SYSTEMS ENGINEERING RESEARCH CENTER

SERC RESEARCH REVIEW 2024 | NOVEMBER 12, 2024

Center for Offshore Wind Energy Cyber Vulnerabilities and Threat Identification

WRT-1087

Office of Enterprise Research and Innovation

Sachin Shetty, Old Dominion University

Peter Beling, Virginia Tech

OLD DOMINION UNIVERSITY

VIRGINIA TECH

Project Overview

- **Mission**
  - Establish a cybersecurity center for wind energy.
  - Address the increasing cybersecurity risks facing **Wind Energy Farms** (WEFs) off the coast of Virginia.
  - Identify and mitigate vulnerabilities in wind energy systems.
  - Develop industry-wide best practices for robust defense strategies
- **Team**
  - Old Dominion University
  - Stevens Institute Of Technology
  - Virginia Tech

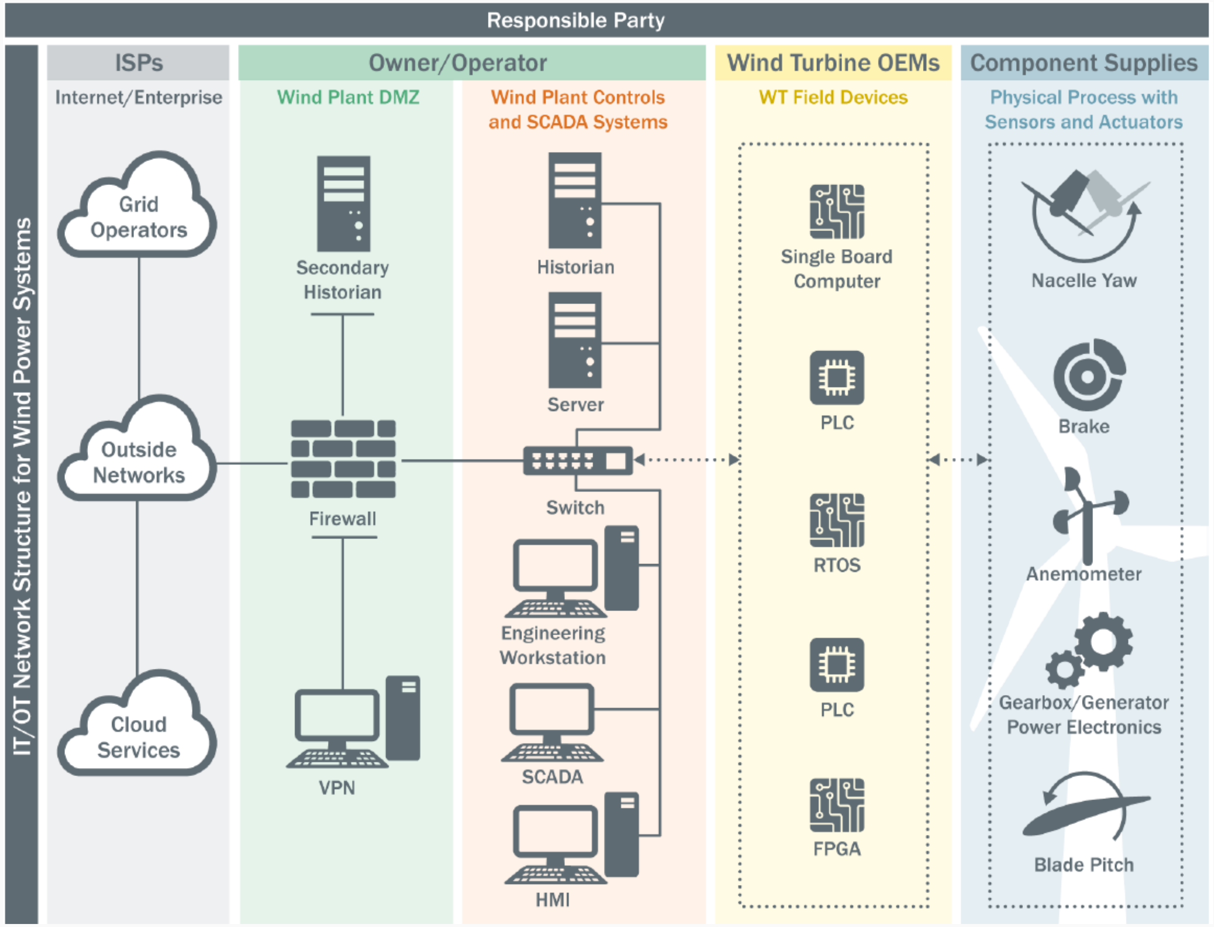
Project Overview

- **Project Objectives**
  - Establish a Center for Collaboration dedicated to cybersecurity R&D for WEFs and related critical infrastructure.
  - Developing testbed to assess cyber readiness and evaluate detection strategies for eavesdropping attacks within offshore wind turbines.
  - Identifying cybersecurity threats to WEFs and other energy infrastructure and devising defense strategies and best practices.
  - Integrating systems engineering methods from the Department of Energy's (DOE) National Nuclear Security Administration’s (NNSA) Operational Technology Assurance (OTA) Guidebook with Secure Cyber-Resilient Engineering (SCRE) methods and tools.

Project Overview

- **Research Tasks**
  - **WEF Security**
    - Focuses on designing detection models for attack surfaces exposed by the convergence of operational technologies (OT) and information technologies (IT) in wind farm systems.
  - **Cyber Resilience Methodologies**
    - Aims to develop systems engineering methods applicable to resilient energy delivery systems and integrate SCRE practices with OTA guidance.

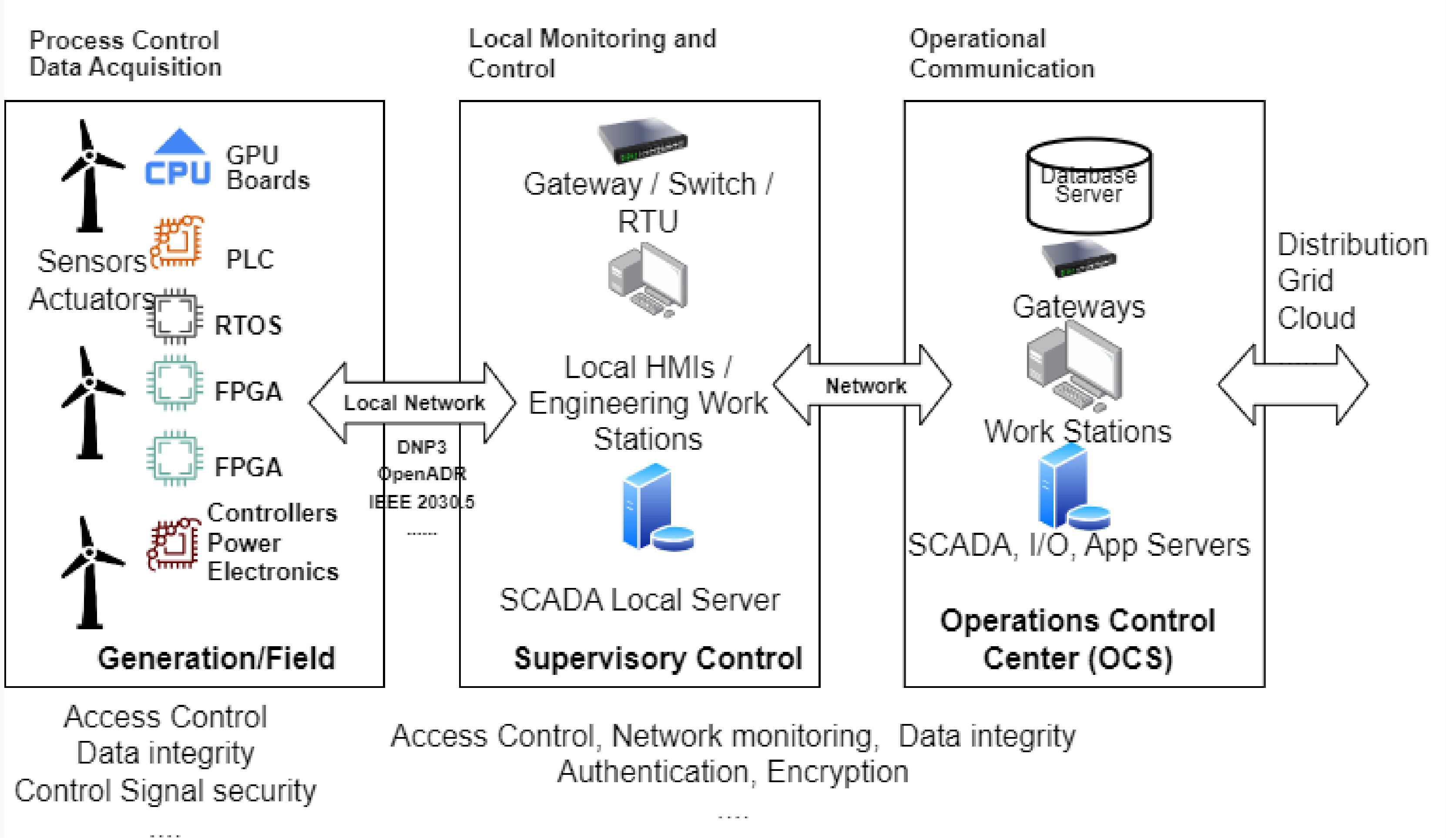
Wind Energy Farm (WEF) – *Overall Schematic*



Schematic representation of the IT/OT infrastructure in a wind plant

Source: DOE Report- *Roadmap for Wind Cybersecurity, July 2020*

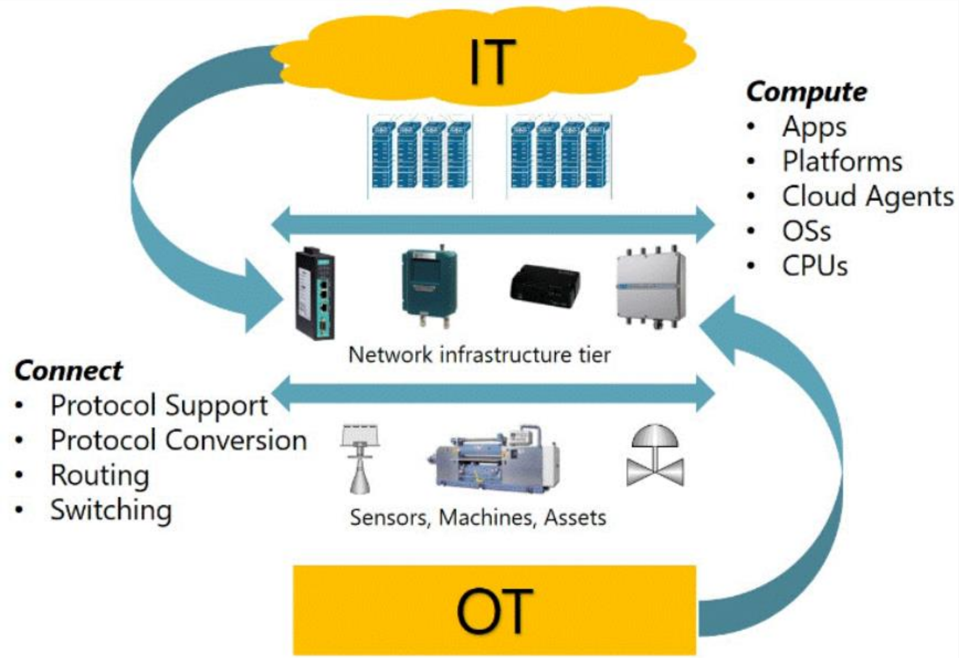
WEF Infrastructure



Wind Energy System Components, Interconnection, Functions, and Security Features

WEF Cyberthreat Landscape

- **Energy systems are increasingly interconnected, digitized, and remotely operated.**
- **Digital assets in Energy systems involve *digital components* from different vendors.**
- **High supply chain risks for digital components**
  - Software (including firmware), virtual platforms and services, and data
- OT, Industrial Control Systems, and ICT systems



* Cybersecurity and Digital Components – "Supply Chain Deep Dive Assessment" U.S. Department of Energy Response to Executive, Order 14017, "America's Supply Chains" February 24, 2022

WEF Cyberthreat Landscape

- **Established Vulnerabilities**
  - **Cyber attack targeting a wind plant SCADA system[1]**
    - Malicious actor could gain unauthorized control of a wind plant, send false commands to target components, and stop or potentially damage wind turbines.
  - **Cyber and Physical attack scenarios focused on wind plant disruption and turbine damage[2]**
    - **Attacker's fabricate turbine control messages by exploiting unsecured implementation of control devices**
  - **Vulnerabilities targeting two wind turbine systems[3-5]**
    - **Loss of power to all attached systems**
  - **Attacks on Local Network and Communication infrastructure**
    - **Disrupt / sabotage distributed energy coordination and control**

1. Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. "Cyberattack to Cyber-Physical Model of Wind Farm SCADA." Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018.
2. Staggs, Jason, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation." *International Journal of Critical Infrastructure Protection* 17 (2017): 3-14. DOI:10.1016/j.ijcip.2017.03.001.
3. ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability." August 27, 2018. https://icscert.us-cert.gov/advisories/ICSA-15-076-01.
4. ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability." August 27, 2018. https://icscert.us-cert.gov/advisories/ICSA-15-076-01.
5. ICS-CERT. "RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability (Update A)." August 27, 2018. https://ics-cert.us-cert.gov/advisories/ICSA-15-162-01A.

