INL/MIS-23-71295-Revision-0

Cybersecurity for System Operators

May 2023

Samuel Douglas Chanoski

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-23-71295-Revision-0

Cybersecurity for System Operators

Samuel Douglas Chanoski

May 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

Cybersecurity for System Operators

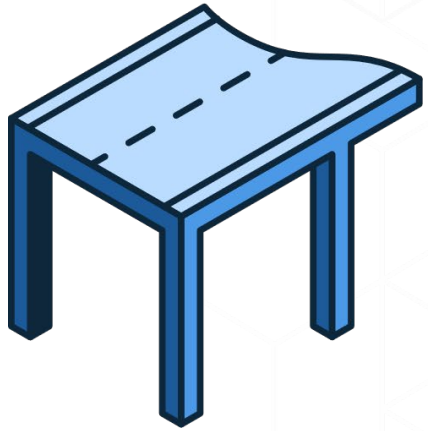
2023 SERC System Operator Conference

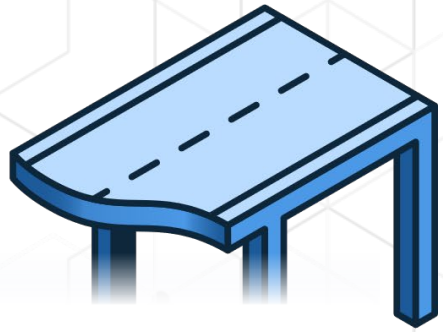
CyOTE Cybersecurity for the Operational Technology Environment

INL/MIS-23-71295

Operational Technology (OT) Security Challenge

- Multidiscipline teams struggle to see and act on early indicators of attack
- Technology alone is insufficient to defend complex and interconnected energy sector systems – human involvement needed





Industry-Identified Gaps

- Training
- Communication across disciplines
- Prioritizing attention to anomalies
- Too much noise from sensors and other data sources
- Incorporation of physical indicators

Different mental models of risk

vs.

Organizational environment?

https://pxhere.com/en/photo/1053142

Organizational environment!

https://www.flickr.com/photos/pugetsoundenergy/37702347174

https://www.flickr.com/photos/vax-o-matic/3808936344/in/photostream/

https://pxhere.com/en/photo/1053142

https://www.flickr.com/photos/deccgovuk/8725424647

https://nara.getarchive.net/media/hoboken-nj-nov-5-2012-supervising-engineer-for-public-service-electric-and-769325

