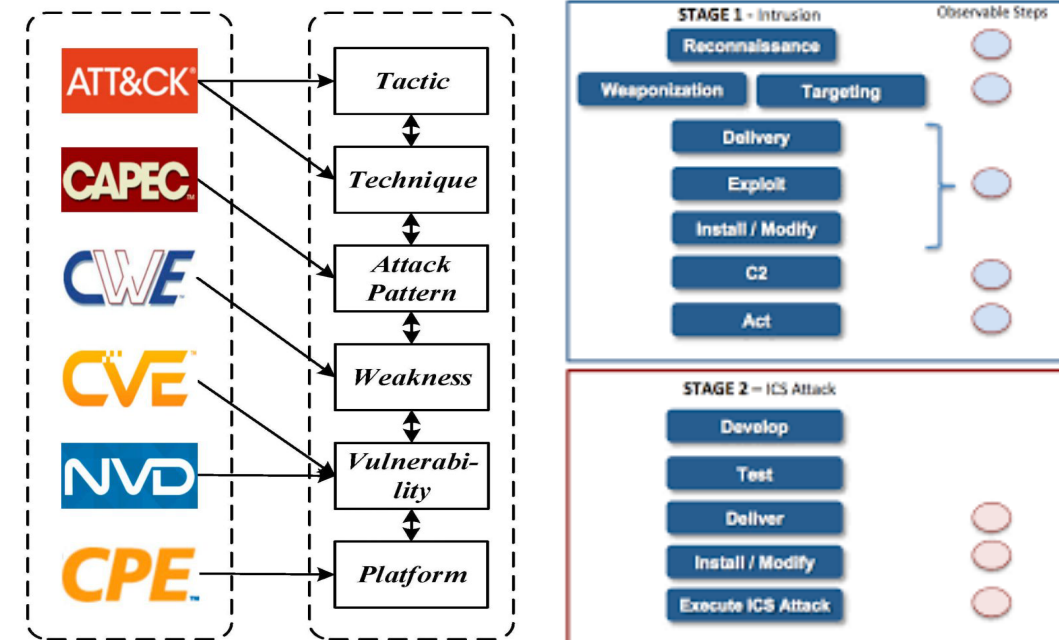
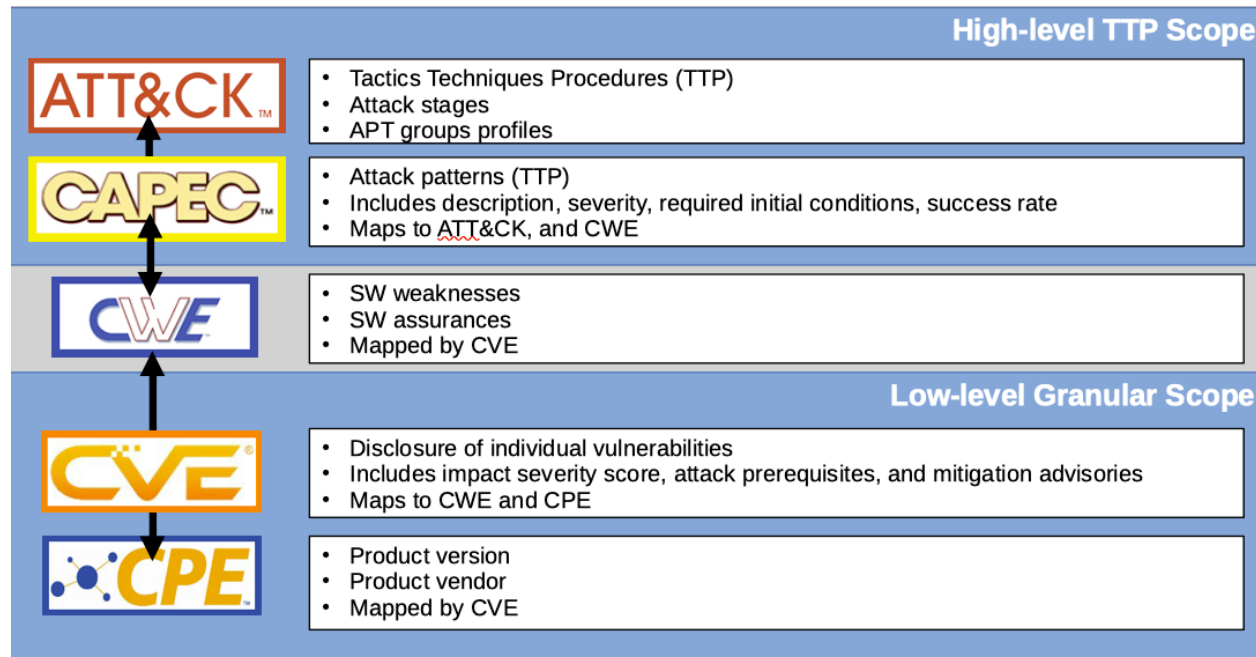