WEF Cyberthreat Landscape

- **Established Vulnerabilities (Continued …)**
  - Most common cybersecurity issues
    - Spoofing of user identity
    - Tampering
    - Repudiation
    - Information disclosure
    - Denial of Service (DoS)
    - Elevation of privilege.
  - Realistic attacks on emulated SCADA and Distributed / Integrated Energy communication networks are possible due to:
    - Interoperability protocols and communication protocols (IEEE 2030.5, IEC 61850, SunSpec Modbus)
    - Network topologies (e.g., utility-to-wind plant, utility-to-aggregator-to-wind plant)
    - Encryption schemes (symmetric, asymmetric), key management, and key sizes
    - Firewall rules and role-based access-control lists
    - Firmware update/patch levels
    - Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)
    - Novel research concepts

WEF Cyberthreat Landscape

- **Established Cyber Events**

AWEA 2018: Increase in cyber security attacks 'inevitable', expert warns

In one incident, a technician logged on to his laptop in a hotel and downloaded malware by mistake. When he went to work the next day and logged on, the wind farm became infected and the turbines stopped working one-by-one, Bailey said during a talk on cyber security.

Grid leaders clear the air around Russian hacking

By Blake Sobczak | 08/01/2018 06:45 AM EST

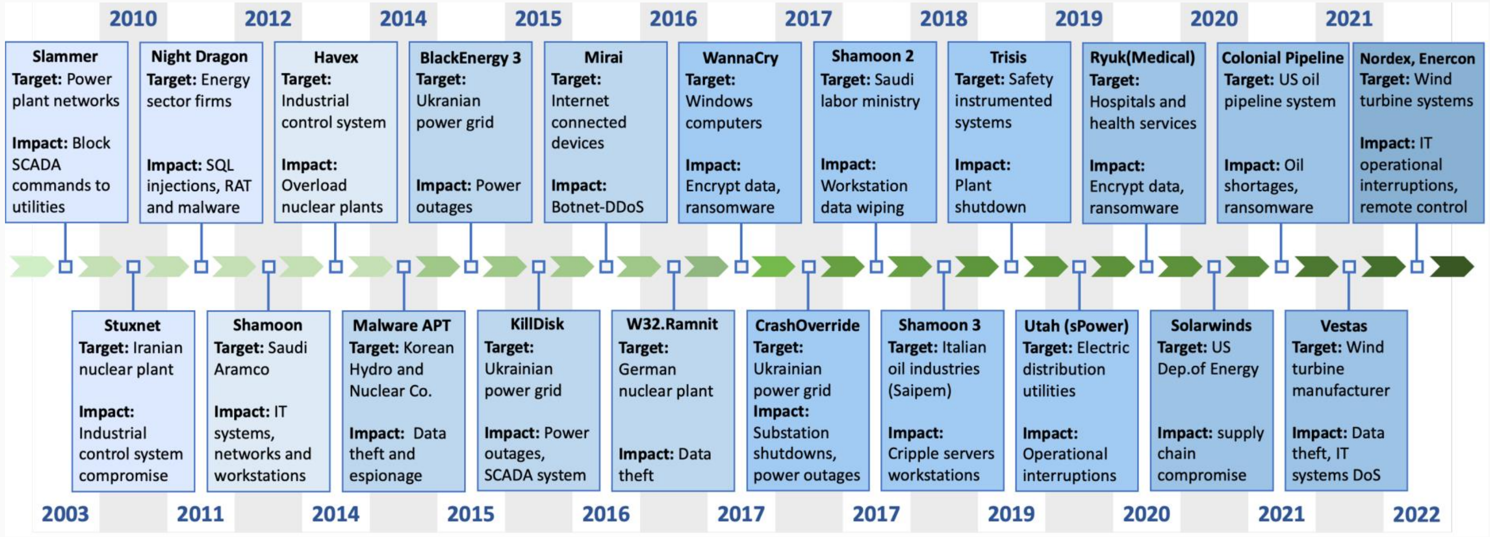
NEW YORK — A wind power generator fell into Russia-linked hackers' crosshairs last year, but the attackers never managed to put the wider U.S. grid at risk, officials confirmed yesterday at a Department of Homeland Security cybersecurity conference here.

Tom Fanning, CEO of utility Southern Co., said the hackers' reach appears to have been "very limited" — perhaps just "one or two wind turbines" at an undisclosed power company.

First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say

New details of a denial-of-service attack earlier this year show an energy sector with uneven security.

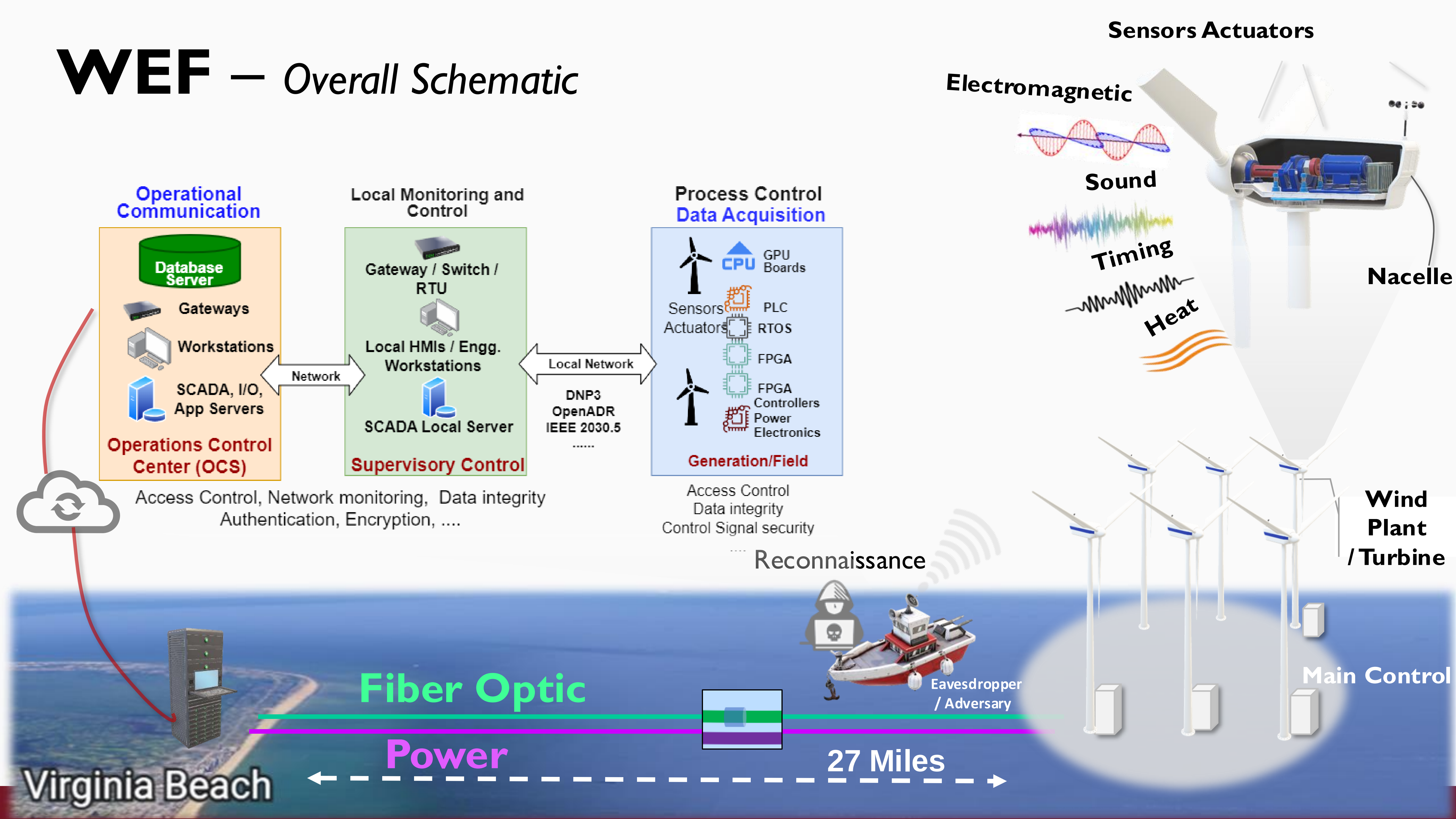
Published Nov. 4, 2019



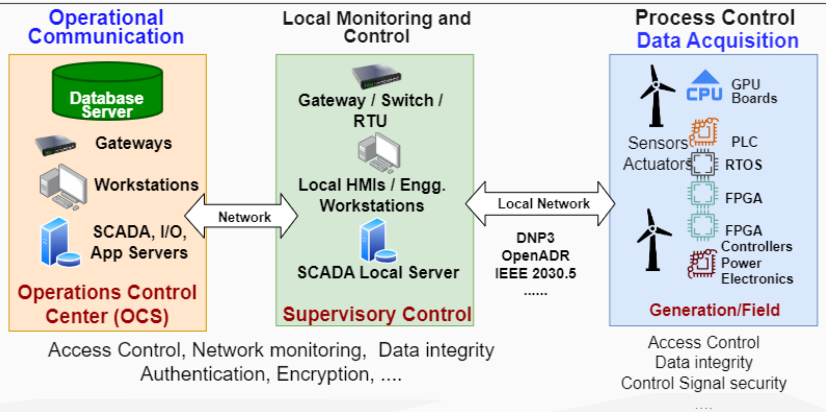
Timeline of cyberattacks targeting the energy sector and other critical infrastructure sectors.

Source: Ioannis et al. "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations." IEEE, Systems Journal (2023)

WEF – *Overall Schematic*



Wind Energy Farm – *Testbed Devices and Software*



Hardware

SCADA Servers
Historian
Station
Switches

Control + Data Acquisition
1. PLCs,
2. RTUs,
3. FPGAs,
4. IoT Boards, and others.

Wind Turbines
1. Vertical / Horizontal,
2. Capacity,
3. Control parameters,
4. MAST and other sensors
5. Operation and Installation.