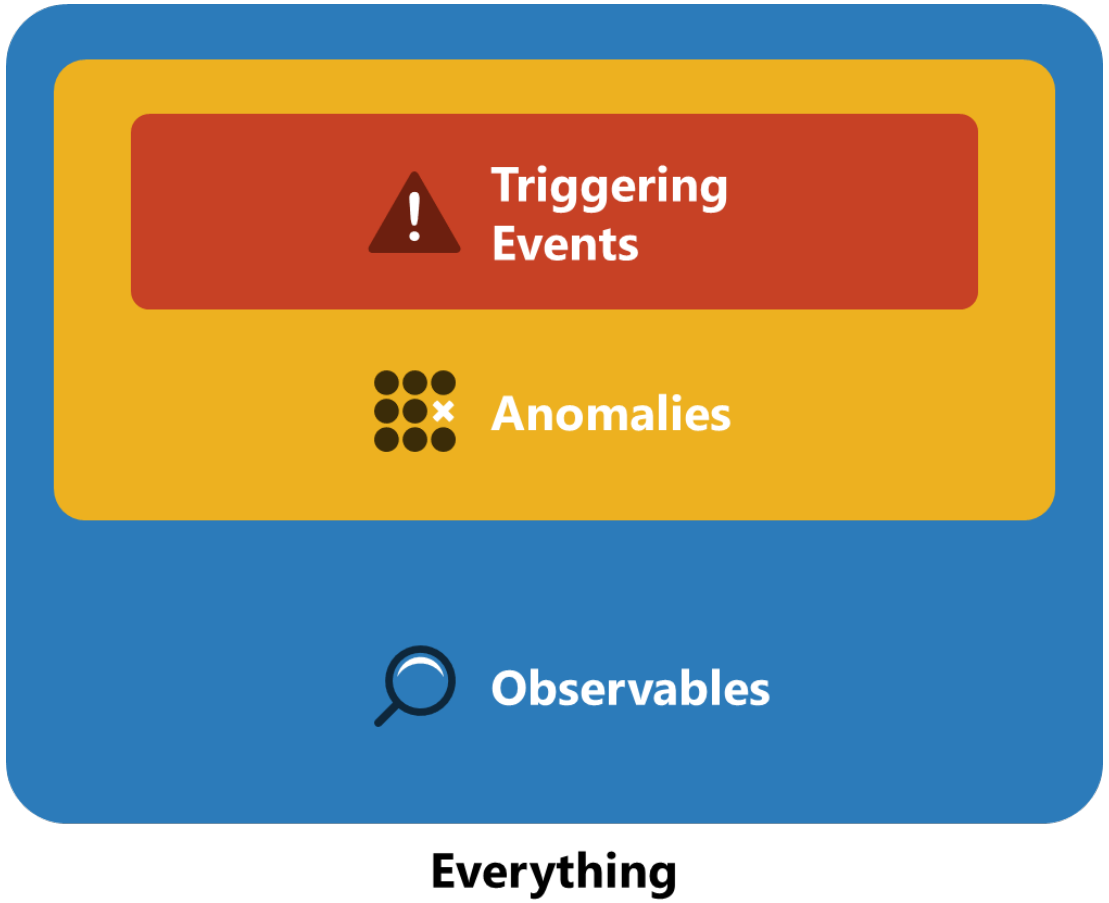
Make it intuitive

CyOTE Vision

Improved **human-led,** technology-enabled analysis of the OT environment at the strategic, operational, and tactical levels.

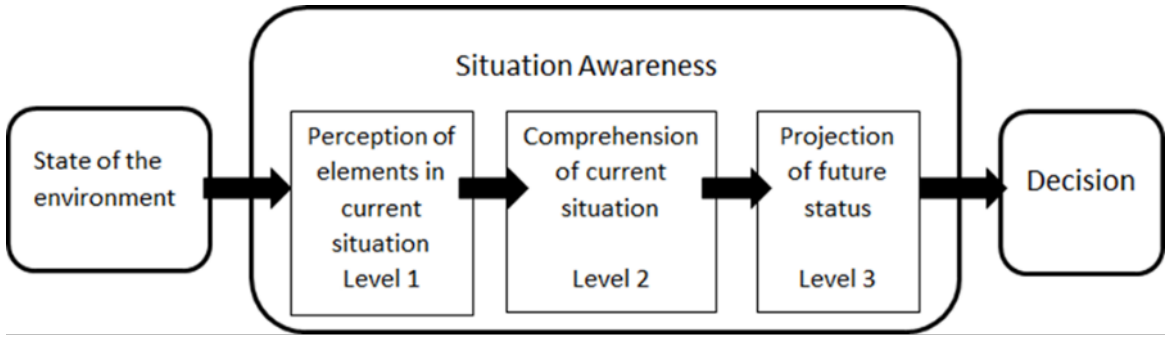
CyOTE **advances capabilities** to help energy system operators better **detect anomalies** in their operational environments, **identify cyber-attacks** earlier in the attack chain, and act decisively to **prevent or limit damage.**

Stuff happens…



- **Observable:** an occurrence that can be perceived
- **Anomaly:** an observable different from what is expected or “normal”
- **Triggering event:** an anomaly that merits investigation

