










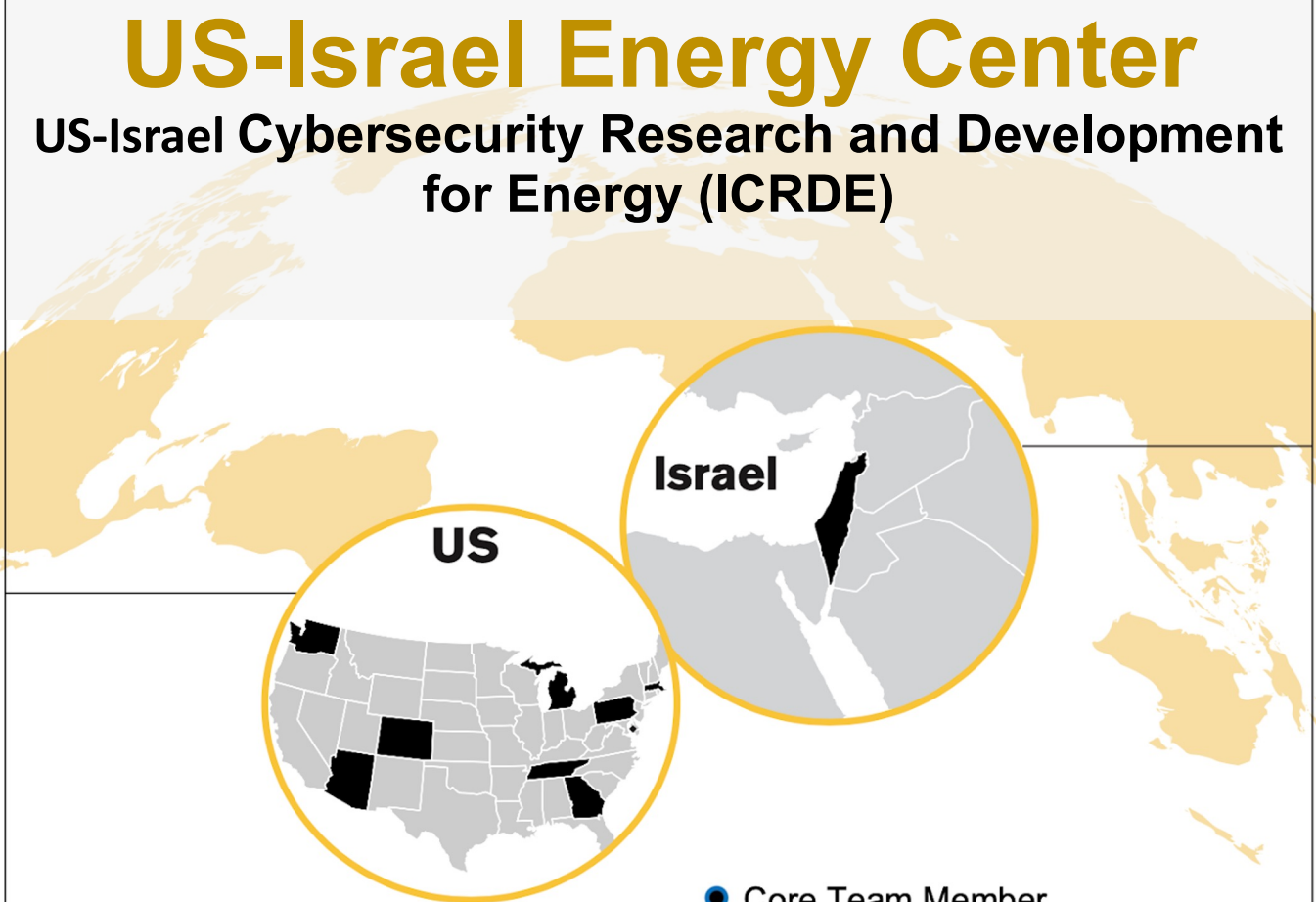





Arizona	  
Colorado	
Georgia	
Tennessee	
Massachusetts	
Michigan	
Pennsylvania	
Washington	
Washington, DC	

US-Israel Energy Center

US-Israel Cybersecurity Research and Development for Energy (ICRDE)



-  Core Team Member
-  Team Member (Volunteering Work)
-  Advisory Board



Grid Software Overview

John Dirkman, P.E.
Vice President, Product Management
jdirkman@resource-innovations.com