Communication Vulnerabilities

Control, Communication (MAC / UDPs), Authentication Protocols
IEEE 2030.5, Modbus, IEEE 1815 / DNP3, OpenADR, and others

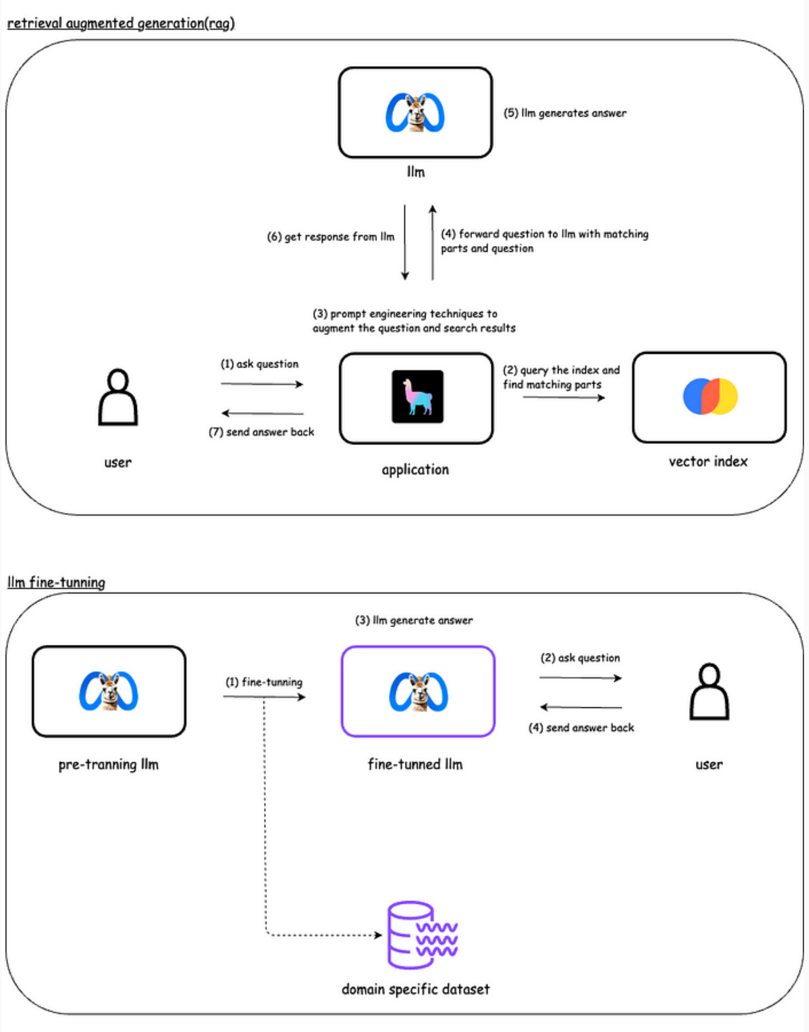
EMC-EMI and Side-Channel Vulnerability Analysis

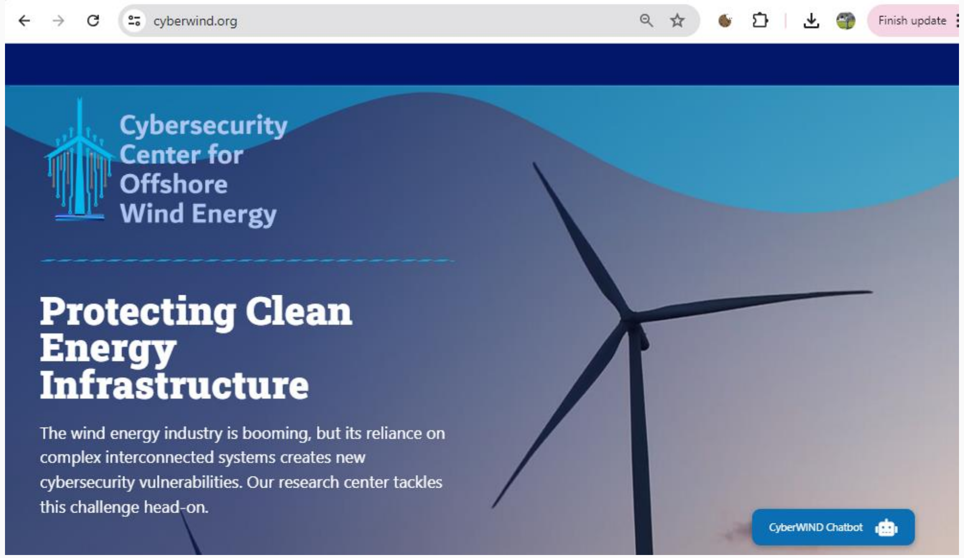
Near and Far Field EM Emanation Analysis of PLCs, RTUs, FPGAs, IoT Boards, and other communication and control equipment.

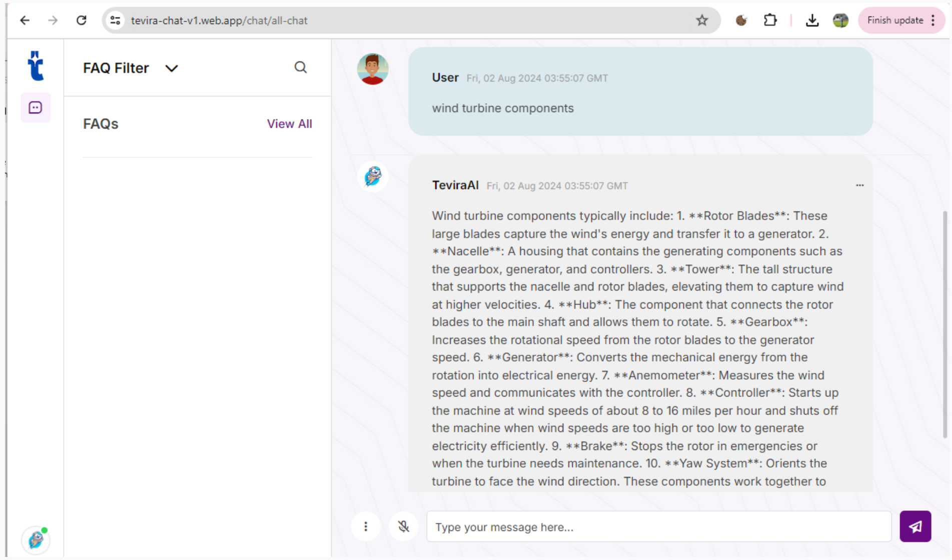
Cybersecur Center for Offshore Wind Energy

Scaled down Testbed

CyberWind Chatbot



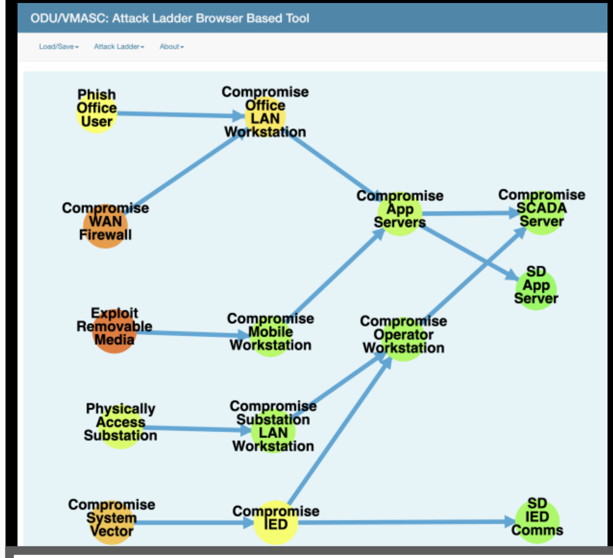




Scaled down Testbed

Attack Ladder Model for Wind Energy

Measuring probabilities of attacks on cyber physical systems to provide a foundation for measuring risk formally.



Phish Office User Rung Achieved	Compromise WAN Firewall Rung Achieved	Exploit Removable Media Rung Achieved	Physically Access Substation Rung Achieved	Compromise System Vector Rung Achieved	Compromise Office LAN Workstation Rung Achieved	Compromise Mobile Workstation Rung Achieved	Compromise Substation LAN Workstation Rung Achieved
48.70% of samples	71.00% of samples	78.10% of samples	39.10% of samples	61.80% of samples	54.10% of samples	27.10% of samples	25.00% of samples
Phish Office User	Compromise WAN Firewall	Exploit Removable Media	Physically Access Substation	Compromise System Vector	Compromise Office LAN Workstation	Compromise Mobile Workstation	Compromise Substation LAN Workstation

Compute probability of success for each successive attack stage

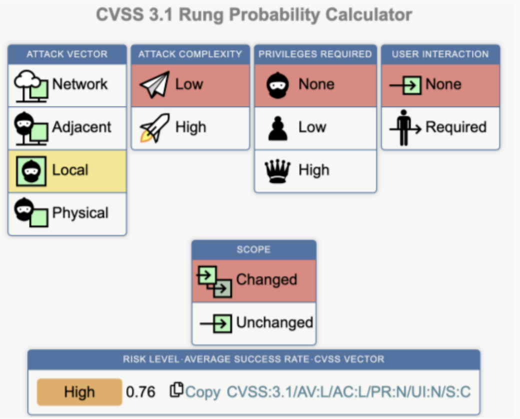
Features:

- Immediate results even for very large attack ladders.
- Export results in csv format for external analysis.
- Quick and easy installation; up and running in minutes.

Integrates with:

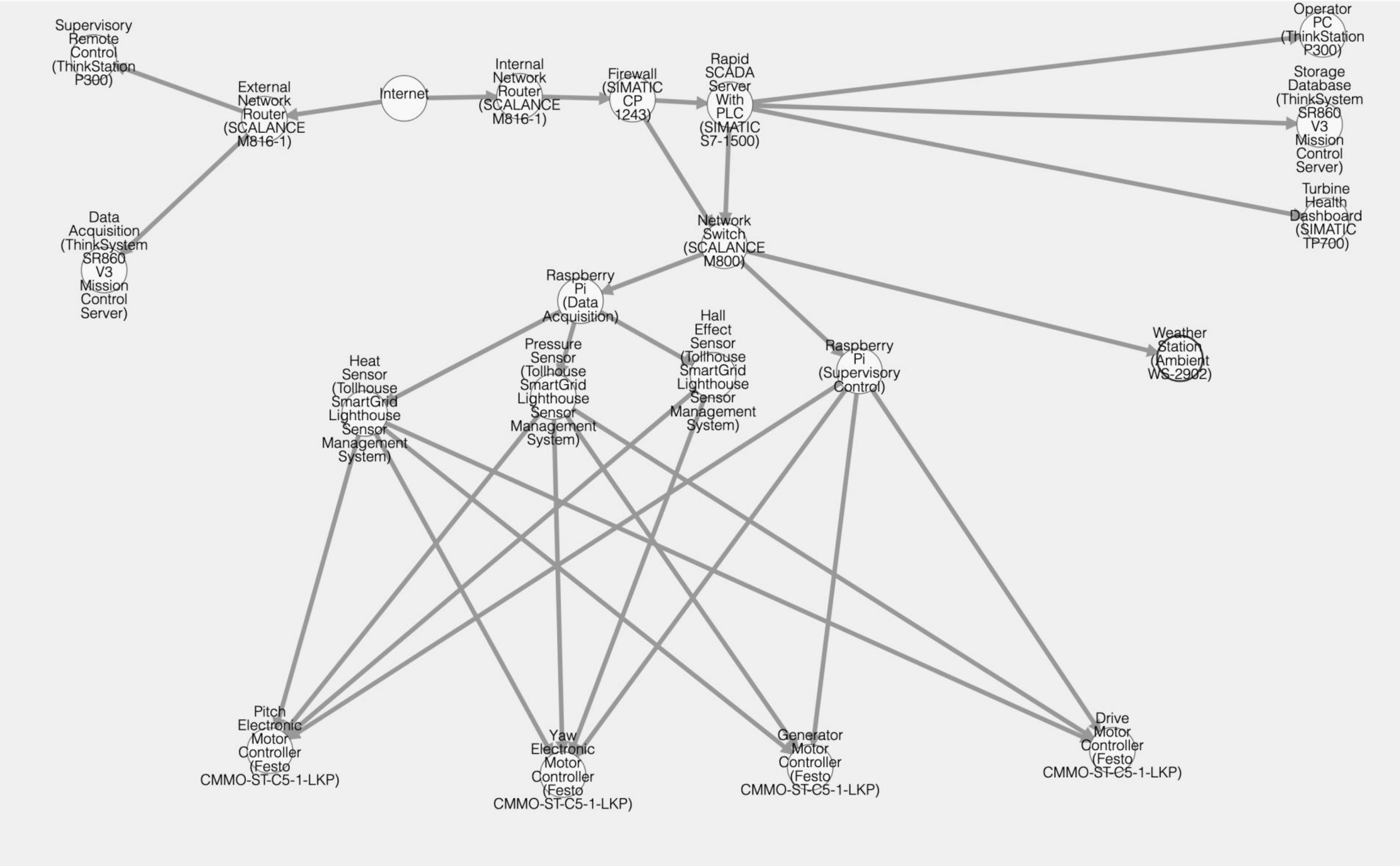
- MITRE ATT&CK Groups and Techniques.
- CVSS 3.1 & Army CVSS to help specify exploit probabilities.
- ODU / VMASC other developed tools