Image courtesy: [NopSec](#), [LinkedIn](#), [E-ISAC](#)

Potential Topics

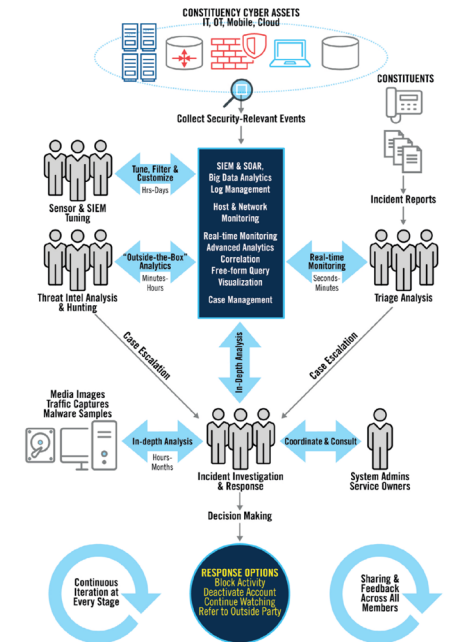
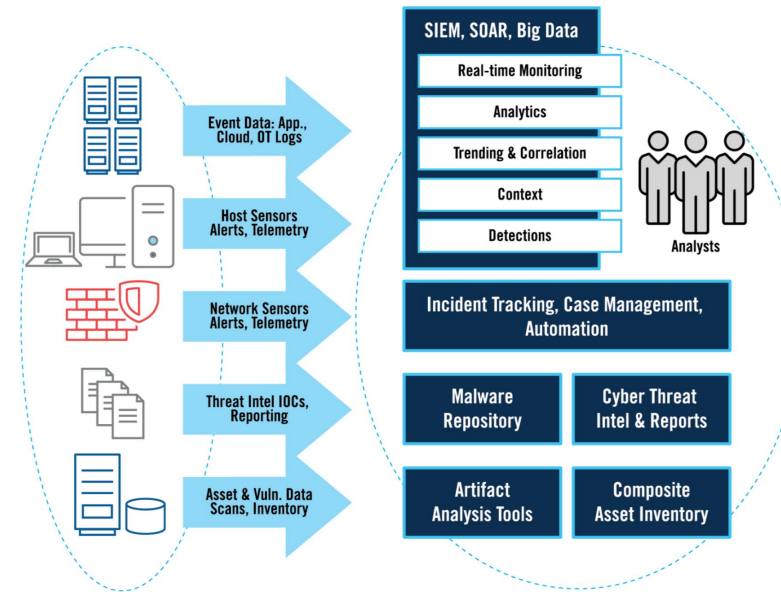
BDA for OT Security Automation in Power Systems

Data

- Telemetries, historian, CTIs, ...

Analytics

- Correlate, hypothesize, triage, respond



Typical SOC data, tools, workflows (Image: [MITRE](#))

Potential Topics

BDA in OT Security Management of Power Systems

- Security metrics and postures
- Network discovery and asset management
- Vulnerability scanning and patch management
- Software/hardware bill of materials and supply chain risk control
- (Continuous) Compliance, auditing, and forensics
- ...



Past & Planned Activities

Past Activities

2023-24

1. Apr. 2023: GridEdge 2023 (initial)
2. May 2023: BBA Headquarter
3. Jul. 2023: PES General Meeting
4. Aug. 2023: PES General Meeting Panel
5. Sep. 2023: NSERC CREATE Application
6. Feb. 2024: ISGT-North America
7. Feb. 2024: Eaton Americas Innovation Center
8. Mar. 2024: NSF EuReCa Workshop
9. Apr. 2024: GridEdge 2025 Panel
10. Jul. 2024: PES GM TF meeting (today)

- Conference meet-ups
- Site visits
- Panel/grant proposals

Planned Activities

2024-25 and beyond

1. Publication

- Technical report and transaction papers (technical surveys and papers alike)

2. Conference session

- Panels, workshops, and special sessions at, e.g., GridEdge, GM, SmartGridComm

3. Online resource

- Webinars and repositories

4. Other collaboration

- Invited seminars and grant proposals (e.g., NSF Global Centers, NSERC CREATE, EU Horizon)



Discussions

Questions, suggestions, other businesses

Everyone

Follow-up and contribute to the TF

Scan the QR to enter if you haven't done so

- **Core team members**
 - Organize and/or coordinate various TF activities:
 - Workshops, meetings, panels, reports, webinars, websites, special issues, reviews ...
- **Regular members**
 - Participate in and/or contribute to the TF activities above



<https://forms.office.com/r/D2k6gkmZkL>



Adjournment

IEEE PES Task Force on Big Data &
Analytics for Security and Re-
silience of Power Systems



<https://forms.office.com/r/D2k6gkmZkL>

Thank you!

Future contact:
jun.yan@concordia.ca