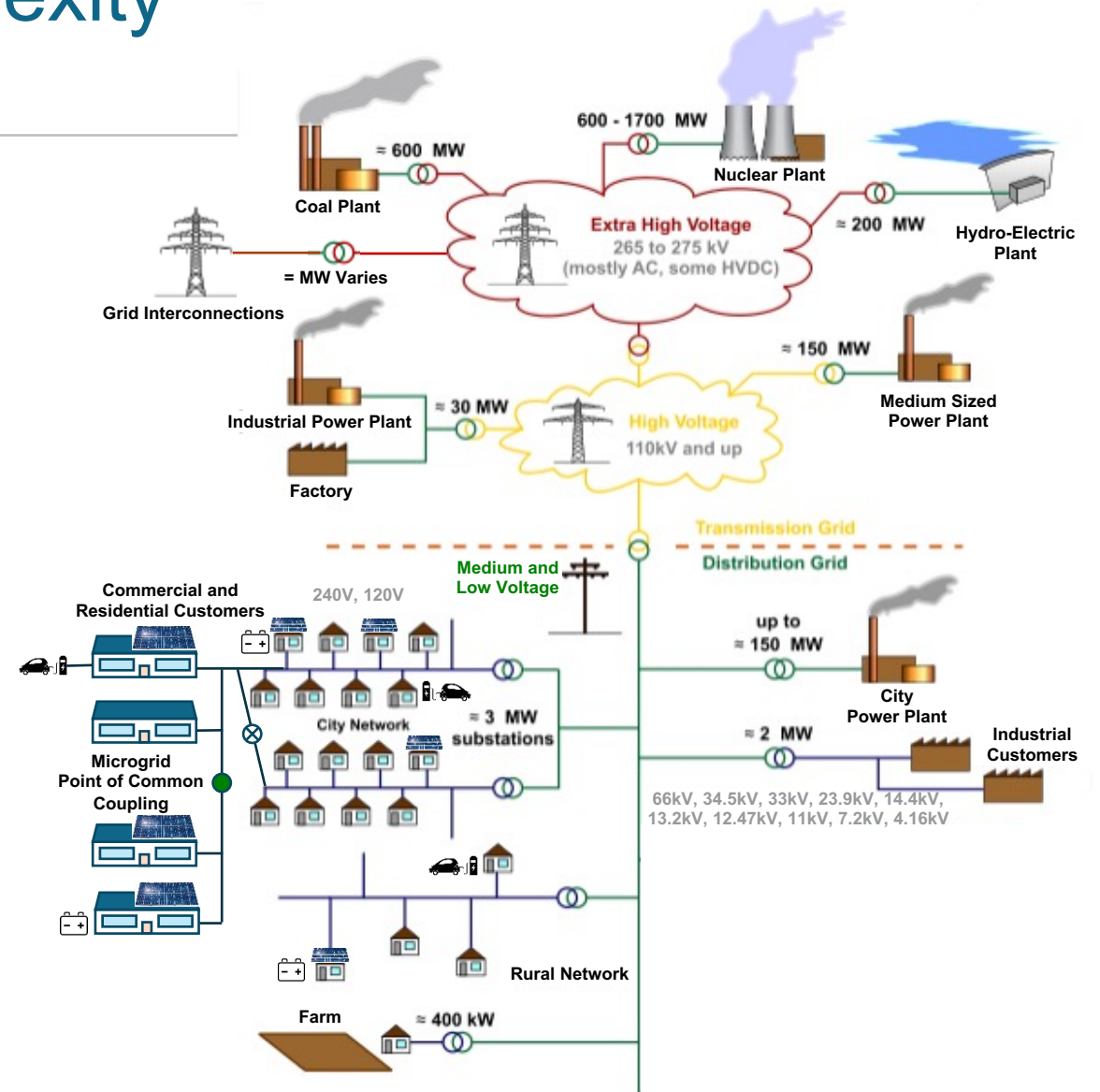
Electric Grid Organization Complexity and RI Grid Software Solutions

Customers Served

- Electric Transmission and Distribution Utilities
- Independent System Operators
- Energy Traders
- Grid Control System Suppliers (GE, Hitachi Energy, Toshiba, Smarter Grid Solutions)
- Department of Energy via Arizona State University

RI Grid software for planning, operational, and financial analytics

- Utilities must always balance supply (generation) and demand (load), or risk voltage and frequency problems which can lead to brownouts and blackouts.
- Variable renewable generation in transmission and distribution contributes to potential unbalance between supply and demand.
- Utilities have less control over the modern grid.



https://en.wikipedia.org/wiki/Electric_power_distribution

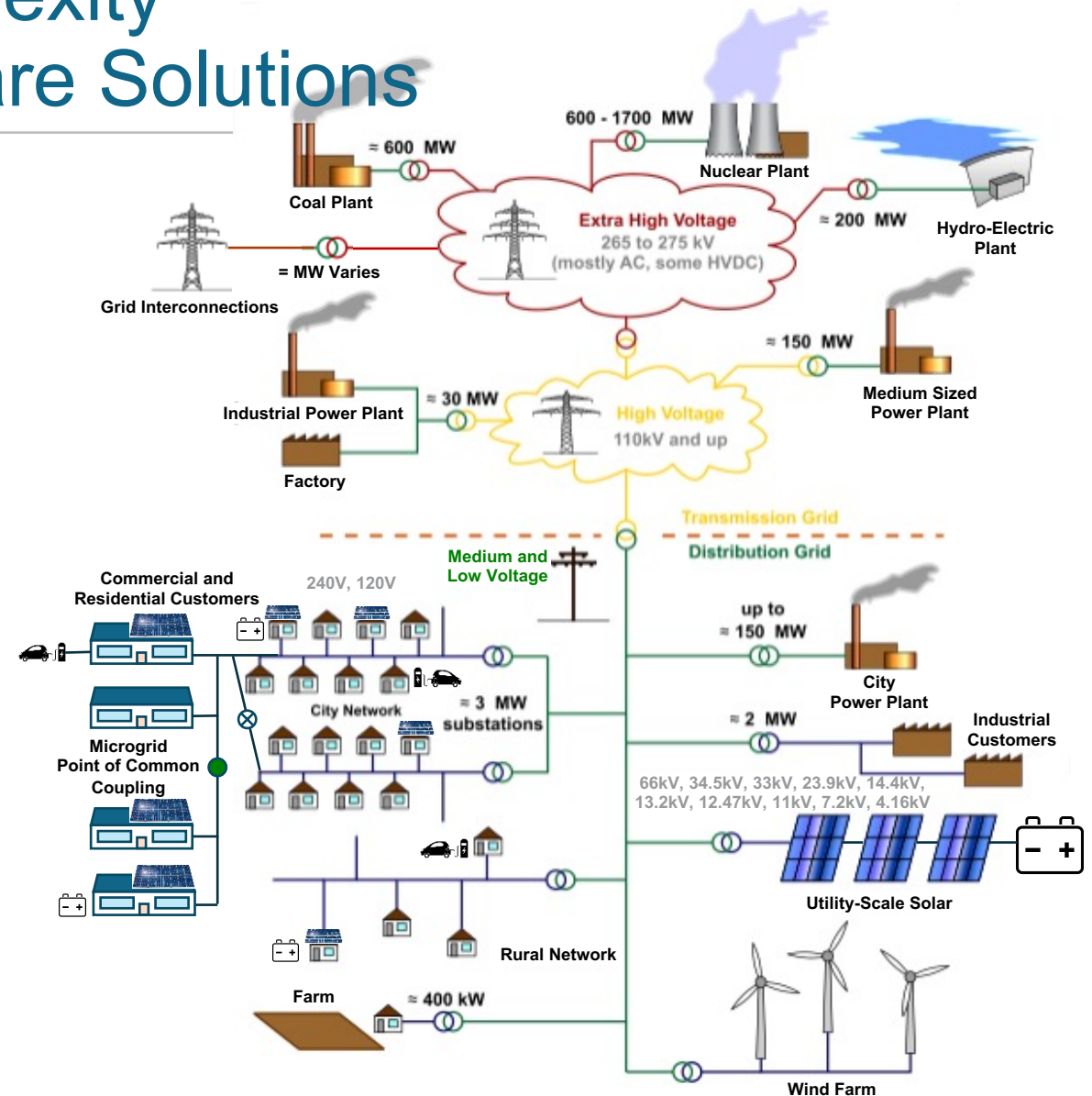
Electric Grid Organization Complexity and RI Transmission Grid Software Solutions