MITRE ATT&CK™

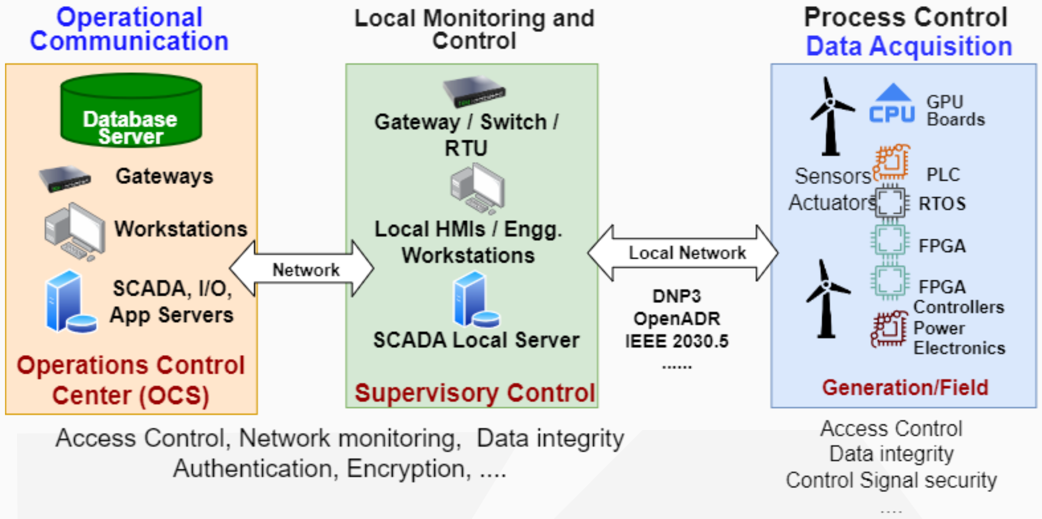


Scaled down Testbed

Attack Ladder Model for Wind Energy



PNNL – Collaboration



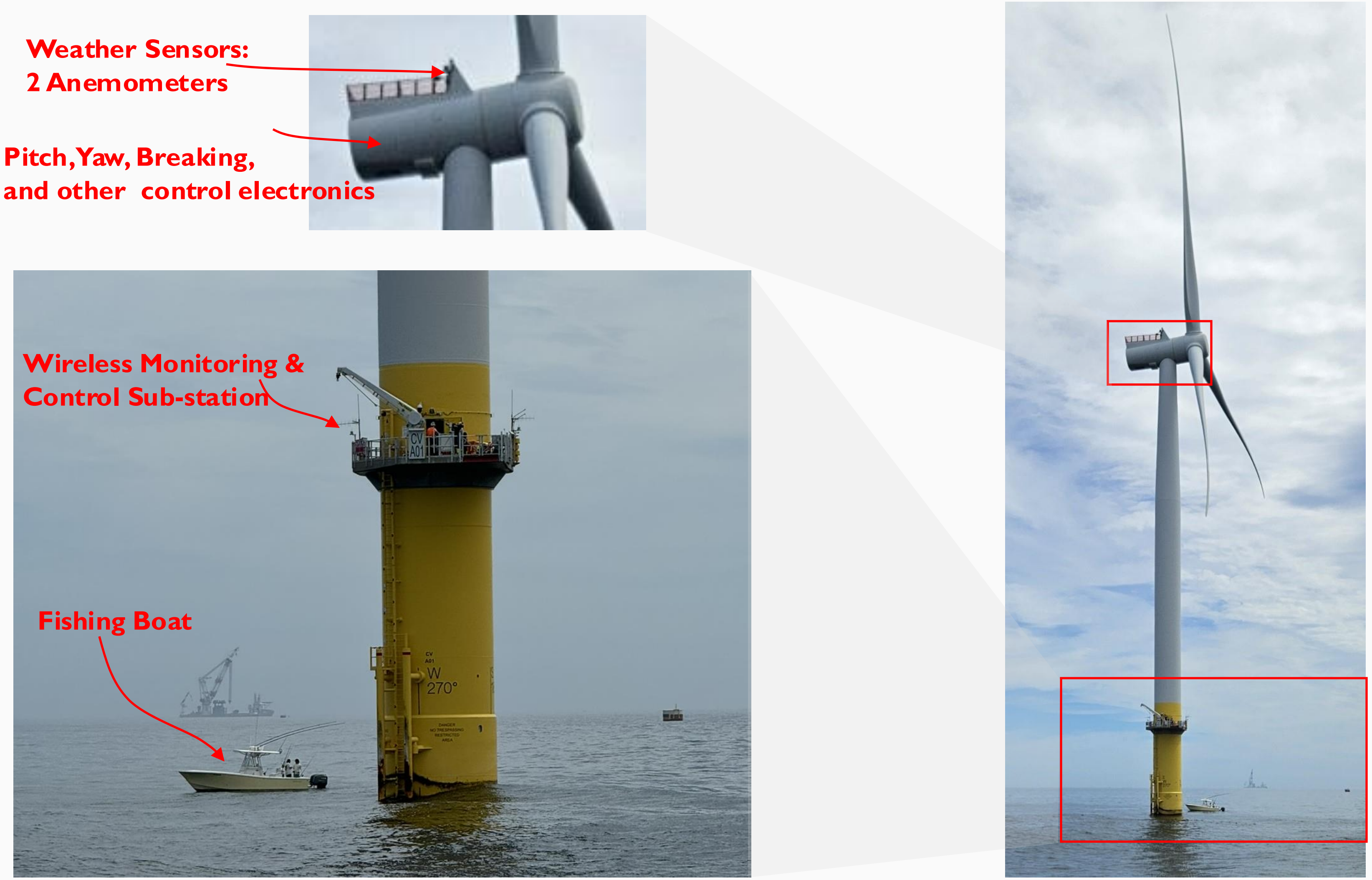
SCADA Servers
Historian
Station
Switches

Control + Data Acquisition
PLCs | RTUs |
IoT Boards, and others.

Wind Turbines and Turbine Models
(Simulink + Raspberry PI)

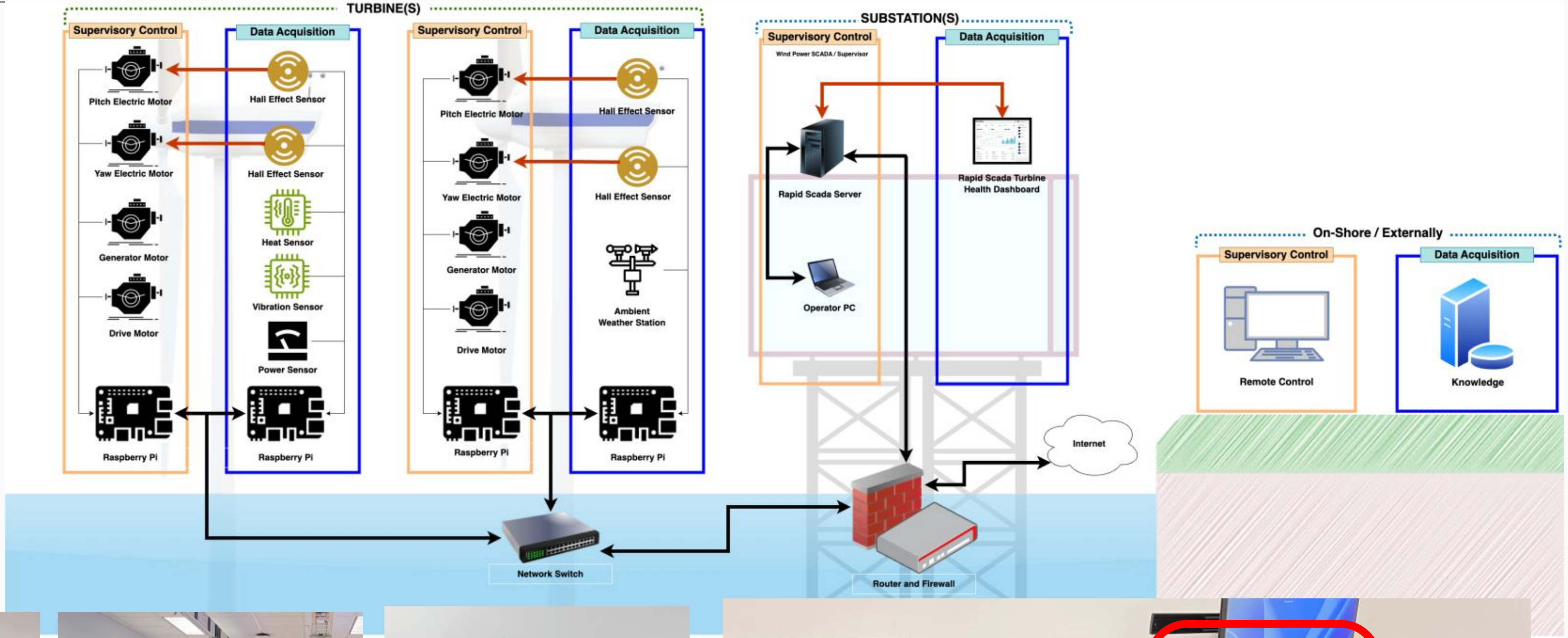
Exchange: PCAP, EMC-EMI, Turbine Models (Simulink+RPi), m

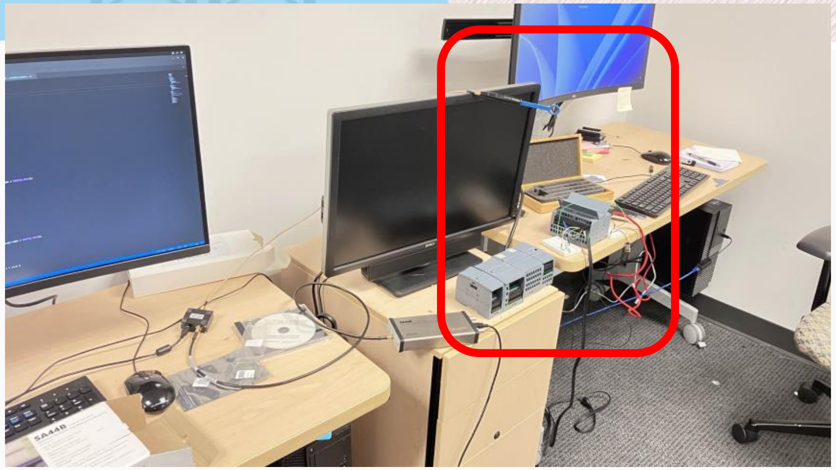
Coastal Virginia Offshore Wind (CVOW)