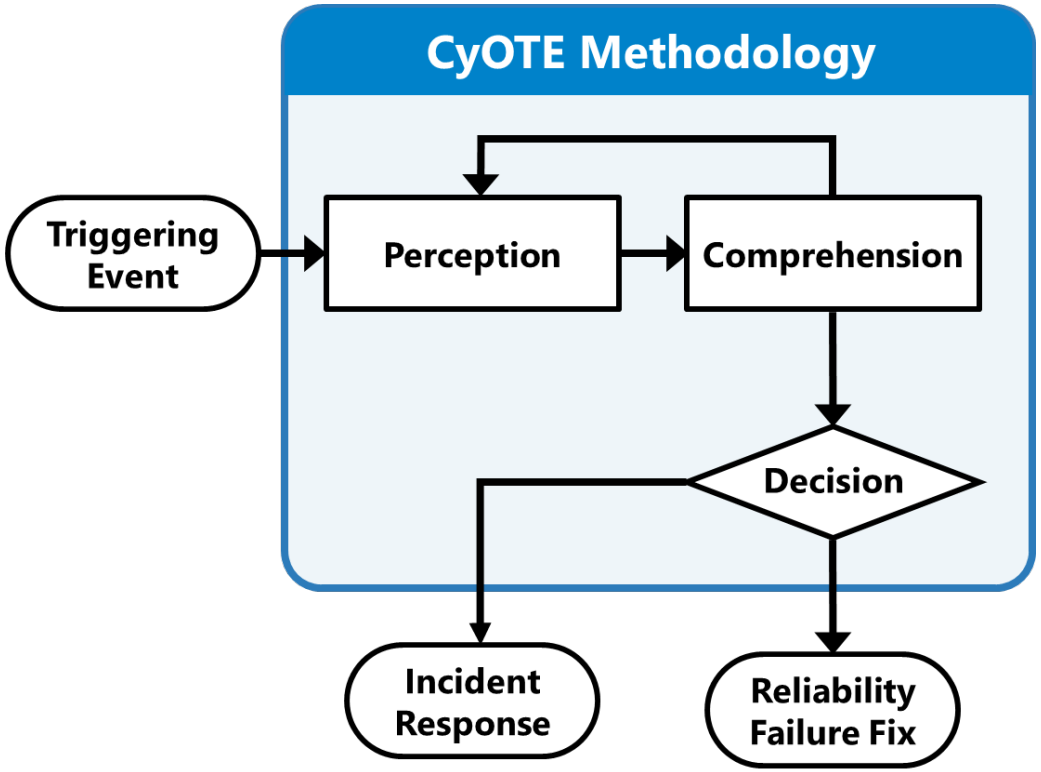
Central Concept



https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SA_for_System_Operators.pdf

- Adapted from Endsley's 1995 Model of Situation Awareness
- **Perception**: individual human ability to detect an observable
- **Comprehension**: organizational human ability to understand an observable

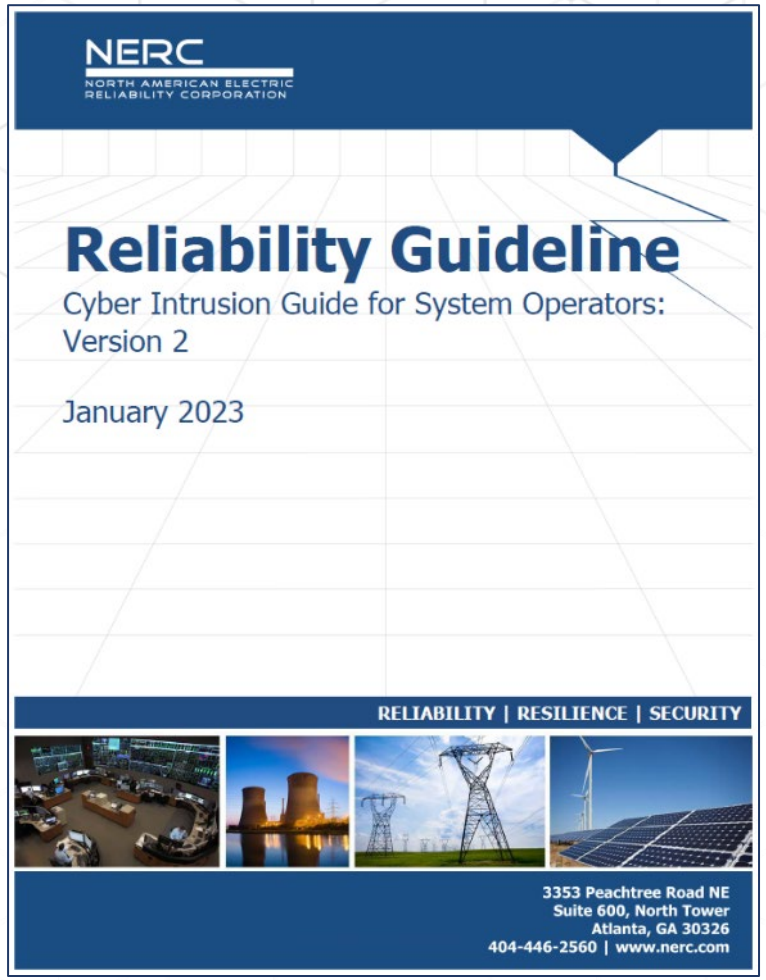
The CYOTE Methodology



- Understand the information you have, not get more data
- Applies concepts of perception and comprehension to a world of knowns and unknowns
- MITRE ATT&CK® Framework for ICS describes threat behaviors
- Goal is making a risk-informed decision to conduct incident response or to treat as a reliability failure