Transmission Energy Analytics Software

Grid360 Engines: T&D grid planning, operations and analytics

Day-Ahead Reactive Planning (DARP): Forecast and optimally dispatch grid resources to mitigate renewable variability, powered by the Grid360 Engines

Grid360 External Network Modeling (Modelex): Simplifies and consolidates transmission network models to improve analytical performance

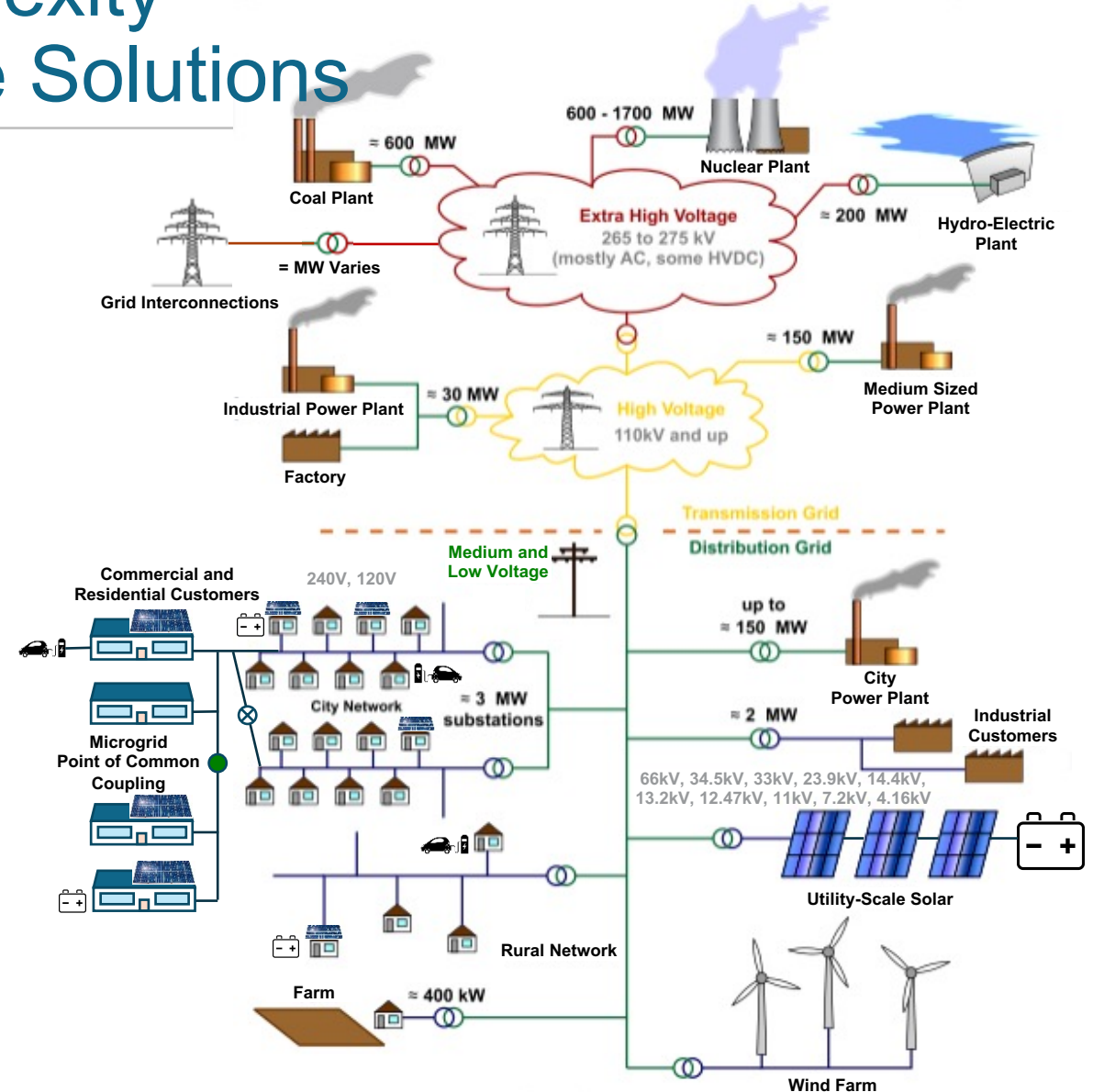


https://en.wikipedia.org/wiki/Electric_power_distribution

Electric Grid Organization Complexity and RI Distribution Grid Software Solutions

Distribution Energy Analytics Software

Grid360 Distribution Analytics: Advanced visualization, analytics, and planning applications, enabling demand response, distributed energy resources (solar and wind generation), electric vehicles, cybersecurity, and smart meter analysis and optimization, powered by the Grid360 Engines