Scaled down Testbed

WEF Testbed Design and Development

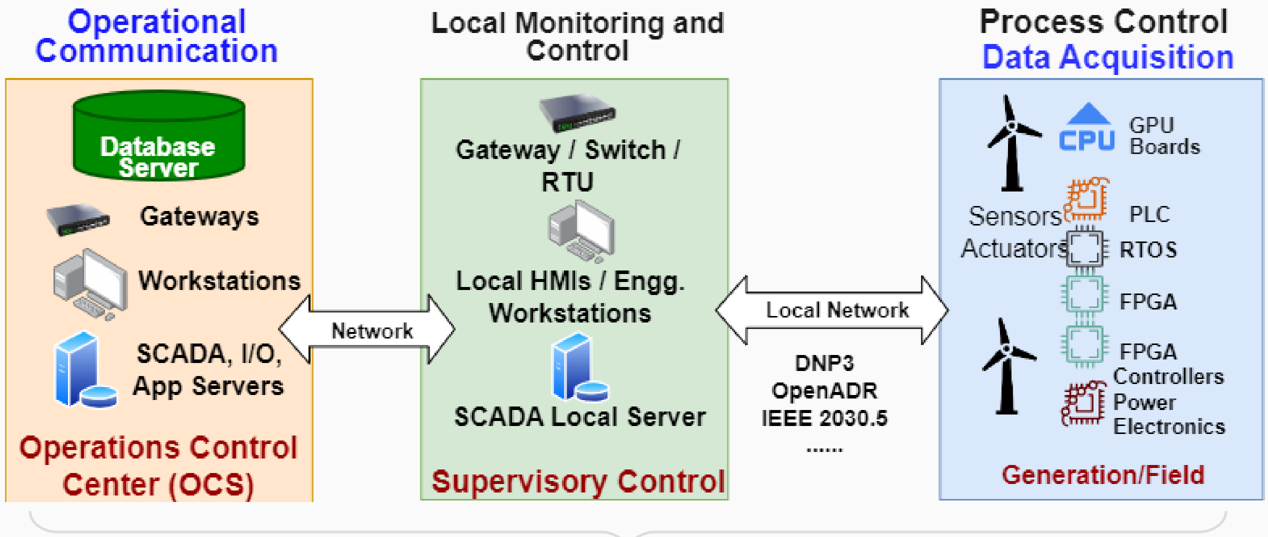




MAST Sensors and Near-Field Probes' Testing

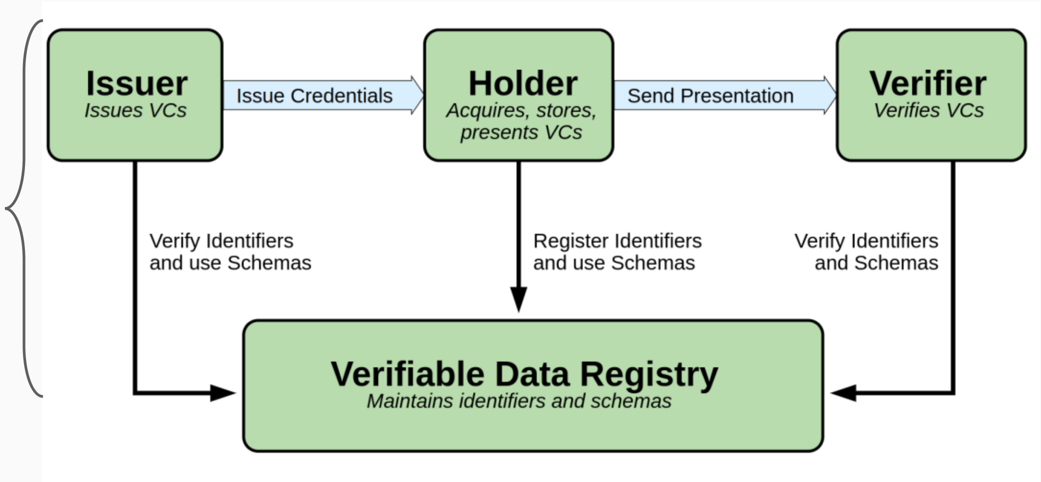
Scaled down Testbed

***SSI-based** Device Identity Management*



Each Device in Wind SCADA system needs Identity

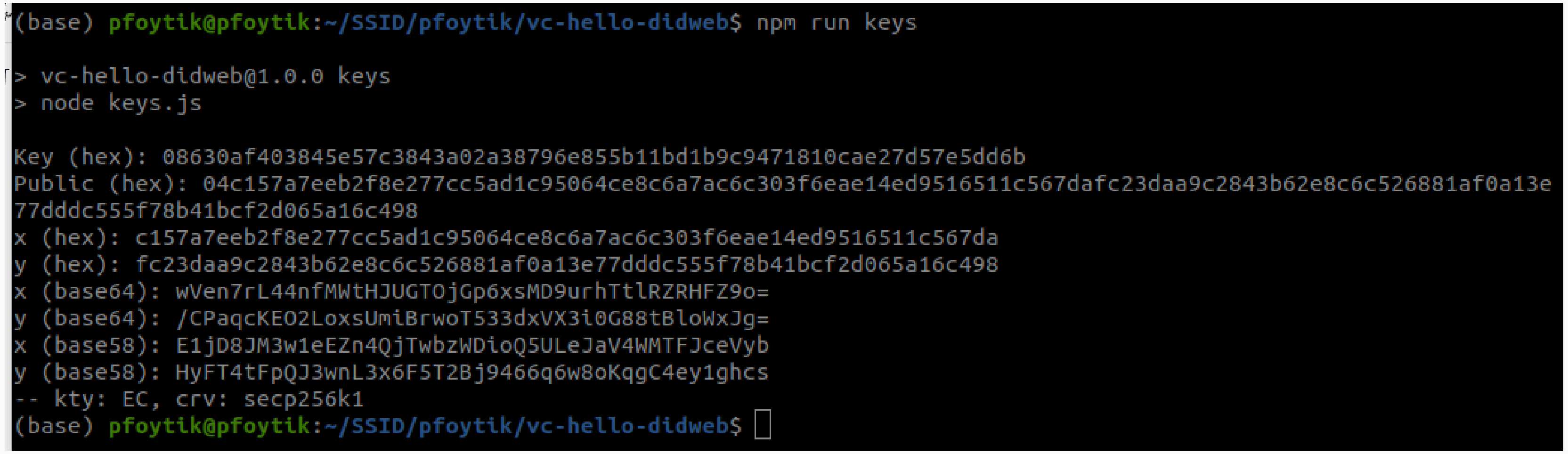
SSI-based identity management system



SSI-based Device Identity Management

Key Generation (Javascript)

- Javascript source code facilitates the creation of DID
- Public and Private keys are created and used
- Different formats available based on needs of system
- Using standard cryptographic libraries (secp256k1, elliptic curve cryptography)
- New Key is established for every relationship (stronger system if key becomes compromised)



```
(base) pfoytik@pfoytik:~/SSID/pfoytik/vc-hello-didweb$ npm run keys

> vc-hello-didweb@1.0.0 keys
> node keys.js

Key (hex): 08630af403845e57c3843a02a38796e855b11bd1b9c9471810cae27d57e5dd6b
Public (hex): 04c157a7eeb2f8e277cc5ad1c95064ce8c6a7ac6c303f6eae14ed9516511c567dafc23daa9c2843b62e8c6c526881af0a13e
77dddc555f78b41bcf2d065a16c498
x (hex): c157a7eeb2f8e277cc5ad1c95064ce8c6a7ac6c303f6eae14ed9516511c567da
y (hex): fc23daa9c2843b62e8c6c526881af0a13e77dddc555f78b41bcf2d065a16c498
x (base64): wVen7rL44nfMWtHJUGTOjGp6xsMD9urhTtlRZRHFZ9o=
y (base64): /CPaqcKEO2LoxsUmiBrwoT533dxVX3i0G88tBloWxJg=
x (base58): E1jD8JM3w1eEZn4QjTwbzWDioQ5ULeJaV4WMTFJceVyb
y (base58): HyFT4tFpQJ3wnL3x6F5T2Bj9466q6w8oKqgC4ey1ghcs
-- kty: EC, crv: secp256k1
(base) pfoytik@pfoytik:~/SSID/pfoytik/vc-hello-didweb$
```

SSI-based Device Identity Management

Signed Jason Web Token Data Structures

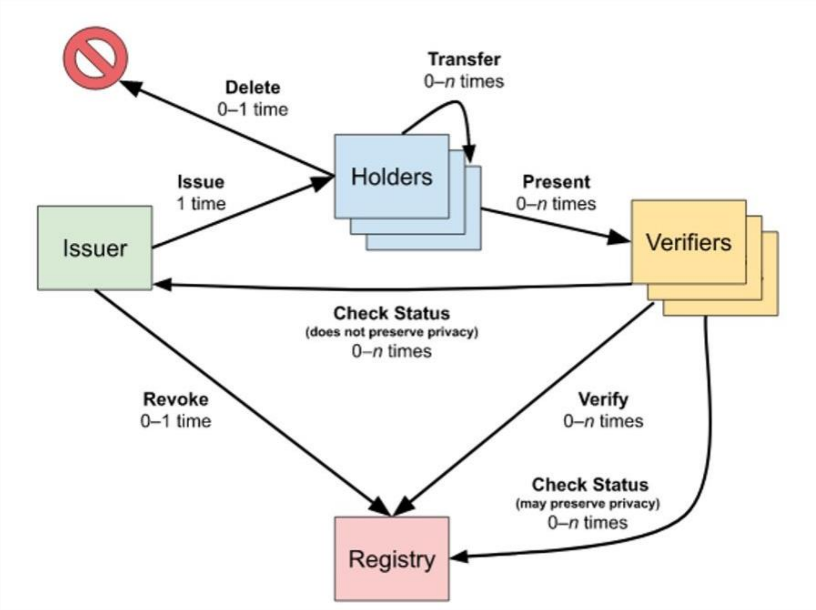
- Using DID an Jason Web Token standards (JWT)
  - Data can be signed
  - Encrypted or Plain text
- Provides means to prove ownership of data
- All credentialed data uses JWT to provide signed content by both the issuer and the owner


```
//// JWT:
eyJhbGciOiJFUzI1NksiLCJ0eXAiOiJKV1QifQ.eyJpYXQiOjE3MjgzMzI5NDcsImF1ZCI6ImRpZDp3ZWI6cGZveXRpay5naXRo
dWIuaW8iLCJuYW1lIjoiUGV0ZXIgRm95dGlrIiwiaXNzIjoiZGlkOndlYjpwZm95dGlrLmdpdGh1Yi5pbyJ9.Z7CiO-4_BgKJb0
3fKQ08bXcjMgKnlM3qpwF0prmcfdq_9rcdlwtmYKZg0wIg44AhUM8_BciSW69PXm-e9w8Vjw

//// JWT Decoded:
 {
  header: { alg: 'ES256K', typ: 'JWT' },
  payload: {
    iat: 1728332947,
    aud: 'did:web:pfoytik.github.io',
    name: 'Peter Foytik',
    iss: 'did:web:pfoytik.github.io'
  },
  signature: 'Z7CiO-4_BgKJb03fKQ08bXcjMgKnlM3qpwF0prmcfdq_9rcdlwtmYKZg0wIg44AhUM8_BciSW69PXm-e9w8Vj
w',
  data: 'eyJhbGciOiJFUzI1NksiLCJ0eXAiOiJKV1QifQ.eyJpYXQiOjE3MjgzMzI5NDcsImF1ZCI6ImRpZDp3ZWI6cGZveXR
pay5naXRodWIuaW8iLCJuYW1lIjoiUGV0ZXIgRm95dGlrIiwiaXNzIjoiZGlkOndlYjpwZm95dGlrLmdpdGh1Yi5pbyJ9'
}

//// Verified:
 {
  iat: 1728332947,
  aud: 'did:web:pfoytik.github.io',
  name: 'Peter Foytik',
  iss: 'did:web:pfoytik.github.io'
}
```