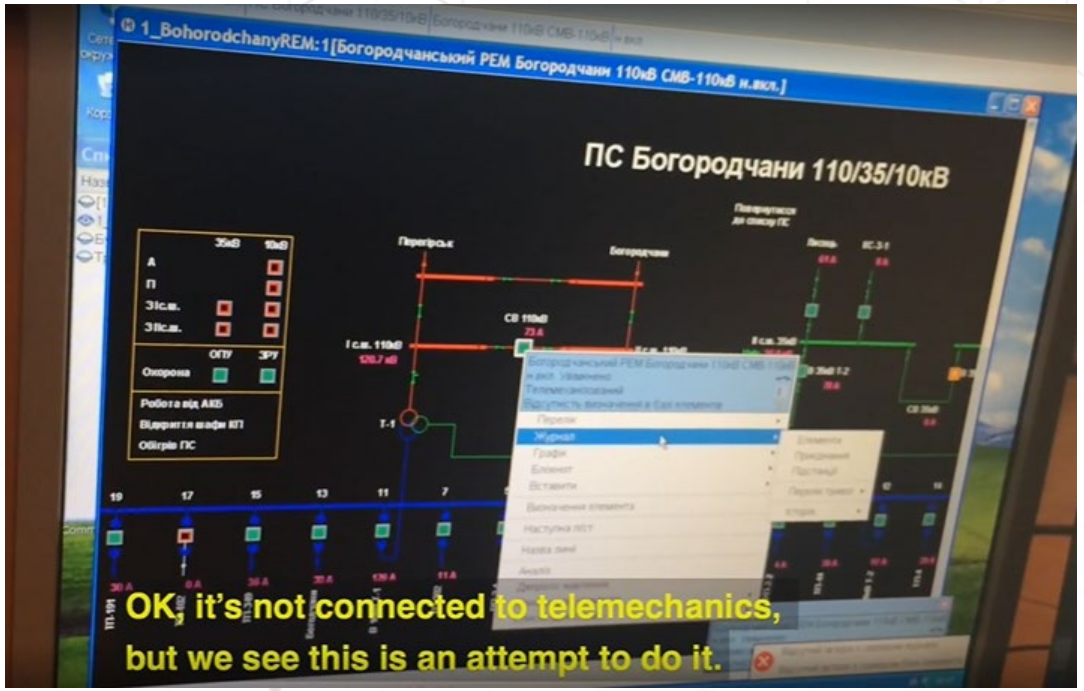
NERC Reliability Guideline: Cyber Intrusion Guide for System Operators, v2

- Guide to assist System Operators in recognizing events that may be an indicator of a cyber attack, and what to do and expect
  - Understand your role and expectations according to your company's Cyber Security Incident Response Plan
  - Provide *examples* of anomalies that *could be* associated with malicious cyber activity
  - Help plan owners understand and consider System Operators' perspectives
- Practically applicable beyond System Operators in RC, BA, and TOP roles



Could this be a sign of an attack?

- Sophisticated attacks targeting control systems often first appear as malfunctions, misoperations, or maintenance problems
  - On computer workstations
  - On protection and controls equipment
  - Other unusual occurrences
- Use a questioning attitude
- “See something, say something”



Initial actions and internal notifications

- Follow your company's plan and your supervisor's guidance!
- Continue to operate the system safely and reliably
- Escalations and notifications
  - OT or EMS, IT support and Cybersecurity
  - Field personnel
- Be ready to provide details on observed and potential effects

Response actions and external communications

- Follow your company's plan and your supervisor's guidance!
- *Possible* actions you may be asked to take:
  - Notify other operators
  - Guidance on release of information
  - Support isolation of devices or systems
- Be prepared to take operational actions in support of the investigation

For more information

Visit cyote.inl.gov

Sam Chanoski, CyOTE Program Principal Investigator
Samuel.Chanoski@inl.gov

NERC's Reliability Guidelines, Security Guidelines, Technical Reference Documents, and White Papers

https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

Thank You!

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response