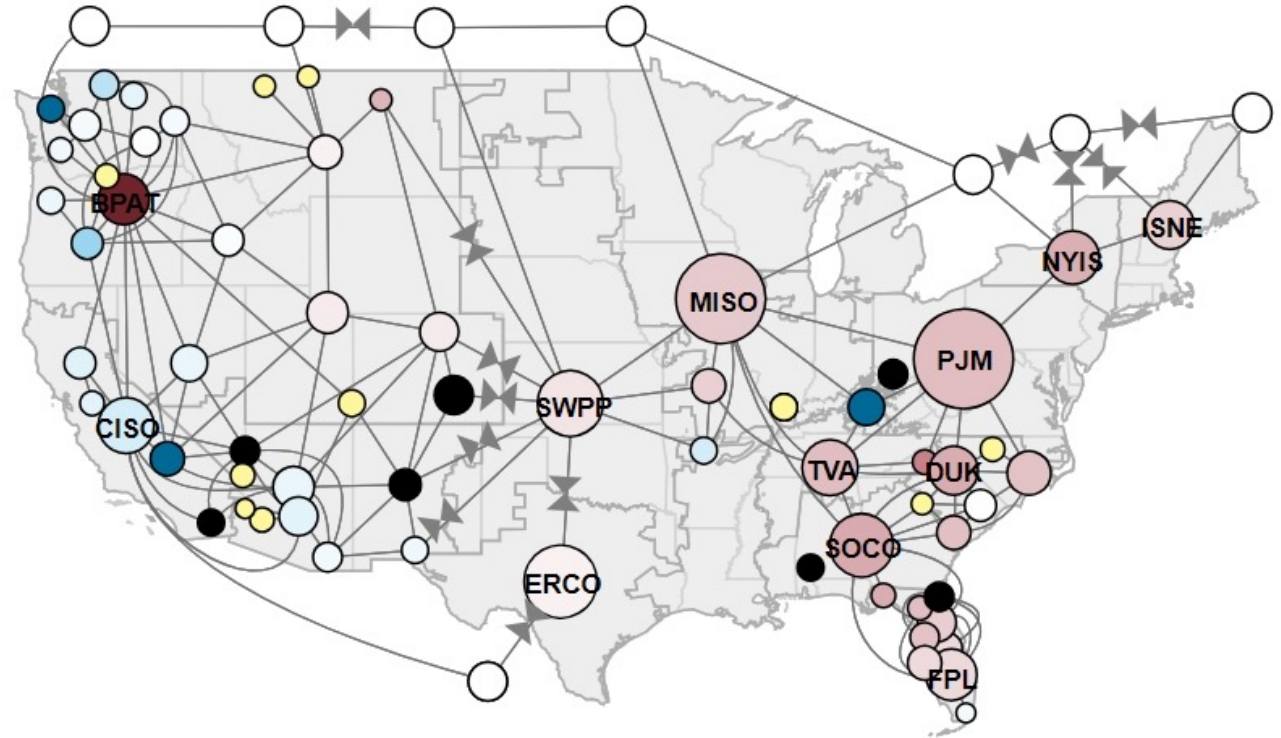
https://en.wikipedia.org/wiki/Electric_power_distribution

Electric Grid Organization Complexity and RI Financial Grid Software Solutions

Transmission Financial Analytics Software

iHedge: Energy market financial simulation, analysis, and engagement; used at ISOs in North America and New Zealand for congestion hedging by load serving entities and power traders, powered by the Grid360 Engines

\$3B
Annual FTR Value
Managed by iHedge
Software



eia Data source: U.S. Energy Information Administration

https://www.eia.gov/electricity/gridmonitor/dashboard/electric_overview/US48/US48

THANK YOU!

John Dirkman, P.E.