Credentialing: W3C Standard

- Issuer: identified with DID
- Holders: identified with DID
- Credential: specified by unique schema with proof of Issuer

- Registry just hold meta context of credential and encrypted code used by holder to prove



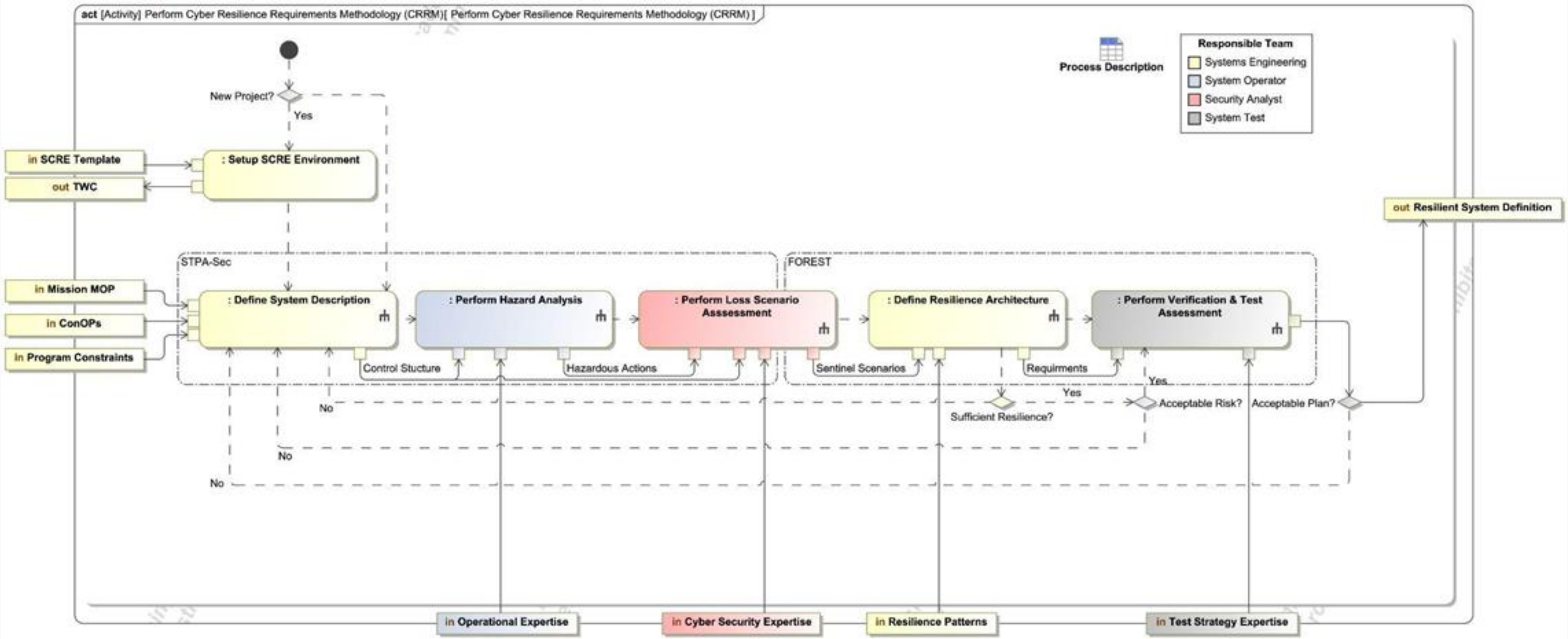
SSID Tools and Standard Bodies Examples using W3C

Example Code, New Development focused on TBD

- **Hyperledger INDY** – Uses public foundation controlled distributed ledger Hyperledger
  - https://www.hyperledger.org/use/hyperledger-indy
- **Ethereum Decentralized Identity** – Uses public foundation controlled distributed ledger Ethereum
  - https://ethereum.org/en/decentralized-identity/
- **Microsoft ION** – Uses public blockchain Bitcoin
  - https://identity.foundation/ion/
- **Synonym** – Uses gossip network hyperdrive
  - https://synonym.to/
- **TBD business at Block –** Uses public free open source code. Focuses on user specified registry source (web, ION, Ethereum, P2P)
  - https://tbd.website/
  - https://developer.tbd.website/projects/web5/
- **W3C** – Decentralized Identity and Verifiable Claims
  - https://www.w3.org/2020/12/did-wg-charter.html
- **Decentralized Identity Foundation**
  - https://identity.foundation/
- **Sovrin Foundation**
  - https://sovrin.org/
- **Ethereum Foundation**
  - https://ethereum.org/en/foundation/

Secure Cyber Resilient Engineering (SCRE)

Cyber Resilience Requirements Methodology



- CRRM is a means of identifying resilience requirements during the initial design phase of physical systems.
- The methodology involves five sequential steps, iteratively executed by one of four distinct teams representing stakeholders in the security engineering process.

Systems-Theoretic Process Assessment (STPA)

STPA is an iterative, methodical hazard analysis technique to identify causes of hazardous conditions intended to improve or promote system safety. Systems-Theoretic Accident Model and Processes (STAMP) is the core modeling framework.

- In cyber-physical systems, security can be treated as analogous to safety.

STPA Outputs and Traceability

Figure 2.21 shows the traceability that is maintained between various STPA outputs.

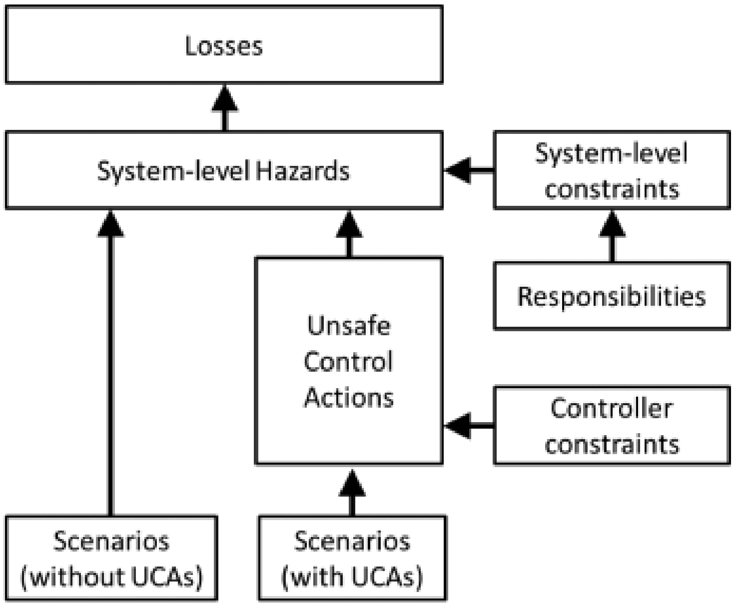


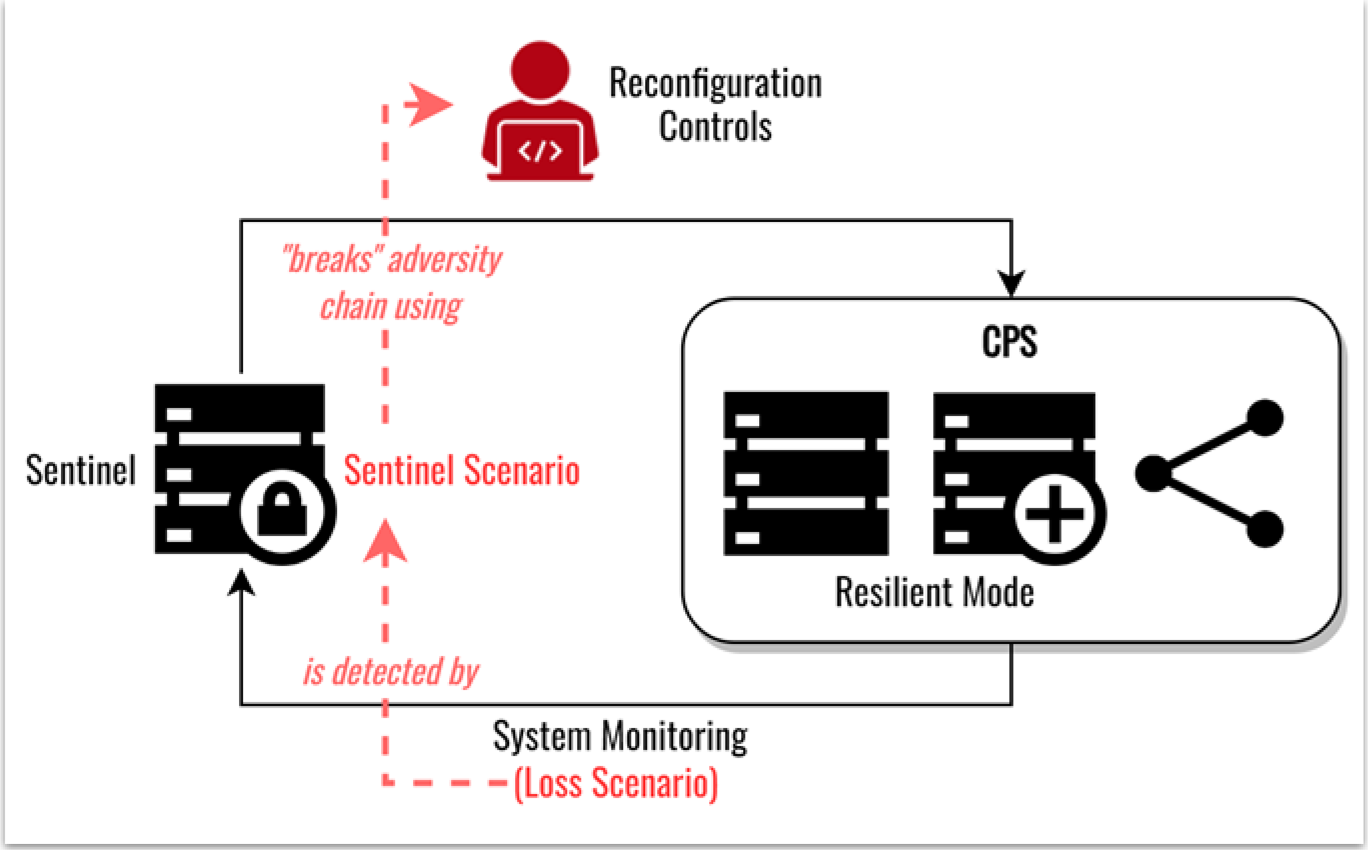
Figure 2.21: Traceability between STPA outputs

Leveson, Thomas https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

- A ***Loss*** involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.
- A ***Hazard*** is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.
- An ***Unsafe Control Action*** (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard.
- A ***Loss Scenario*** describes the causal factors that can lead to the unsafe control and to hazards.