Vice President, Product Management

jdirkman@resource-innovations.com

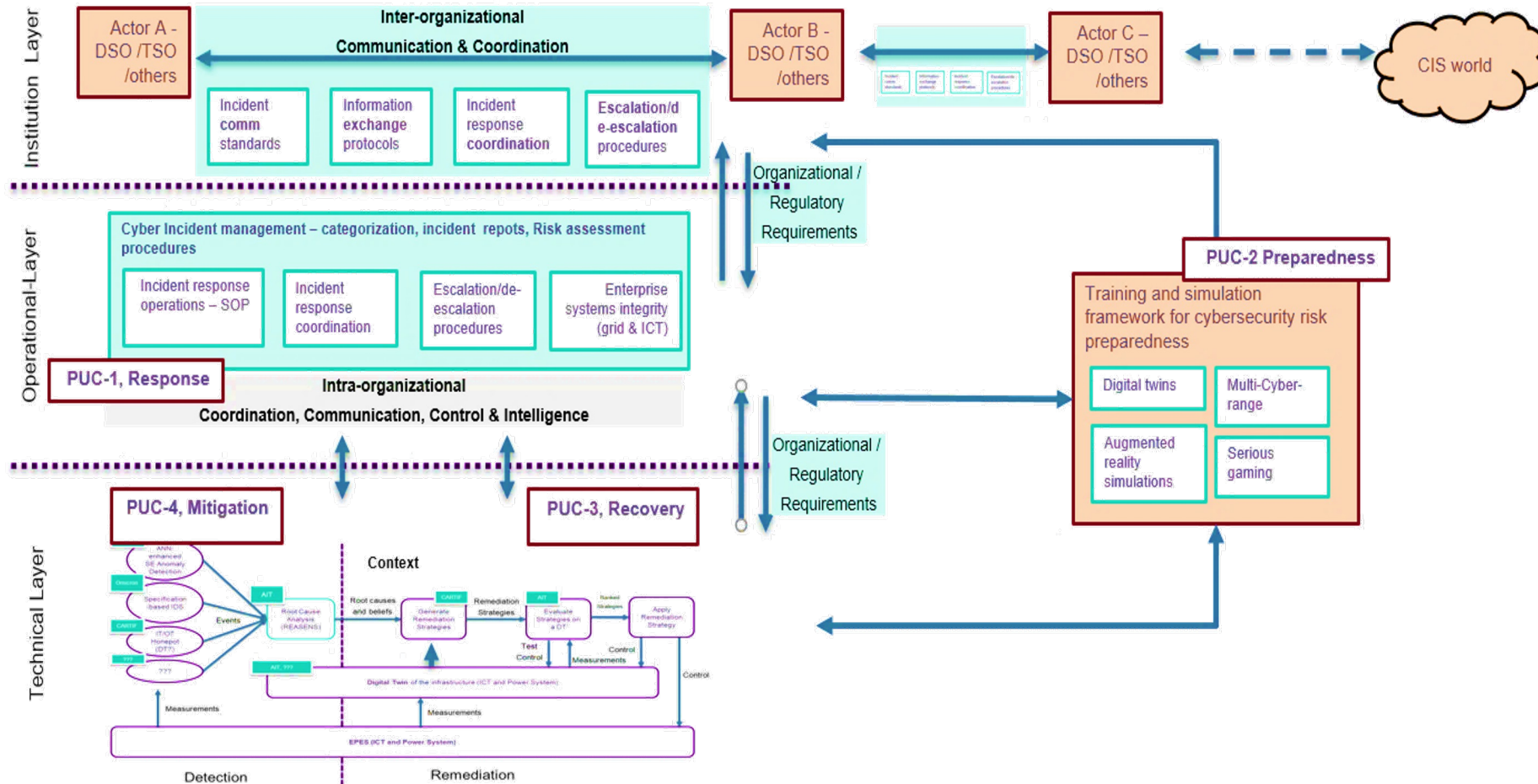


Situational Awareness in Cyber Incident Management: no one-size fits all

Senter for integrert krisehåndtering (CIEM)

Nadia Noori, PhD
Associate Professor i Institutt for IKT
Forsker, Senter for integrert krisehåndtering
Universitetet i Agder

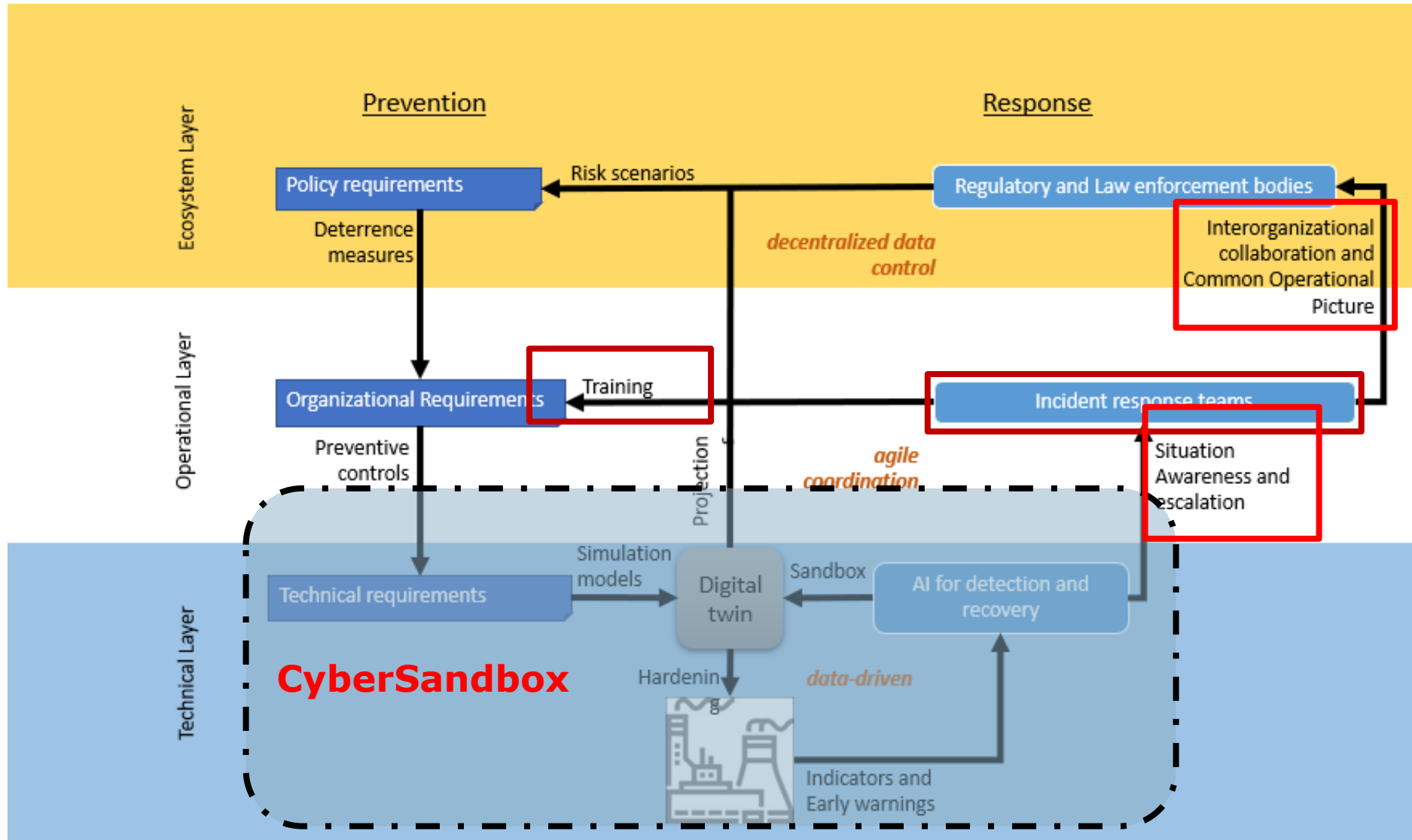
Cybersecurity incident management layers – energy sector



Integrated approach to effective cybersecurity incident management

- CI for energy sector is complex, multiple layers → multiple levels of vulnerabilities and cyber threats to assets - OT / IT infrastructure
- Need for mapping and classifications of the threats and the responses → SoP (*safety & security* CI CPS) → automation of detection and response (OT/IT levels)
- Coordination and communications between responder teams → Human in the Loop → SA, COP and CC2C, C3I

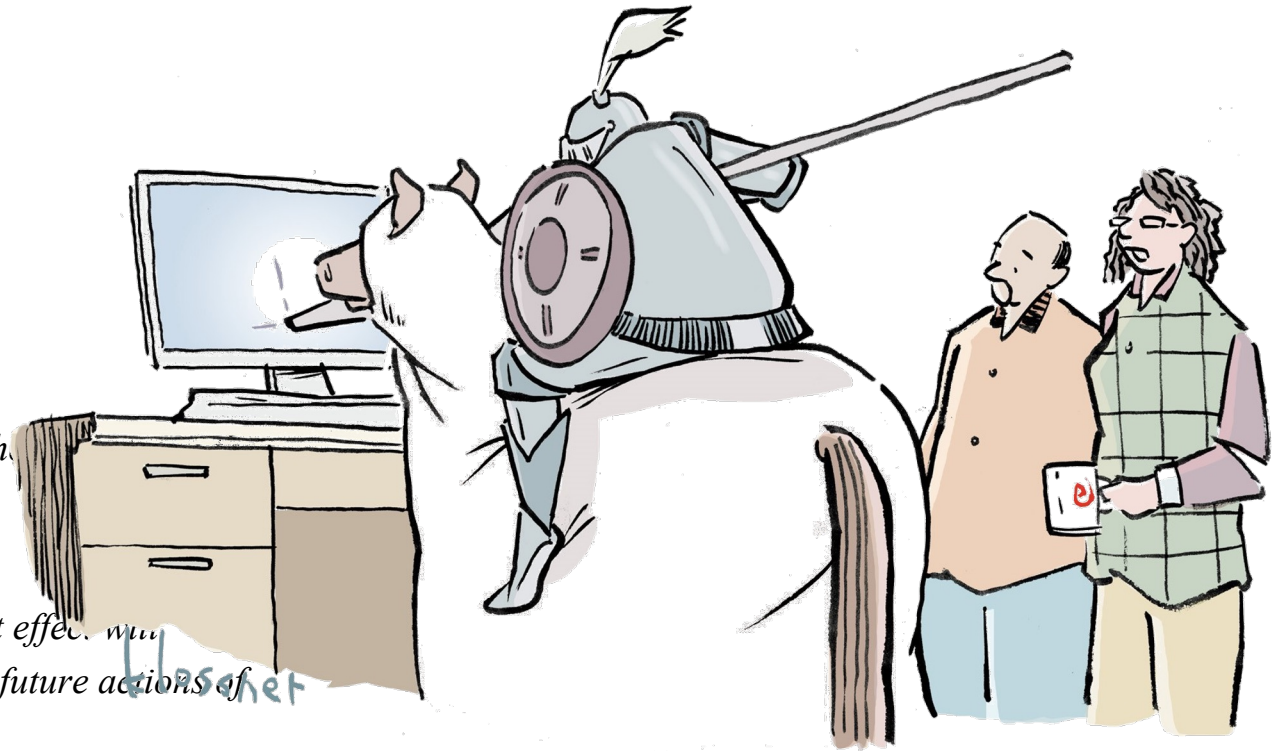
Information is KEY!



Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, 112, 102507.

Do we know anything about cyber security responders?

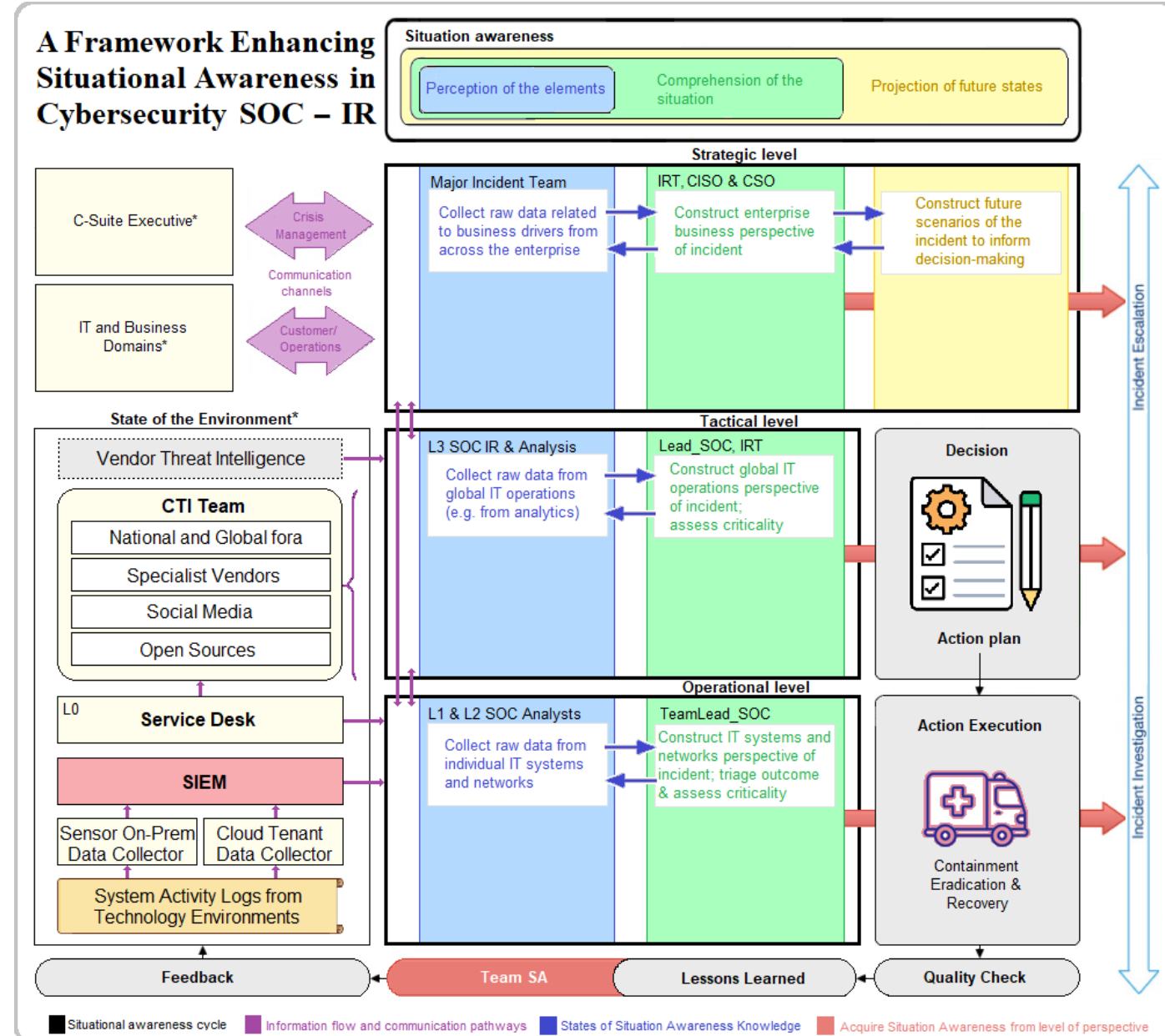
1. *Are attacks happening?*
2. *What might be their origin?*
3. *What might the attackers be trying to do?*
4. *What might the attackers do next?*
5. *Is deception and/or counter-deception involved?*
6. *How might the attacks affect my mission now, and how might they affect the future?*
7. *What options do I have to defend against these attacks?*
8. *How effective will a given option be against these attacks, what effect will exercising it have on my mission, and how is it likely to affect the future actions of allies and adversaries?*
9. *Might a defensive action “give me away”?*
10. *How do I prevent or mitigate the impact of such attacks in the future?*



Research on cyber security focus on *technical* and *managerial planning* (before the threat materializes)

Lack of an integrated approach to CERT Ops (tools and COPs)

Situational Awareness (SA) Framework for SoC – Incident Response

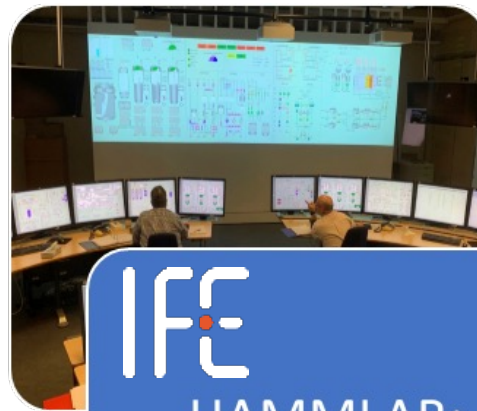


Andreassen, J., Eileraas, M., Herrera, L. C., & Noori, N. S. (2022, October). InCREASE: A Dynamic Framework Towards Enhancing Situational Awareness in Cyber Incident Response. In *International Conference on Information Technology in Disaster Risk Reduction* (pp. 230-243). Cham: Springer Nature Switzerland.

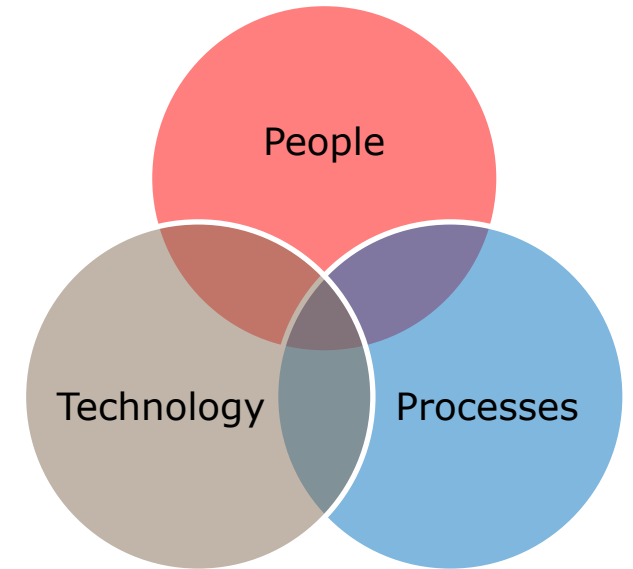
A realistic environment for studying cybersecurity incident response



Cybersecurity center:
Security operations center



IFE
HAMMLAB:
Control room



Evaluation of human preparedness and decision-making during cybersecurity incidents

*HAMMLAB - Halden Advanced Man-Machine Laboratory

Can automation be engaged as a partner?

- Critical challenges of cyber operations is ability to keep up with the increasing volume and sophistication of network attacks



Software agents as sensemaking partners and enhanced threat intelligence

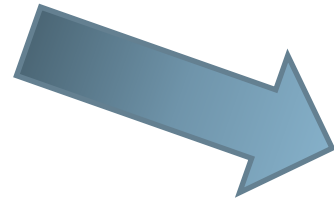
- Automation help reducing volume of uncorrelated events (AI-ML)
- Agent learning (Reinforcement learning)



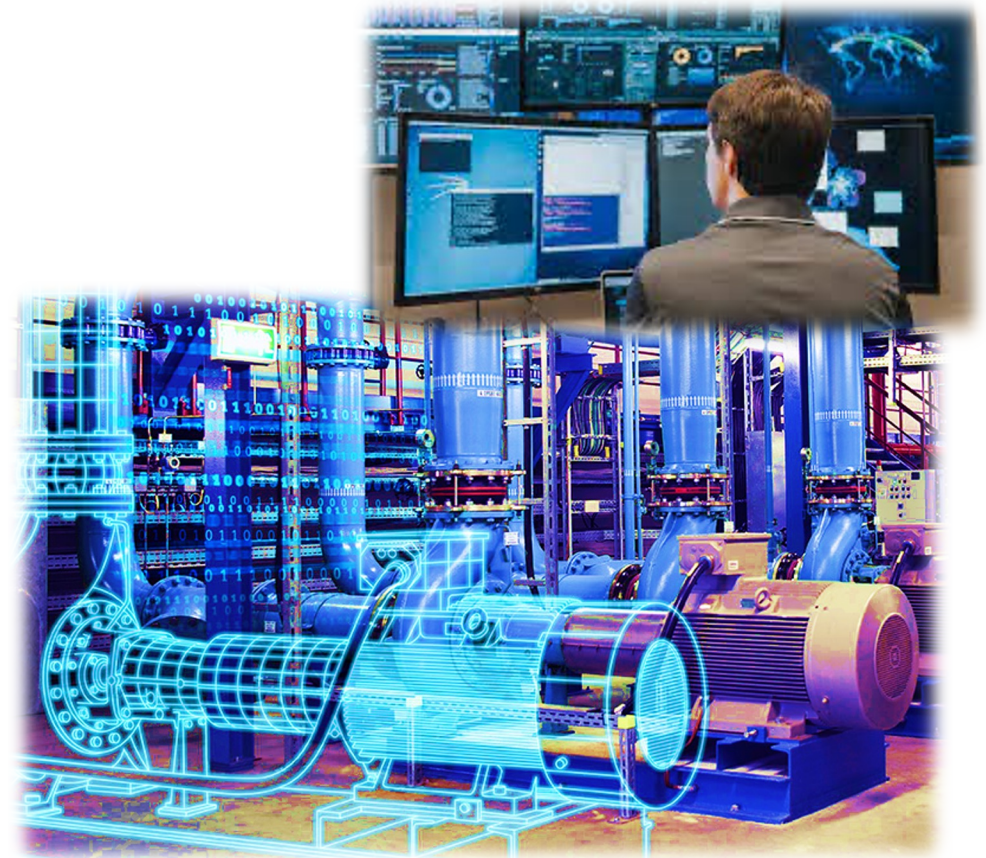
Cybersecurity preparedness?



Human-Military Operations Coordination Centre (HuMOCC) during the TRIPLEX 2016 at camp Lista, Norway. Credit: OCHA



CCI-CERT operations



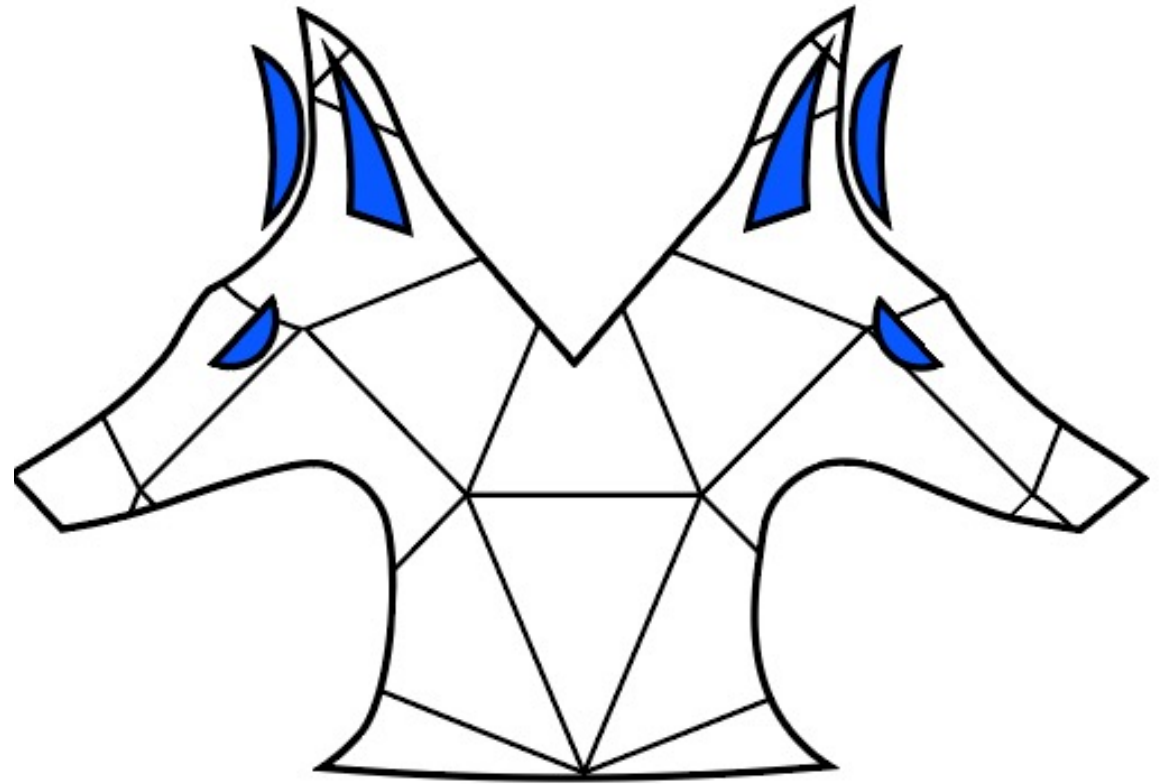
**Tusen takk!
Thank you!**

Nadia Noori, PhD

Nadia.saad.noori@uia.no

Associate Professor i Institutt for IKT
Forsker, Senter for integrert krisehåndtering

- Reinforcing Today, Securing the Future



Orthros



About us

- Based in Montreal, Canada
- 10+ years experiences on the field as technician
- Certificate in industrial automation and cybersecurity at Polytechnique de Montreal
- Experience in working with diverse industries and infrastructures
 - Petrochemical
 - Water treatment
 - Manufacturing
 - Aeronautic
 - Public transportation



Our goal : Securing critical infrastructure

- Provide advice and support to protect critical infrastructure against cyber treats based on industry standard
- Provide long-term solutions and roadmap to ensure business continuity and resilience
- Customer-centric approach for better customized cybersecurity strategies
- Be an active member in the cybersecurity community

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 2:

What approach do you propose for legacy environments where digital transformation is a real challenge?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 3:

Assuming attacks happen and will happen -
How can you deal with the loss of assets
visibility & control in the most common
attacks – i.e., Ransomware type attacks?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 4:

How could AI help detect and mitigate cyber vulnerabilities? (in Panel A)

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 5:

How can emerging sensing technologies be leveraged to protect the power system against cyber threats?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 7:

How do you manage cyber threats (e.g., ATT&CK) to critical infrastructure?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 8:

How do you leverage important information to inform detection/information sharing?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 9:

What are the most important aspects to consider in risk management on the energy infrastructures?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 10:

How to prioritize risks in OT networks?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 11:

Proactive vs. Reactive approach in OT security?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 12:

How do you manage anomalies when you receive an alert?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 13:

Which AI products are most helpful for security management?

QUESTIONS @ PANEL C:

SECURITY MANAGEMENT AND INFORMATION SHARING



Question 14:

How do the advanced language models and chatbots affect security management and information sharing?