Resilience Mechanism – Breaking Adversity Chain

Observe the System rather than the Adversary

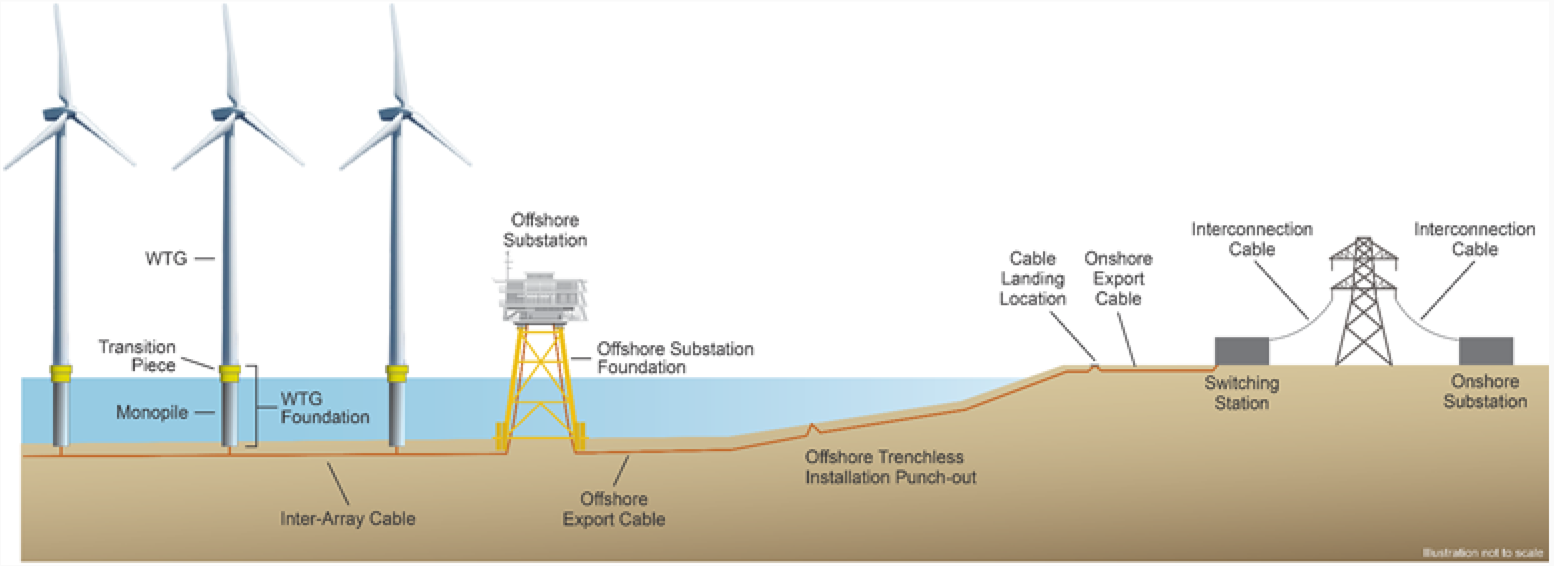


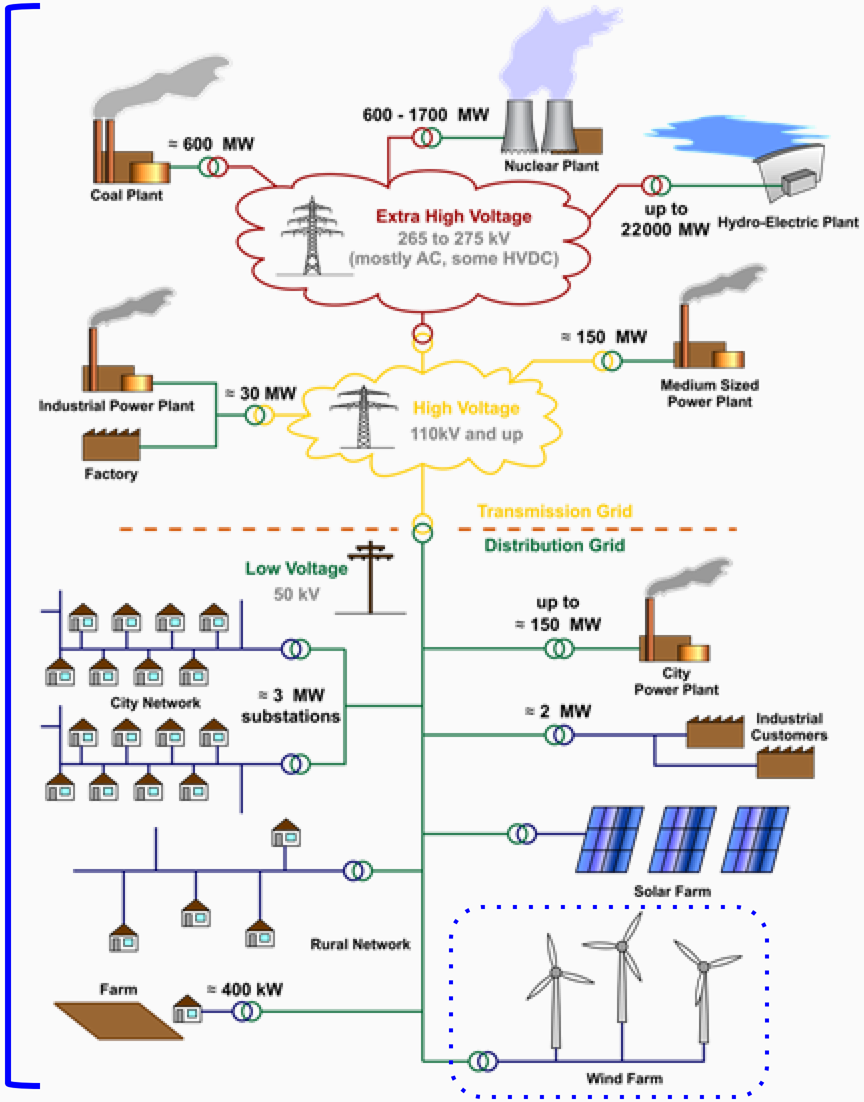
Can specify and test:
- Time to detect
- Characteristics of resilience modes
- Human-autonomy control roles
- Information / communications

SCRE Project Plan

SCRE Generic Modeling	SCRE Dominion Power Model	Domain Application for Method Improvement	LLM Co-Piloting for System Models	Co-Pilot for SCRE Modeling	Program Integration
SCADA MBSE Model	Dominion Specific System Model	Reference Architecture for OTA	Explore SysML tooling for usability	Develop Exemplar for Systems Theoretic Assistant	Coordination with Sponsor
Generic Windfarm Model	Specific Resilient Design	Tabletop Assessment for OSWF	Train model in SysML and Windfarm	MVP of STPA Assistant	Integration with ODU
SCRE Outreach		High Level Requirement Definition	Develop Capability Model	MVP for SCRE Assistant	
			Compare SysML models: human vs LLM		

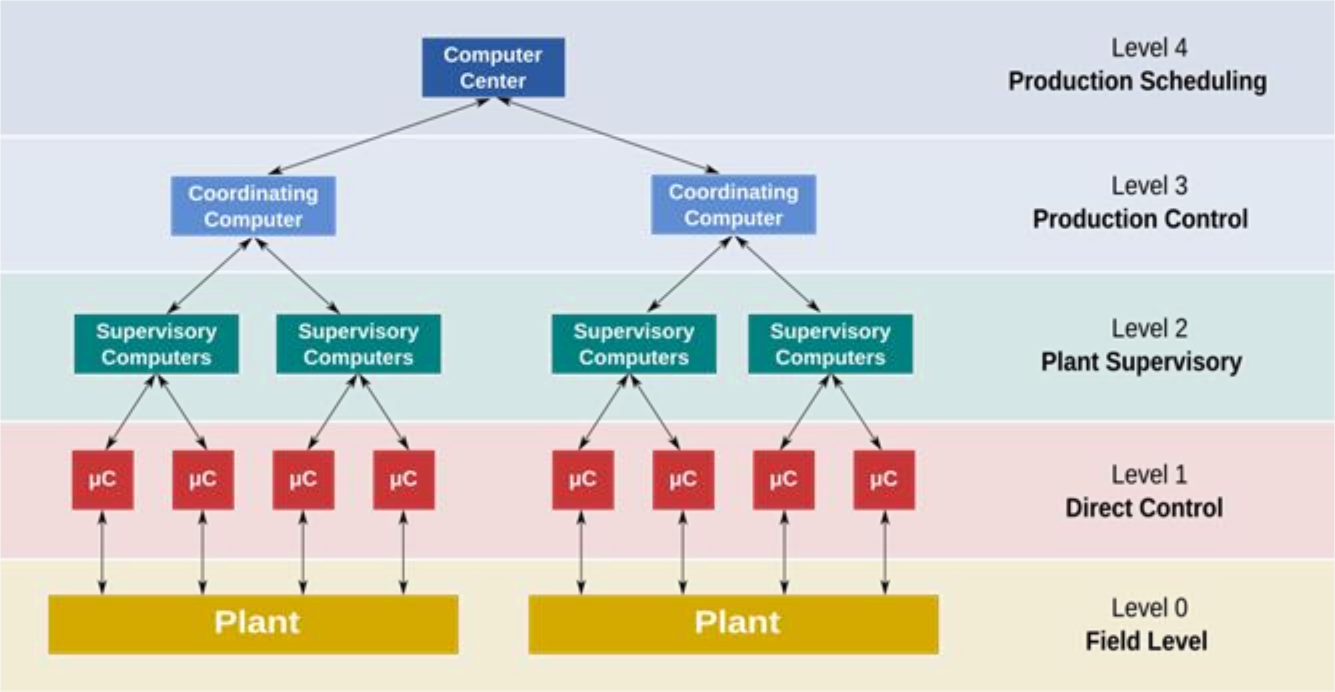
Wind Energy Farm - In Context of Energy Grid



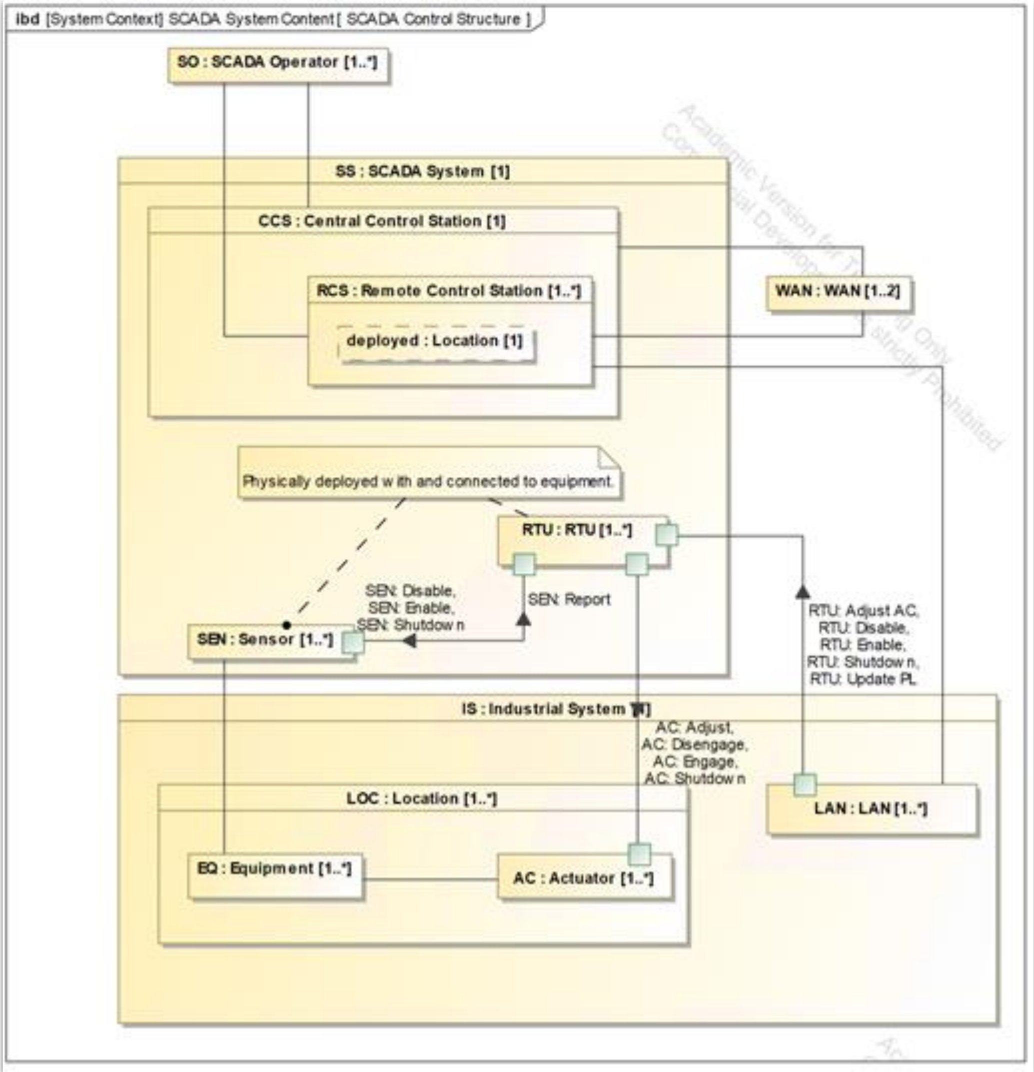


Coastal Virginia Offshore Wind (CVOW)

Wind Energy Farm as Industrial SCADA System



SCADA (supervisory control and data acquisition)



SCADA MBSE - Control Structure

SCADA Hazard Analysis (wip)

pkg [Package] Hazard Analysis [Hazard Analysis]

Table [Package] Losses [Losses]

#	Loss.id	Loss.title	Loss.priority	Hazard.isCausedBy.id	Hazard.isCausedBy.title
1	L.1	People injured or killed by industrial equipment.	1	H.1	Equipment operated out-of-specification.
2	L.2	Industrial equipment damaged.	3	H.1	Equipment operated out-of-specification.
3	L.3	Industrial process does not provide optimal revenue.	3	H.2	Equipment inadvertently taken off line.
4	L.4	Industrial equipment/process causes environmental damage.	2	H.3	Industrial 'content' inadvertently released.

Table [Package] Hazards [Hazards]

#	Hazard.id	Hazard.title	Loss.leadsTo.id	Loss.leadsTo.title
1	H.1	Equipment operated out-of-specification.	L.1	People injured or killed by industrial equipment.
			L.2	Industrial equipment damaged.
2	H.2	Equipment inadvertently taken off line.	L.3	Industrial process does not provide optimal revenue.
3	H.3	Industrial 'content' inadvertently released.	L.4	Industrial equipment/process causes environmental damage.

Hazard Analysis as SysML v2 (textual notation)

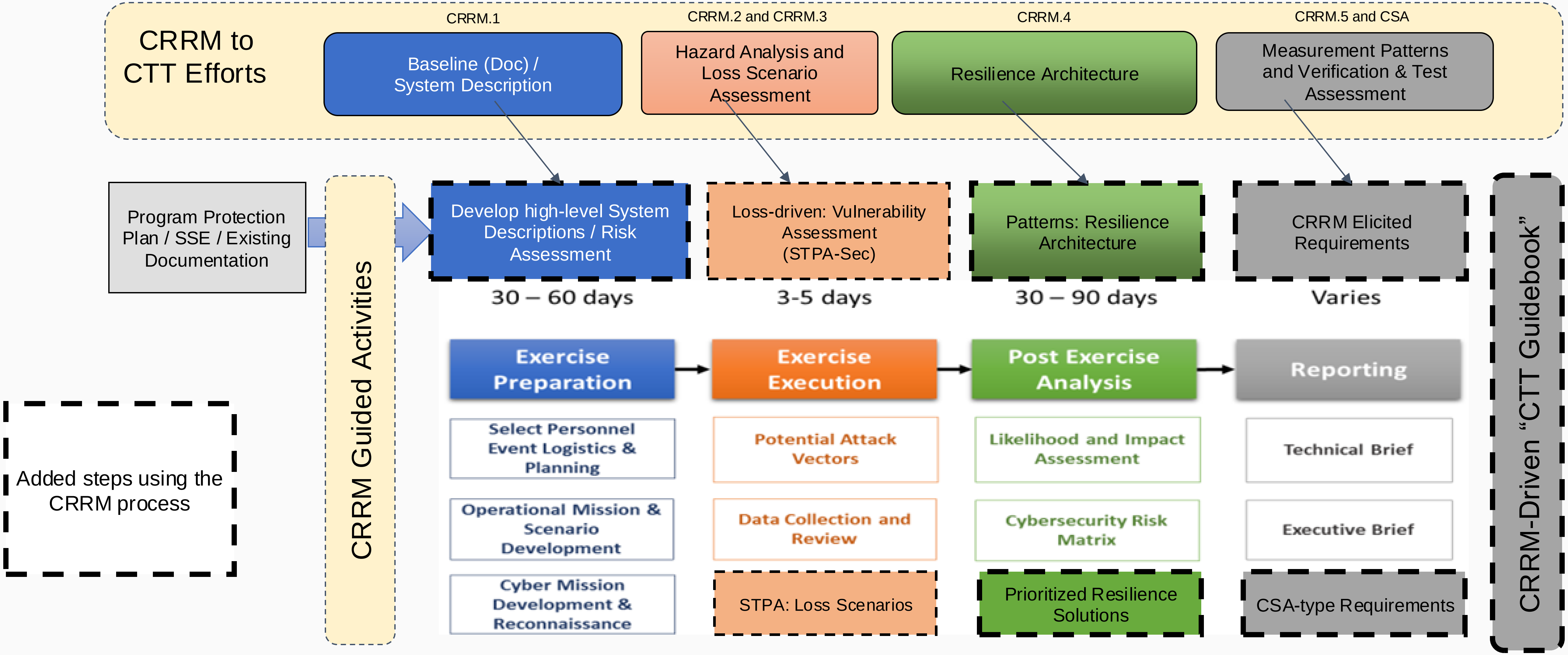
scre > sysmlv2 > stpa.sysml > STPA

```
library package STPA {
  doc /* Systems Theoretic Process Analysis */

  private import ScalarValues::*;

  item def Loss {
    doc
      /* A Loss involves something of value to stakeholders.
      * Losses may include a loss of human life or human injury,
      * property damage, environmental pollution, loss of mission,
      * loss of reputation, loss or leak of sensitive information,
      * or any other loss that is unacceptable to the stakeholders.
      */
    attribute priority: Integer;
    ref isCausedBy : Hazard[1..*];
  }

  item def Hazard {
    doc
      /* A hazard is a system state or set of conditions that,
      * together with a particular set of worst-case environmental
      * conditions (Environment State), will lead to a loss.
      */
    ref whenEnvironmentStateIs : SysML::StateUsage[1..*];
    ref isCausedBy : HazardousAction[1..*];
    ref leadsTo : Loss[1..*];
  }

  abstract item def ControlAction;
  abstract item def Feedback;

  enum def VariationType {
    doc /* Control Action: 'Variation Type' */
    enum NotProviding;
    enum Providing;
    enum OutOfSequence;
  }
```

scada > sysmlv2 > scada-ha.sysml > SCADA_HA

```
package SCADA_HA {
  doc /* SCADA Hazard Analysis */
  import STPA::*;

  package <'LO'> Losses {
    item <'L.1'> injury : Loss {
      doc /* People injured or killed by industrial equipment. */
      attribute :>> priority = 1;
      ref :>> isCausedBy = (HZ::'H.1');
    }
    item <'L.2'> damage : Loss {
      doc /* Industrial equipment damaged. */
      attribute :>> priority = 2;
      ref :>> isCausedBy = (HZ::'H.1');
    }
    item <'L.3'> revenue : Loss {
      doc /* Industrial process does not provide optimal revenue. */
      attribute :>> priority = 2;
      ref :>> isCausedBy = (HZ::'H.2');
    }
    item <'L.4'> environment : Loss {
      doc /* Industrial equipment/process causes environmental damage. */
      attribute :>> priority = 3;
      ref :>> isCausedBy = (HZ::'H.3');
    }
  }

  package <'HZ'> Hazards {
    item <'H.1'> outOfspec : Hazard {
      doc /* Equipment operated out-of-specification. */
      ref :>> leadsTo = (LO::'L.1', LO::'L.2');
    }
    item <'H.2'> offLine : Hazard {
      doc /* Equipment inadvertently taken off line. */
      ref :>> leadsTo = (LO::'L.3');
    }
    item <'H.3'> release : Hazard {
      doc /* Industrial 'content' inadvertently released */
      ref :>> leadsTo = (LO::'L.4');
    }
  }
```

Resilience-Focused Cyber Table-Top – Process Flow



CTT Process flow steps from Fig. 2, DAU Cyber Table-Top Guide

LLMs for Modeling Cyber Resilience of Offshore Wind Farms

Faculty Mentors: Ms. Mary Nerayo (mnerayo@vt.edu), Dr. Paul Wach (paulw86@vt.edu), Dr. Peter Beling (beling@vt.edu)

Project Description

Sponsor: Office of the Undersecretary of Defense for Research & Engineering (OUSD R&E).
Concern: The increasing cybersecurity risk to offshore Wind Energy Farm (WEFs) and other distributed energy production systems.
Desire: Seek new methods for understanding how these systems can be made resilient to cyber-attack.
Overall Objective: Explore the use of LLMs to model complex systems in an effort to aid cyber-resilient engineering and digital engineering solutions.

Offshore Wind Farm

Project Objectives/Deliverables

1. Specialize (e.g., finetune) LLMs to become an **expert on wind farms**.
2. Automate transformation of legacy documents (**text**) to **MBSE models**, and vice versa.
3. Specialize (e.g., finetune) LLMs to aid in create **cyber-physical resilience** MBSE models.
4. **Report on utility** of LLMs in the context of modeling and analyzing cyber resilience of WEFs or other distributed energy production systems.

Student Learning Objectives

- Learn principles of cyber resilience.
- Learn cutting edge LLM applications and methods.
- Learn model-based systems engineering (MBSE) and principles of systems modeling.
- Learn digital engineering concepts and methods.

GOALS

Objective:

Explore the use of **LLMs** to **model complex systems** in an effort to aid **cyber-resilient engineering** and **digital transformation**.

1. Train LLM to become an **expert on wind farms**.

2. Automate transformation of legacy documents (**text**) to **MBSE models.**

3. Automate transformation of **MBSE models** to descriptive **text**.

4. Train LLM to aid in creating **cyber-physical resilient** MBSE models.

5. Report on **utility** of LLM in the context of modeling and analyzing the cyber resilience of WEFs or other distributed energy production systems.

Project Team

Name	Organization	Labor Category	Contact
Tom McDermott	Stevens Institute of Technology	Principal Investigator (PI)	tmcdermo@stevens.edu
Dr. Sachin Shetty	Old Dominion University	PI	sshetty@odu.edu
Dr. Peter Beling	Virginia Tech	PI	beling@vt.edu
Dr. Safdar Bouk	Old Dominion University	Research Faculty	sbouk@odu.edu
Dr. Masud Rana	Old Dominion University	Research Faculty	mrana@odu.edu
Dr. Peter Foytik	Old Dominion University	Research Faculty	pfoytik@odu.edu
Jerry Cronin	Old Dominion University	Researcher	jcronin@odu.edu
Soumya Banerjee	Old Dominion University	Post-Doc	S1banerj@odu.edu
Graduate Research Students	Old Dominion University	GRA	TBA
Dr. Stephen Adams	Virginia Tech	Research Faculty	scadams21@vt.edu
Dr. Kelli Esser	Virginia Tech	Researcher	kesser@vt.edu
Dr. Paul Wach	Virginia Tech	Researcher	
Tim Sherburne	Virginia Tech	Researcher	sherburne@vt.edu
Geoff Kerr	Virginia Tech	Researcher	geoffreykerr@vt.edu
Megan Clifford	Stevens Institute of Technology	Researcher	mcliffor@stevens.edu

SYSTEMS ENGINEERING RESEARCH CENTER

Thank you!

Stay connected with SERC Online: