LA-UR-22-22768

Approved for public release; distribution is unlimited.

Title:	Framework for Evaluating Cyberthreats targeted at Cyber-Physical Energy Systems (CPES): From Threat Modeling to Co-simulation Case Studies.
Author(s):	Ospina Casas, Juan Jose
Intended for:	Invited Talk for IEEE Power Electronics Society (PELS) Technical Committee on Design Methodologies (TC 10).
Issued:	2022-03-25 (Draft)

Framework for Evaluating Cyberthreats targeted at Cyber-Physical Energy Systems (CPES): From Threat Modeling to Co-simulation Case Studies.

Juan Ospina, *Ph.D*.

Postdoctoral Researcher with the A-1 Information Systems and Modeling group at Los Alamos National Laboratory

April 7, 2022

IEEE PELS Technical Committee on Design Methodologies (TC 10)

LA-UR: XXXXXXXXXX

Outline

- Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)
- Cyber-Physical Energy Systems (CPES) Testing Framework
- Co-Simulation of Cyber-Physical Energy Systems (CPES)

Outline

- Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)
- Cyber-Physical Energy Systems (CPES) Testing Framework
- Co-Simulation of Cyber-Physical Energy Systems (CPES)

Introduction to Cybersecurity in Electric Power Systems: Terminology

Threats: Set of circumstances that has the potential to cause loss or harm.

- *interception*, or unauthorized viewing (confidentiality)
- *modification*, or unauthorized change (integrity failures)
- *fabrication*, or unauthorized creation (integrity failures)
- *interruption*, or preventing authorized access (accessibility)

Vulnerability: A weakness in the system.

Attack: Exploiting a vulnerability; by person or computer system.

Control: A protective measure.

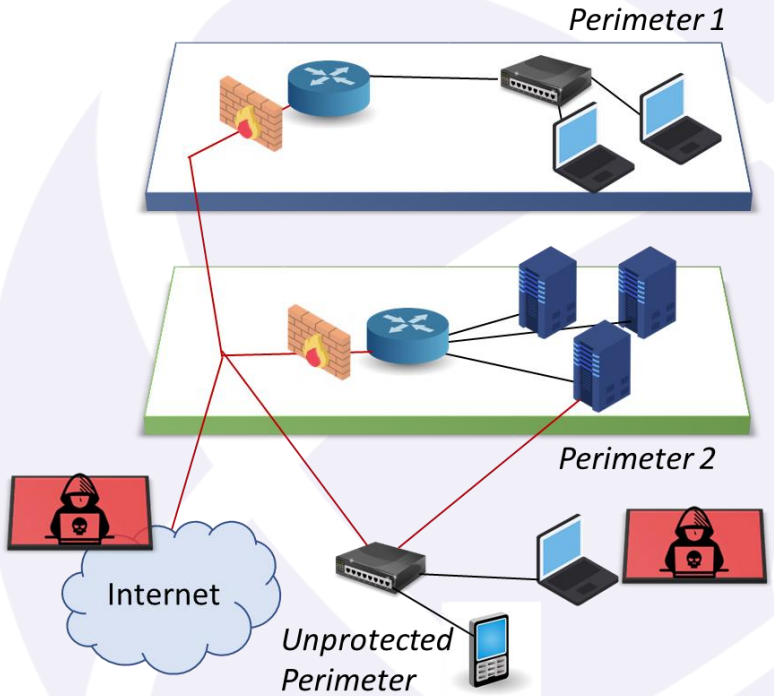
- A technique that removes or reduces a vulnerability

A *threat* is blocked by *control* of a *vulnerability*.

Introduction to Cybersecurity in Electric Power Systems: Networks

What could make a network vulnerable?

- **Anonymity** (An attacker can attempt many attacks, anonymously, from thousands of miles away)
- **Large networks** mean **many points of potential entry** (Many points of attack)
- **Sharing** (Share resources may expose vulnerabilities)
- **Network complexity** (Hard to protect diverse systems with different OS, vulnerabilities)
- **Unknown perimeter** (Complex networks change all the time so may open up potential access vulnerabilities)
- **Unknown path** (There may be many paths, including untrustworthy ones, from one host to another)



Introduction to Cybersecurity in Electric Power Systems: Security Goals & Threats to the Triad

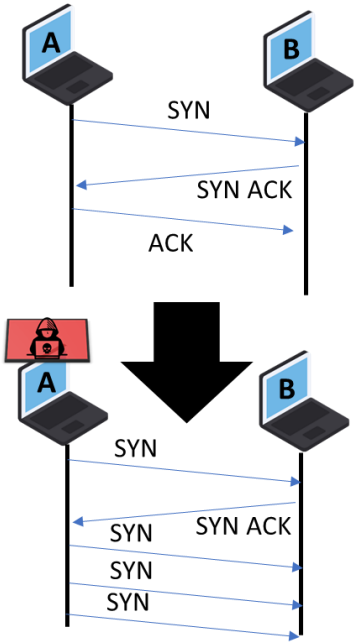
CIA (Confidentiality, Integrity, Accessibility) Triad

- Confidentiality:
  - Only authorized people or computers can access the data.
  - Known as in networking community as Wiretapping (even if no physical wire involved)
- Integrity:
  - The data can only be modified by authorized people or computers.
  - Known as in networking community as Data Corruption
- Accessibility:
  - The data is accessible to authorized people or computer when they need it.
  - Related to attacks such as Denial of Service (DoS)

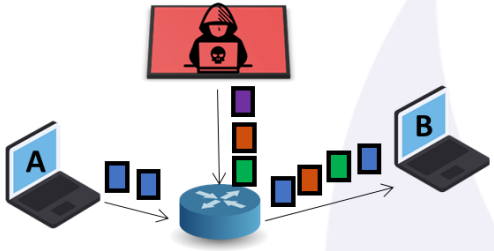
A successful attack violates one or more of these goals.

Introduction to Cybersecurity in Electric Power Systems: Example Cyberattacks

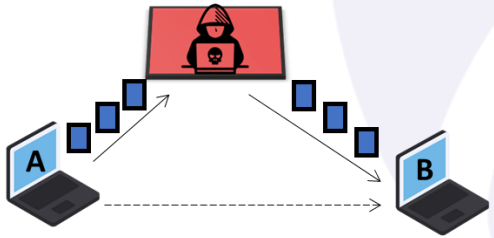
TCP SYN Flooding Attack



IP Spoofing

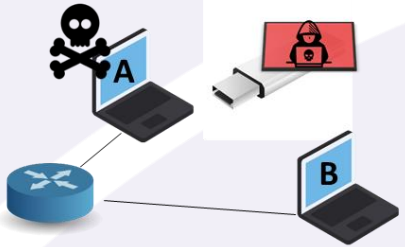


Replay (MiTM)

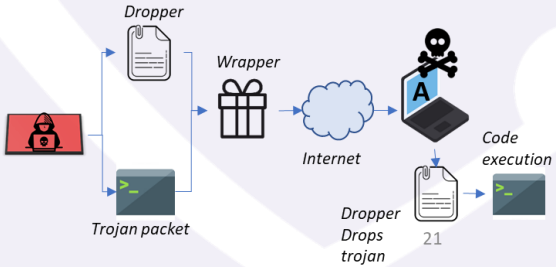


Malware/Rootkits

(Could be Insider threats)



Trojans



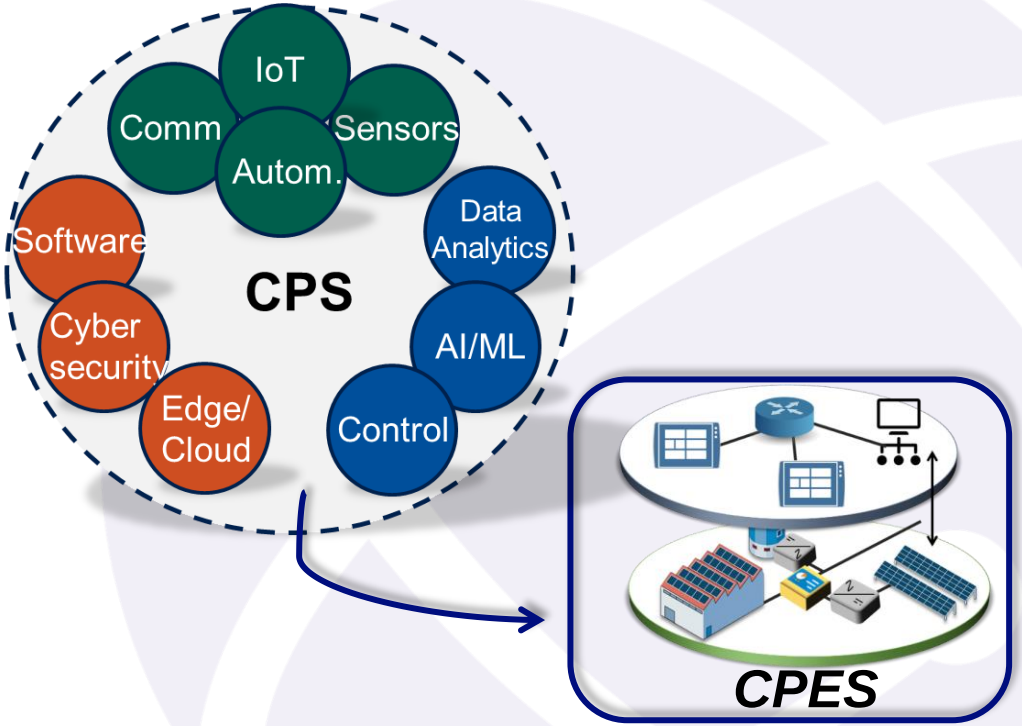
Introduction to Cyber-Physical Energy Systems (CPES): Background and Motivation

- The **modernization** and **decentralization** of electric power systems (EPS) are being facilitated by:
  - integration of distributed energy resources (DERs)
  - wide-scale deployment of information and communication technologies (ICTs).

- This modernization from EPS to CPES have disadvantages:
  - CPES are becoming more challenging to secure due to incorporation of ICT devices
  - ICT devices introduce cyber vulnerabilities to physical systems
  - ICT devices create new attack vectors not considered in traditional power systems

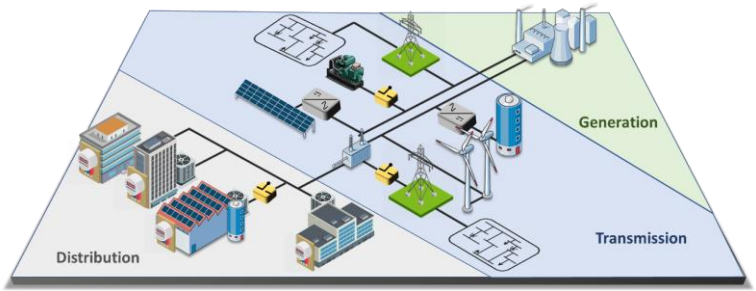
Introduction to Cyber-Physical Energy Systems (CPES)

- **Modern Electric Power Systems (EPS) integrate:**
  - intelligent controllers
  - real-time measurement devices
  - distributed energy resources (DER)
- **Improve:**
  - Security
  - Efficiency
  - Stability
  - Reliability
- **Cyber-Physical Energy Systems (CPES) integrate:**
  - integrate information and communication technologies (ICT)
  - operational technology (OT) and physical devices.

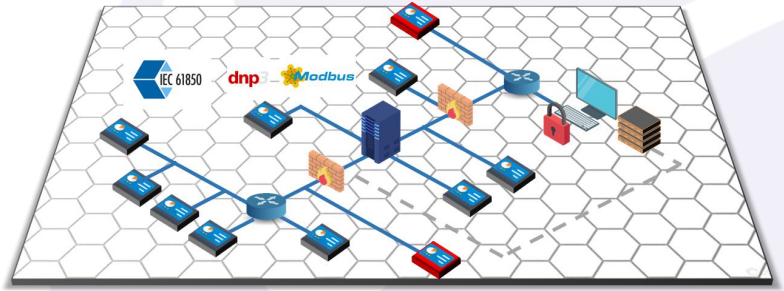


Introduction to Cyber-Physical Energy Systems (CPES)

***CPES** are energy-focused engineered systems that are transforming the way traditional EPS operate.*



Physical



Cyber

- **Cyber:** computation, communication, and control that are discrete, logical, and switched.
- **Physical:** natural and human-made systems governed by the laws of physics and operating continuously.

Introduction to Cyber-Physical Energy Systems (CPES): Physical

- Physical-system layer of a CPS is composed of ***hardware components*** embedded into the system environment.

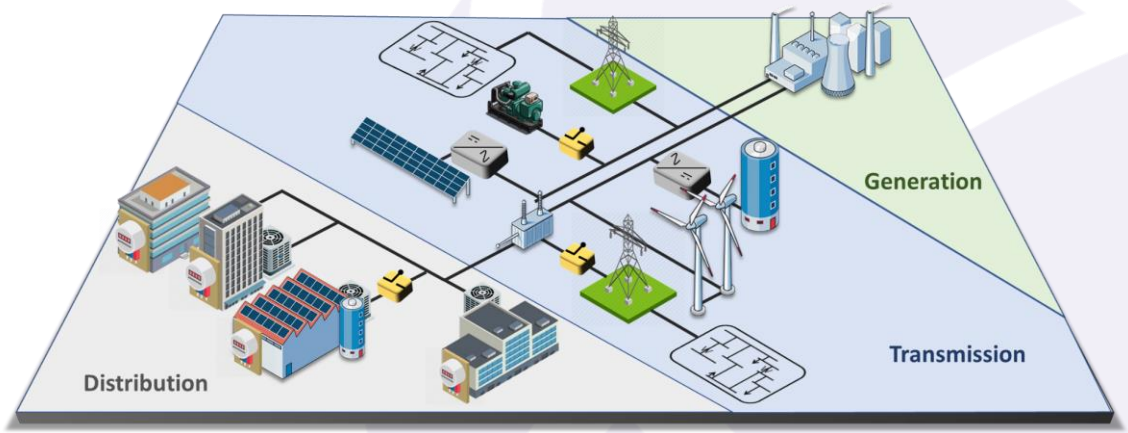
- **Components interact through:**
  - physical means (i.e., sensors and actuators)
  - ***cyber-system layer*** using standard communication protocols

- **Sectors where CPS exist:**
  - Smart Manufacturing
  - Healthcare
  - Robotics
  - Transportation
  - **Electric Power Systems (EPS)**

Introduction to Cyber-Physical Energy Systems (CPES): Physical

- **Physical Divisions of EPS**
  1. Generation
  2. Transmission
  3. Distribution

- **Example Components:**
  - PV Panels
  - Li-ion batteries
  - Wind energy systems
  - Generators
  - Power converters
  - Transformers
  - Voltage regulators
  - Lines
  - Measurement devices



Introduction to Cyber-Physical Energy Systems (CPES): Cyber

- Cyber-system layer of a CPS is composed of ***hardware and software components*** embedded into the **Information Technology (IT)** environment**.**

- Allows the interconnection of multiple computing devices using common ***communication protocols over digital links.***

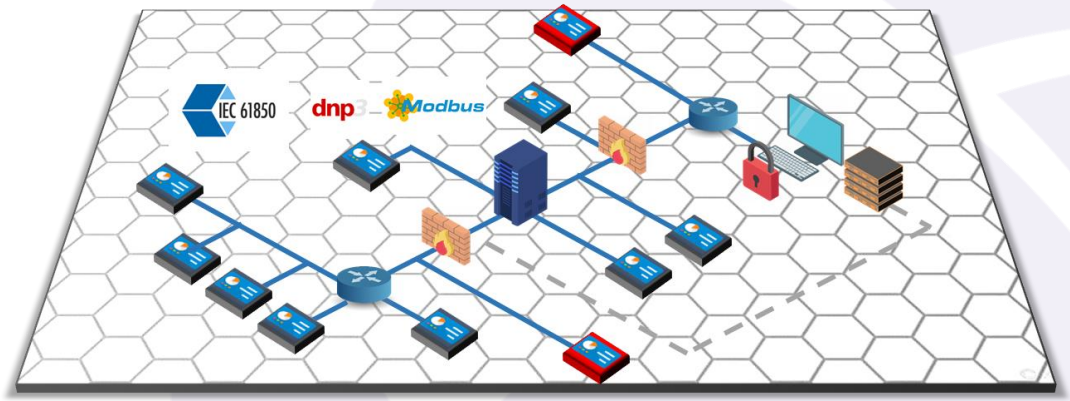
- Allows sharing resources and data located across networking nodes.

- ***In a real-world CPS*** (e.g., cellular networks, military zones, or SCADA systems), the number of networking components layer can be **immense**.

Introduction to Cyber-Physical Energy Systems (CPES): Cyber

- **Cyber Divisions of EPS:**
  - Local Area Networks (LAN).
  - Wide Area Network (WAN)
  - Neighborhood Area Network (NAN)
  - Municipal Area Network (MAN)

- **Example Components:**
  - Hubs
  - Modems
  - Routers
  - Cables
  - Network interface cards (NICs)
  - HMIs
  - Databases



Example Communication Protocols for EPS:

- IEC 61850
- DNP3
- Modbus

Introduction to Cyber-Physical Energy Systems (CPES): Past Cyber Incidents

- **BlackEnergy Malware** (DDoS toolkit)
- **CrashOverride Malware**
  - Automated
  - Control manipulation
  - Denial of control
  - Data wiping
- **Triton**
  - Disable safety instrumented systems in industrial plants
- **2015 Ukraine cyber-attack**
  - Adversaries tripped circuit breakers
  - Caused blackout affecting almost 225,000 customers

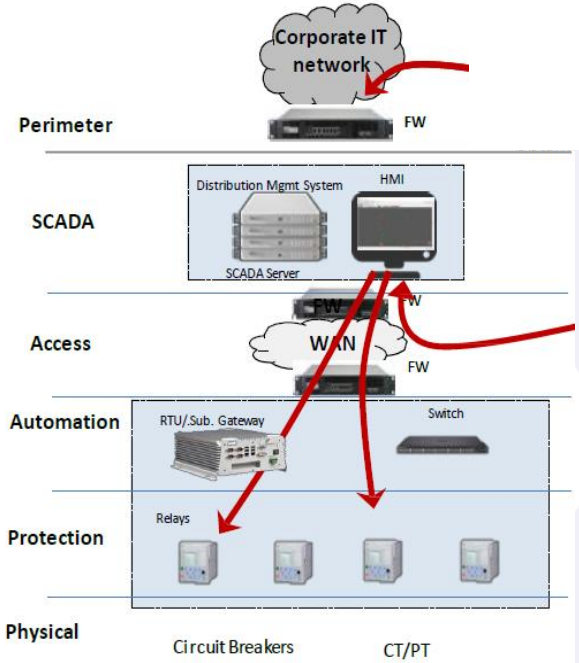
Introduction to Cyber-Physical Energy Systems (CPES): 2015 Ukraine Incident

Attack Description & Impacts:

- Coordinated cyber attack to 3 distribution (electric) companies (around 30 substations)
- 225k customers suffered outages
- Blackouts in multiple regions throughout the country

Attack Path:

1. Spear phishing
2. Stolen VPN credentials
3. VPN login
4. Open breakers in the system



Ack: Adam Hahn, Washington State University

IT	OT Pre-Impact	OT Post-Impact
1. Phishing email to IT network		
2. Privilege escalation	3. OT VPN login from stolen credentials	
	4. Install malware (BlackEnergy)	
	5. Unauthorized remote HMI session access to SCADA	
	6. Trip the Breakers (Blackout)	7. Disable systems, wipe info., brick controllers
		8. Telephone DDOS preventing customers to inform.

Difficulties and Complexities in Modeling and Testing CPES

There are many **difficulties** and **complexities** that exist when modeling, simulating, and testing CPES. Some of them are:

- There are many standards, many system modeling techniques, many threats modeling techniques, etc. So, starting can be overwhelming.

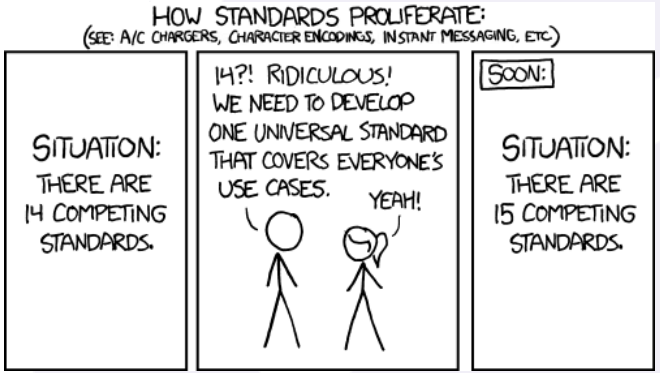
- Due to high number of devices, testing and evaluation of CPES is becoming a very complex task.
  - Many interconnected devices (physical, cyber)
  - Possible damage to real equipment
  - Degradation of service due to testing procedures

- Testing platforms may be unrealistic (e.g., have many non-obvious non-realistic assumptions)*.
  - *Real-time Co-Simulation Testbeds help alleviating these problems providing a real-time environment for testing.

Difficulties and Complexities in Modeling and Testing CPES

- This presentation is **not intended** to present a new standard.

- Its main objective is to provide an **example framework** on how to perform:
  - Threat modeling for threats targeted at CPES
  - Modeling & testing of CPES.



https://xkcd.com/927/

Outline

- Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)
- Cyber-Physical Energy Systems (CPES) Testing Framework
- Co-Simulation of Cyber-Physical Energy Systems (CPES)

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)

- The **threat model is:**
  - **Designed to** elucidate assumptions made for adversary:
    - Intentions
    - Capabilities (Resources)
    - Possible Attack Details (Accessibility, Specificity, Frequency of attack, Assets compromised, Technique)
  - A procedure designed to **discover potential vulnerabilities**.
  - A **critical procedure** to follow when **designing security defenses** and **mitigation strategies**.

- **Examples**:
  - STRIDE
  - DREAD
  - OCTAVE Allegro
  - MITRE ATT&CK for ICS

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)

STRIDE

Framework that model threats to ensure secure application design.

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

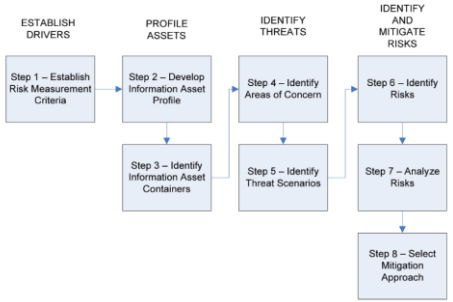
DREAD

- **D**amage – how bad would an attack be?
- **R**eproducibility – how easy is it to reproduce the attack?
- **E**xploitability – how much work is it to launch the attack?
- **A**ffected users – how many people will be impacted?
- **D**iscoverability – how easy is it to discover the threat?

OCTAVE Allegro

Focuses on information assets:

- *how they are used*
- *where they are stored, transported, and processed*
- *how they are exposed to threats, vulnerabilities, and disruptions.*



MITRE ATT&CK for ICS

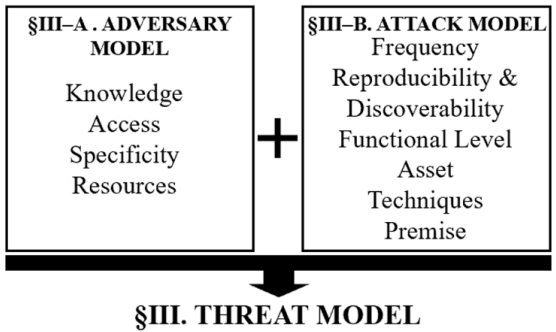
MITRE ATT&CK for ICS

Adversary Access	Attack Level Attacked Asset
Adversary Specificity	Attack Techniques

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)

- As seen, there is no '*threat model*' that can directly be used for CP(E)S while capturing all necessary components designed to describe the ***Adversary*** and the ***Attack***.
- To address this, we developed our **own threat modeling methodology** based on the other threat models researched.
- The proposed threat model is based on **two** components:
  - *Adversary model*
  - *Attack model*



Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES): Adversary Model

Adversary Model:

- Adversary Knowledge:
  - Strong-knowledge adversary (white-box)
  - Limited-knowledge adversary (gray-box)
  - Oblivious-knowledge adversary (black-box)
- Adversary Access:
  - Possession
  - Non-possession
- Adversarial Specificity
  - Targeted attacks
  - Non-targeted attacks
- Adversarial Resources
  - Class I – do not have sufficient resources to perform attack without being detected.
  - Class II – possess sufficient resources to perform sophisticated (undetected) attacks.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES): Attack Model

Attack Model:

- Attack Frequency:
  - Iterative (attack needs multiple iterations)
  - Non-iterative (attack only needs to be realized once)
- Attack Reproducibility & Discoverability:
  - One-time attack (detected after first attempt)
  - Multiple-times attack (detected only after multiple attempts)
- Attack Functional Level:
  - Level 0 (attack targeted to sensors, actuators, etc.)
  - Level 1 (attack targeted at network devices/controllers)
  - Level 2 (attack targeted at workstations, data historians, etc.)
- Attacked Asset
  - RTUs, servers, safety equipment, workstations, HMIs.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES): Attack Model

Attack Model:

- Attack Techniques:
  - Control logic modification
  - Asset compromise (e.g., workstation, wireless)
  - Denial-of-Service (DoS)
  - Man-in-the-Middle (MitM)
  - Spoofing
  - Firmware attack
  - Rootkits
- Attack Premise:
  - Cyber-domain (i.e., Confidentiality, Integrity, Availability)
  - Physical domain (i.e., invasive, semi-invasive, non-invasive)

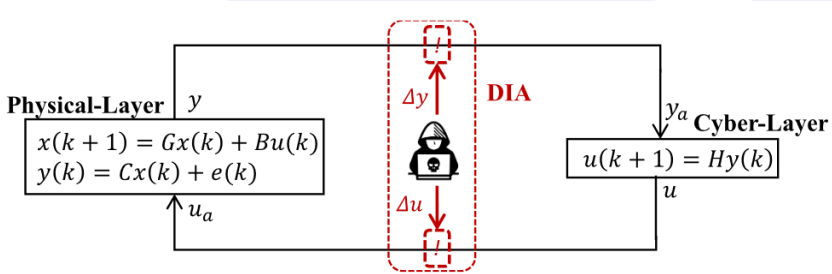
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES): Load-Changing/Altering (LCA) Attack Example

General Formulation:

- Let's consider a CPS plant

$$x(k+1) = Gx(k) + Bu(k)$$
$$y(k) = Cx(k) + e(k)$$
$$u(k+1) = Hy(k)$$



The LCA can be characterized as a data integrity attack (DIA) where either the:

- measurements (*y*) or
- controls (*u*)

could be compromised.

Ospina, J., Liu, X., Konstantinou, C., & Dvorkin, Y. (2020). On the feasibility of load-changing attacks in power systems during the covid-19 pandemic. IEEE Access, 9, 2545-2563.

Threat Modeling Framework for Cyber-Physical Energy Systems (CPES): Load-Changing/Altering Attack Example

In the LCA case, controls (*u*) represent the controls performed by IoT-controllable loads.

$$u_a = u + \Delta u$$

where u_a, represents the 'altered/attacked' control variables and Δu, represents the variations injected by the adversary.

$$x_a(k+1) = Gx(k) + Bu_a(k)$$
$$y_a(k) = Cx_a(k+1) + e(k+1)$$

- The ***threat model*** of a botnet attack designed to compromise the power grid via LCAs can described as follows:

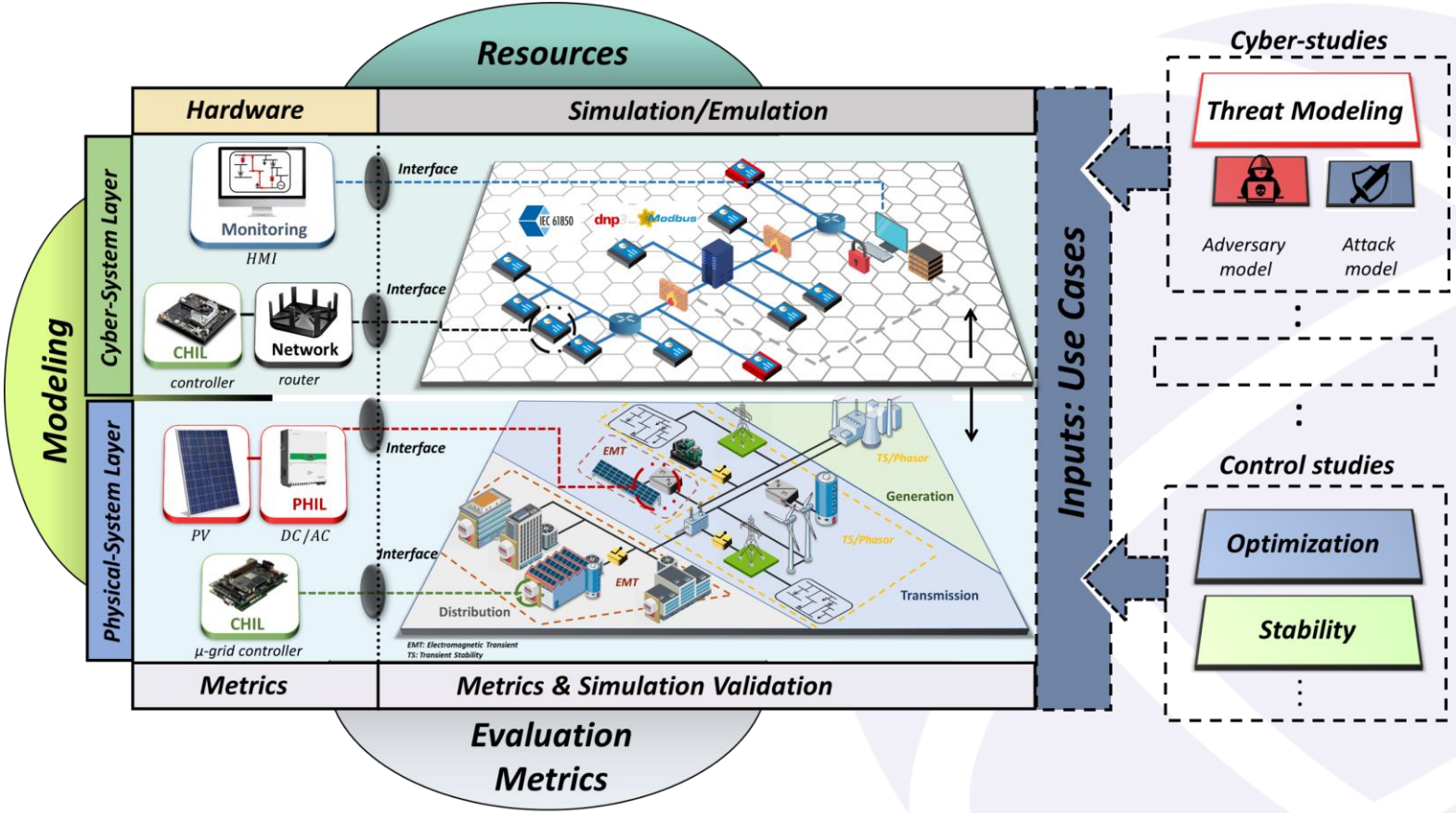
Threat Model \Threat	Load-changing Attack
Knowledge	Oblivious or Semi-Oblivious
Access	Non-possession
Specificity	Targeted
Resources	Class II
Frequency	Iterative
Reproducibility	Multiple-times
Level	L1 or L2
Asset	Smart HVAC, IoT-connected motors, PLCs, EV chargers, water heaters, etc.
Technique	Modify control logic or wireless compromise
Premise	Cyber: Integrity

Ospina, J., Liu, X., Konstantinou, C., & Dvorkin, Y. (2020). On the feasibility of load-changing attacks in power systems during the covid-19 pandemic. IEEE Access, 9, 2545-2563.

Outline

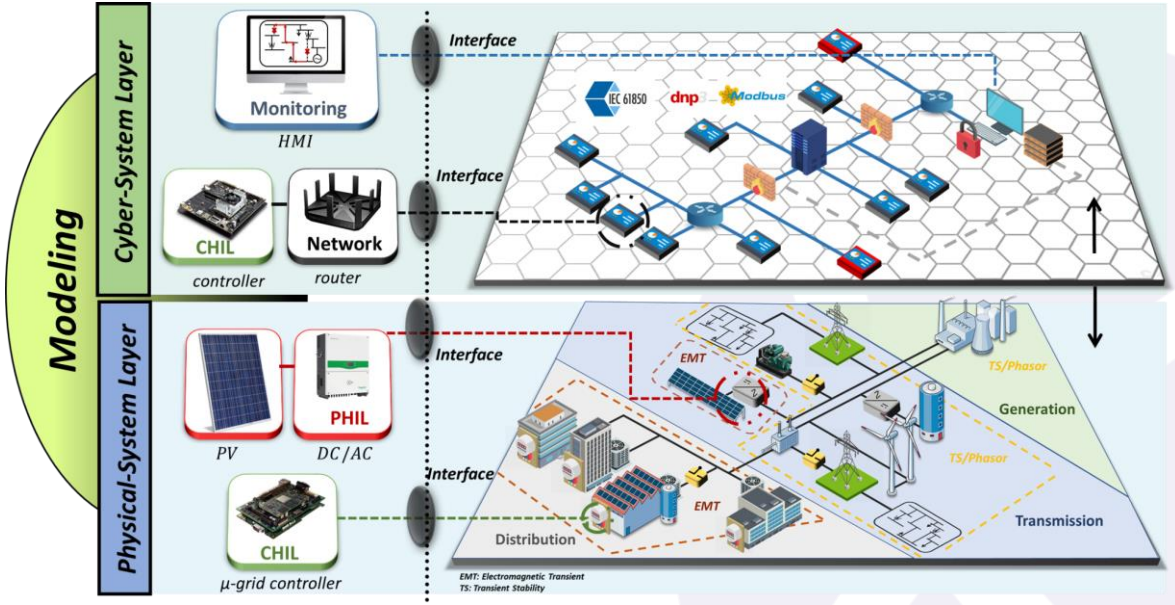
- Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)
- Cyber-Physical Energy Systems (CPES) Testing Framework
- Co-Simulation of Cyber-Physical Energy Systems (CPES)

Cyber-Physical Energy Systems (CPES) Testing Framework



Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Modeling



Models are built from mathematical equations and/or data that are used to explain and predict the behavior and response of complex systems.

* "*All models are wrong, but some are useful*". George E. P. Box.

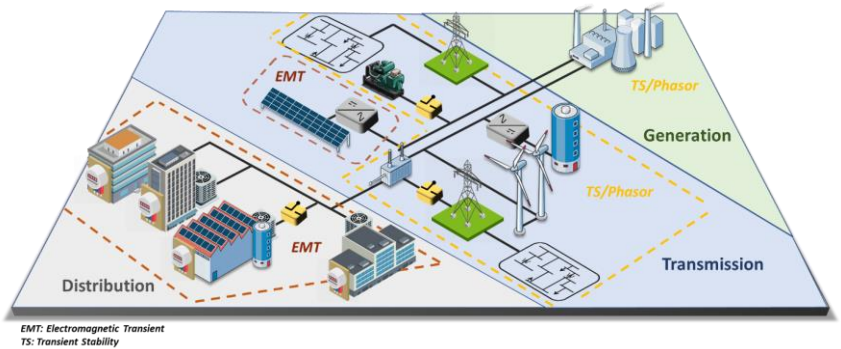
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Modeling - Physical-System Layer

Objective: capture and simulate physical system behavior so that the real system can be re-created.

- *This 'virtualization' capability allows the analysis and study of different types of scenarios which can arise during the operation of the CPS.*

- **EPS modeling simulation:**
  1. **Electromagnetic transient (EMT):** *fast dynamic events and system perturbations, that occur in the range of tens of microseconds or lower.*
  2. **Transient stability (TS) / Steady-State**: *slow dynamic events, i.e., events in the range of tens of milliseconds and higher /Snapshots.*
  3. **Hybrid (TS+EMT)**



- **EPS modeling hardware:**
  1. Controllers
  2. PV systems
  3. Converters
  4. ….

µ-grid controller

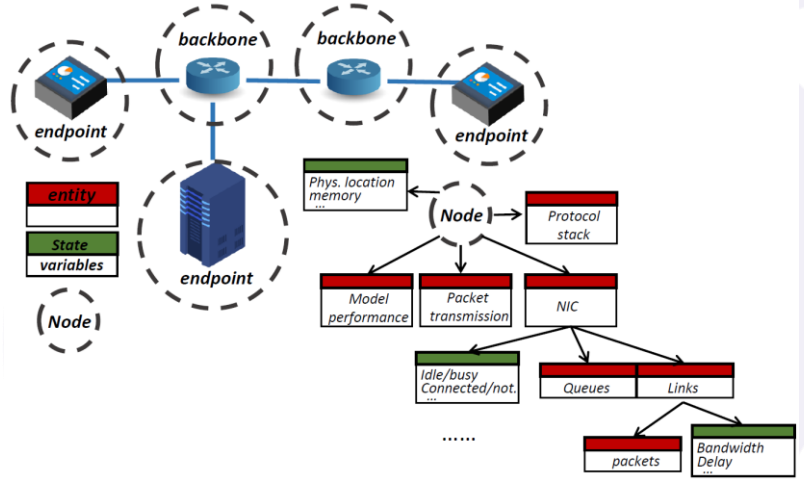
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Modeling - Cyber-System Layer

- **The design and modeling involve:**
  - Communication network modeling
  - Communication protocol implementation
  - Design of information systems
  - Data storage processing.

- **Characteristics to consider for modeling the communication networks:**
  1. Topology of the communication network
  2. Physical characteristics
  3. Quality-of-Service (QoS), etc.

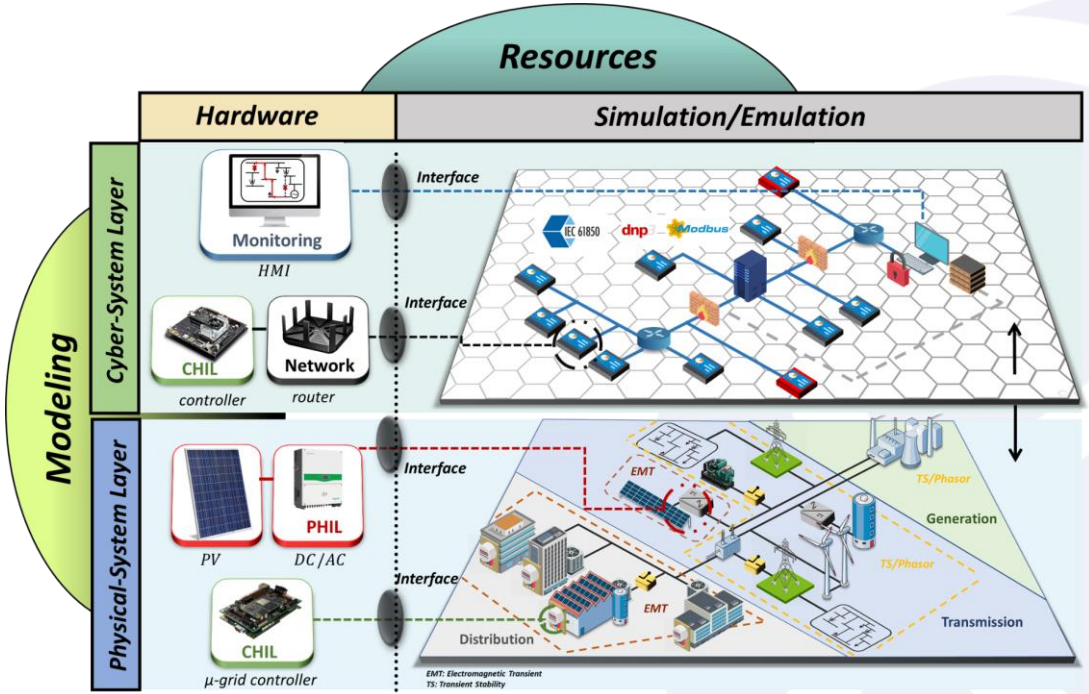
- **Network Modeling Process**
  - Network entities (nodes, links, queues, packets)
    - Nodes -> routers (backbone), switches, hubs, PCs (endpoint), RTUs, etc.
  - State variables: behavior of modeled nodes
    - Variables -> memory consumption, physical location, CPU utilization, etc.
  - **Discrete-event simulation**



Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

M. S. Obaidat, F. Zarai, and P. Nicopolitidis, Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications. San Mateo, CA, USA: Morgan Kaufmann, 2015.

Cyber-Physical Energy Systems (CPES) Testing Framework: Resources



The ***'resources'*** factor represents the different hardware and software systems used to model and simulate the cyber/physical-system layers of the CPES.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Resources - Physical-System Layer

Simulation:

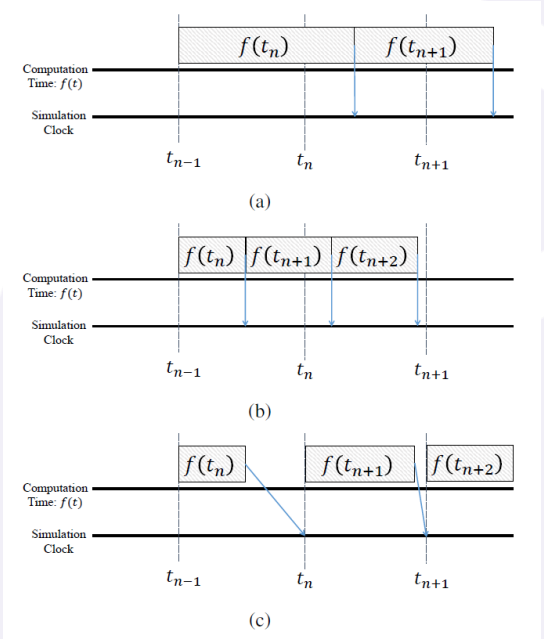
- Offline Simulation *(slower or faster than real-time)*
- Real-time simulation

Hardware:

- Controller HIL (CHIL)
- Power HIL (PHIL)

Tools:

- **Offline**
  - OpenDSS
  - MATLAB/Simscape Electrical
  - Gridlab-D
  - PowerModels.jl & PowerModelsDistribution.jl
- **Real-time**
  - eMegaSim
  - ePhasorSim
  - ETAP eMTP



Offline vs. Real-time simulation

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Resources - Cyber-System Layer

Network simulation/emulation tools use **discrete-event simulation**

Discrete-event driven simulators include:

- The simulation time variable
- A list of pending future events.

Simulation/Emulation:

- **Simulation**
  - Simulation models are designed to replicate the behavior of the system.
- **Emulation:**
  - Emulation models are designed to duplicate the behavior of the system.

***simulation** can **be adapted for emulation** purposes by adding real-time synchronization.*

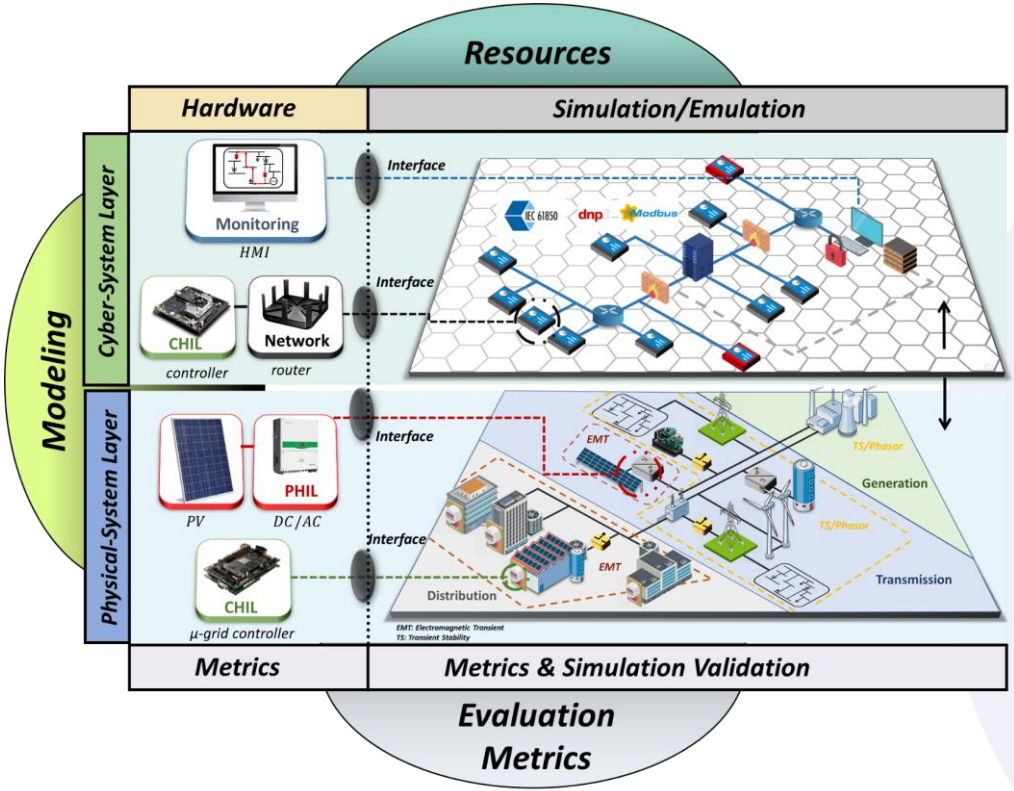
Hardware

- Controller (CHIL)

Tools	
Simulation	**Emulation**
ns-2	CORE
ns-3	NetEm
SimPy	EXata

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Metrics



- A multitude of **metrics** exists to **evaluate the performance** of the modeled cyber and physical-system layers.
- The **use of metrics** allows the proper evaluation of the overall system alongside its corresponding subsystems.
- These metrics provide **quantitative ways to measure and evaluate the performance of the system's operation** at a particular time, both at the cyber and the physical-system layers.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Metrics - Physical-System Layer

Name	Description	Domain
Rise time	Evaluates the time required for the output to rise from %x to %y of the steady-state response	Control
Percent overshoot	Evaluates the maximum peak value of the output minus the step value divided by the step value	Control
Settling time	Evaluates the time required for the output to reach and remain within a defined error band	Control
Steady-state error	Evaluates the difference between the input (command) and the output of the system	Control
Integrate absolute error (IAE)	Evaluates the absolute error of the system over time	Control
Voltage stability	Metrics that evaluate the voltage stability and regulation of the EPS according to defined limits	EPS
Frequency stability	Metrics that evaluate the frequency stability of the EPS according to defined limits	EPS
Optimization	Optimization metrics used to evaluate energy and power management functions, e.g., energy cost, efficiency	EPS
Power quality	Power quality metrics such as THD, transients, flickering, and voltage sags used to evaluate EPS operation [146]	EPS
Reliability	Reliability indices to evaluate EPS operation, e.g., SAIFI, SAIDI, ASAI, lost load % [146]	EPS
Command vs. Measured % error	Percentage error between signal command coming from controller and signal measured	Simulation (CHIL)
PHIL Accuracy	Metrics that evaluate the accuracy of the PHIL integration [147]	Simulation (PHIL)

Physical-system layer performance metrics. These metrics are divided according to the domain where they can be measured.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.
[146] T. Key and K. Forsten, "Security, quality, reliability and availability: Metrics definition: Progress report," EPRI, 2005.
[147] W. Ren, "Accuracy evaluation of power hardware-in-the-loop (PHIL) simulation," Florida State University, 2007.

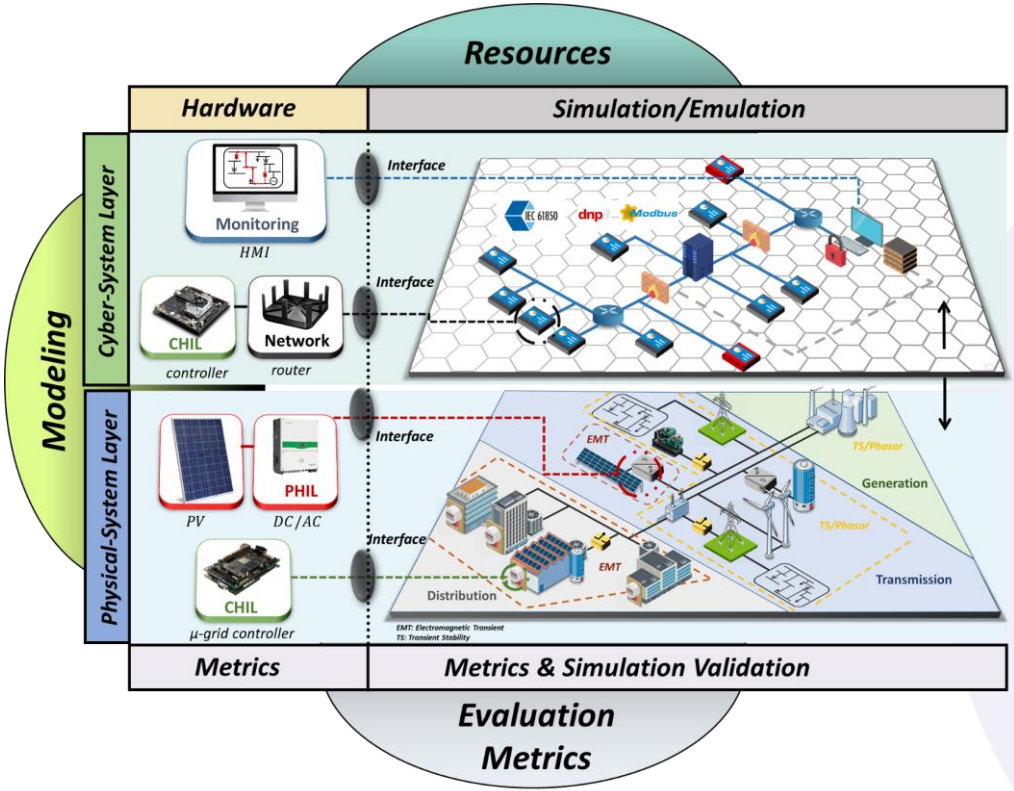
Cyber-Physical Energy Systems (CPES) Testing Framework: Metrics - Cyber-System Layer

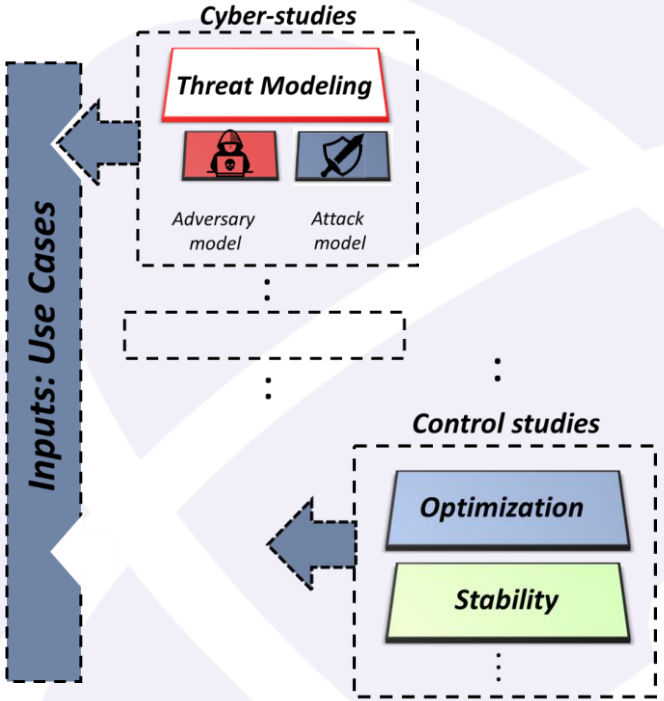
These metrics are divided according to the OSI model layer and connection where they can be measured.

Name	Description	Layer	Connection
Bit rate (R)	Number of bits conveyed per unit of time	*L1/L2*	Wired/Wireless
Bit-error rate (BER)	Ratio of the number of received bits altered during transmission to the total number of bits sent	*L1/L2*	Wired/Wireless
Packet-error rate (PER)	Ratio of the number of packets received incorrectly to the total number of packets received	*L1/L2*	Wired/Wireless
Nominal channel capacity (NCC)	Maximum number of bits that can be transmitted per unit of time	*L1/L2*	Wired/Wireless
Channel utilization (CU)	Ratio between NCC and the total number of bits received per transmission time	*L1/L2*	Wired/Wireless
Signal-to-noise ratio (SNR)	Ratio of the signal power to the background noise	*L1/L2*	Wired
Signal-to-interference-plus-noise ratio (SINR)	Similar to SNR but considers the interference power from other signals	*L1/L2*	Wireless
Spectral efficiency (SE)	Number of received bits per unit of time per unit of bandwidth and per unit areas (i.e., $\frac{b/s}{Hz \cdot m^2}$)	*L1/L2*	Wireless
Received signal strength indication (RSSI)	Signal strength measured at the receiver's antenna during packet reception	*L1/L2*	Wireless
Hop count	Minimum hop-count from source node to destination node	*L3*	Wired/Wireless
Round trip time (RTT)	Time that it takes for a signal to be sent and the acknowledgement received	*L3*	Wired/Wireless
Expected transmission time (ETT)	Time needed for a data packet to be correctly transmitted over a link	*L3*	Wireless
Betweenness	Number of shortest paths between any two nodes that pass through the evaluated node	*L3*	Wired/Wireless
Node degree	Number of nodes that depend on the evaluated node.	*L3*	Wired/Wireless
End-to-end delay	Time required to transmit a packet along the path between source and destination nodes	*L4/L5/L6/L7*	Wired/Wireless
Jitter	Packet delay variation	*L4/L5/L6/L7*	Wired/Wireless
Bandwidth	Overall bandwidth consumption in the network	*L4/L5/L6/L7*	Wired/Wireless
Link stress	Number of packet replicas traversing the same physical link	*L4/L5/L6/L7*	Wired/Wireless

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Cyber-Physical Energy Systems (CPES) Testing Framework: Overall





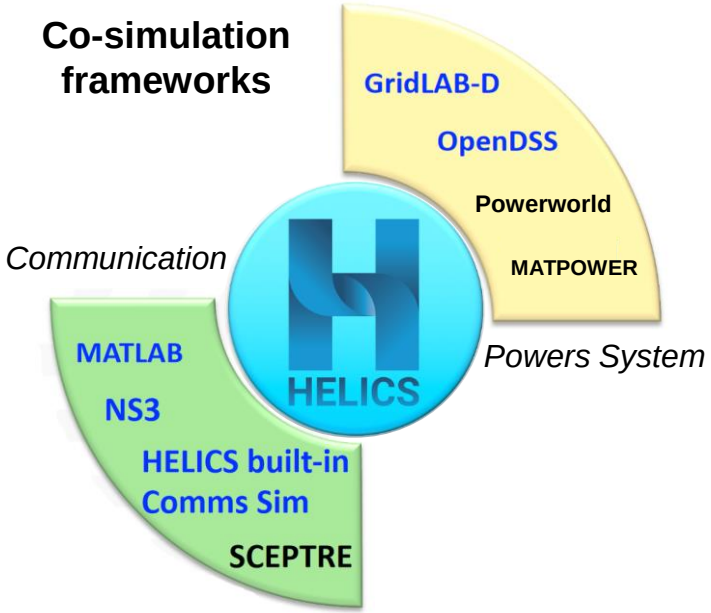
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

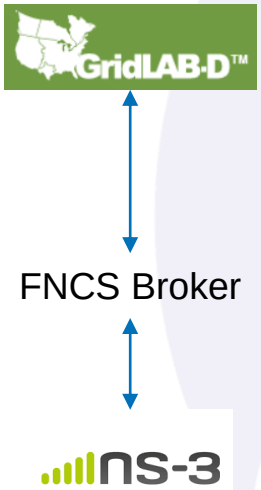
Outline

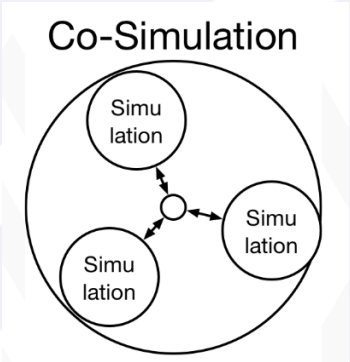
- Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- Threat Modeling Framework for Cyber-Physical Energy Systems (CPES)
- Cyber-Physical Energy Systems (CPES) Testing Framework
- Co-Simulation of Cyber-Physical Energy Systems (CPES)

Co-Simulation of Cyber-Physical Energy Systems (CPES): What is Co-Simulation?

Co-simulation can be defined as an emerging technique that enables the **global simulation** of a **coupled system** by allowing the simulation of its composing parts using different simulation platforms.







https://www.energy.gov/sites/prod/files/2019/08/f65/3.1.b.%20-%20SETO%20Modeling%20Workshop%20-%20NREL.pdf

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 1 - Time-Delay Attacks

- **Time-Delay Attack (TDA)**
  - Data Availability Attack (DAA)
  - Attackers try destabilize a compromised control system by delaying measurements and/or controls
  - Implemented via network congestion (flooding the network with data)

- **Time-Delay Attack (TDA) Case Study**
  - **Physical:** EMT Real-time (Opal-RT-eMegaSIM)
    - Generator: 1 MW
    - Lithium-ion ES: 100 kW/100 kWh
    - Sheddable Load: L1 – 400 kW
    - Non-controllable loads: L2 & L3
  - **Cyber:** Emulation (EXataCPS)
    - Switch
    - Master & Outstations (DNP3)

Mathematical formulation

$$f_D\big(s_r(k)\big) = \begin{cases} s_r(k-d), & \text{if } k \in \mathrm{T}_{\text{attack}} \\ s_r(k), & \text{otherwise} \end{cases}$$

$\mathrm{T}_{\text{attack}}$ - period of time when TDA is performed.

s_r - compromised signal (*u* or *y*).

f_D - time-delay function.

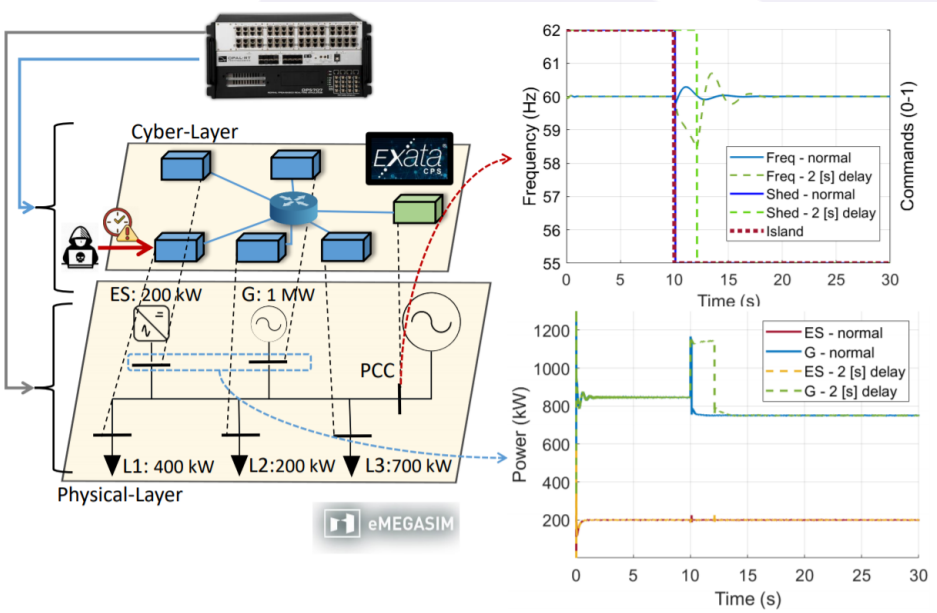
d – discrete constant delay or time-varying delay fcn.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 1 - Time-Delay Attacks

Threat Model	TDA
Knowledge	Oblivious
Access	Non-possession
Specificity	Targeted
Resources	Class II
Frequency	Iterative
Reproducibility	Multiple-times
Functional Level	L1
Asset	Controller
Technique	DoS
Premise	Cyber: Availability

Threat Modeling

TDA – 2 seconds delay attack control values.



Cyber-Physical Energy Systems (CPES) Testing Framework

Layers	Modeling	Resources	Metrics
Cyber-System	Emulation	EXataCPS	- Avg. delay - # Packets delayed
Physical-System	EMT : Real-time	eMegaSim	Frequency stability

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 1 - Time-Delay Attacks

TDA (Video): 30 seconds TDA Demonstration.

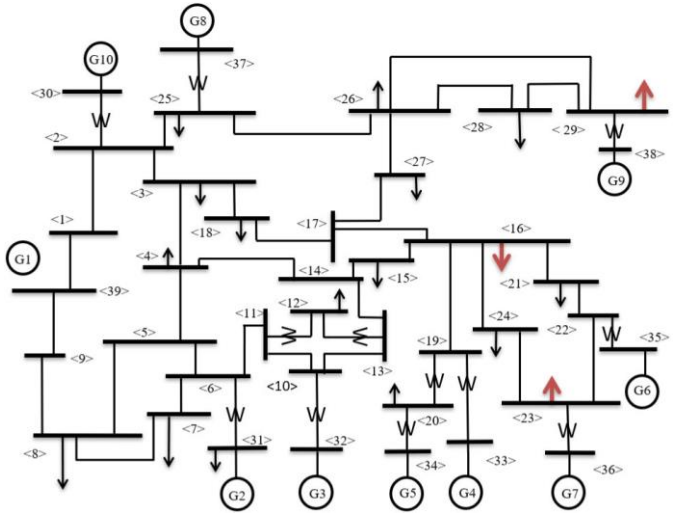
https://youtu.be/2ThAvBp72Bc?t=355

Minute: 5:55

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 2 – Load Changing/Altering Attacks

- **Generators** modeled as synchronous machines (dynamics are modeled + excitation system)
- **Loads** modeled as constant impedance, current, and power (ZIP) AND **Variables Loads**



Threat Modeling

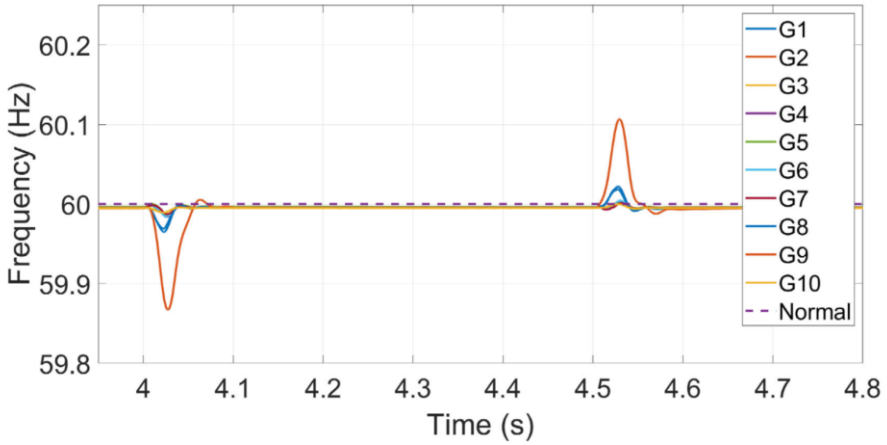
Threat Model	TDA
Knowledge	Semi-Oblivious
Access	Non-possession
Specificity	Targeted
Resources	Class II
Frequency	Iterative
Reproducibility	Multiple-times
Functional Level	L1
Asset	Smart HVAC, High-wattage IoT devices
Technique	False Data Injection
Premise	Cyber: Integrity

Cyber-Physical Energy Systems (CPES) Testing Framework

Layers	Modeling	Resources	Metrics
Cyber-System	-	-	-
Physical-System	EMT: Real-time	OPAL-RT (eMegaSim)	Frequency Stability

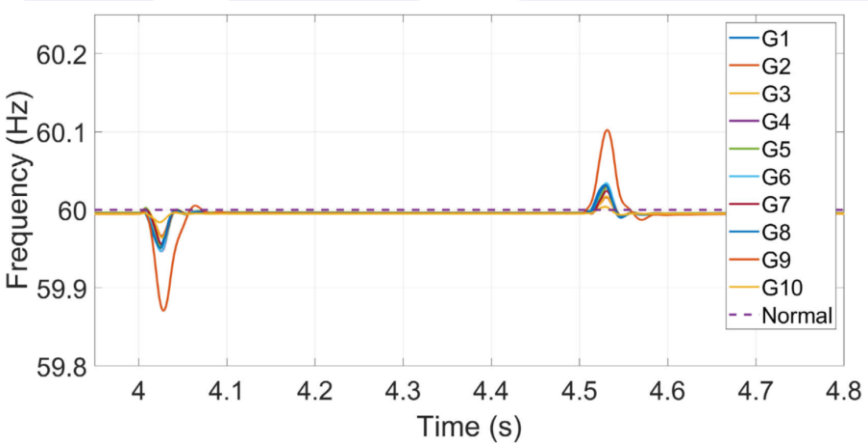
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 2 – Load Changing/Altering Attacks



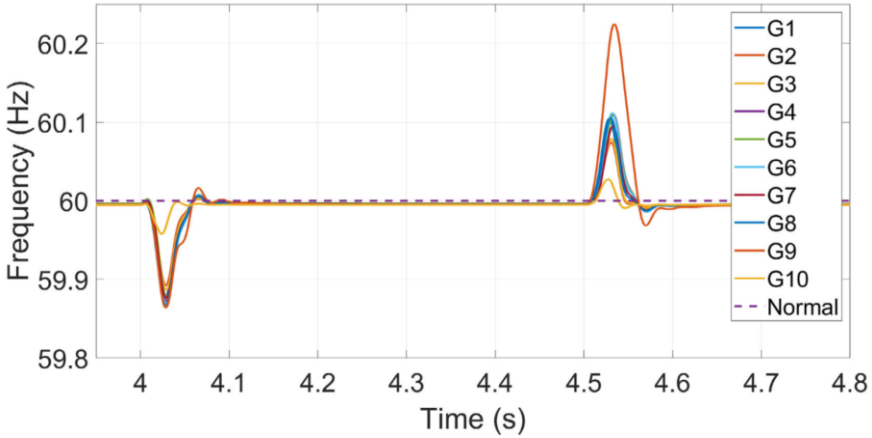
Frequency variation impact on the power grid with 20% demand increased at bus 29

Frequency variation impact on the power grid with 20% demand increased at bus 29 & 16



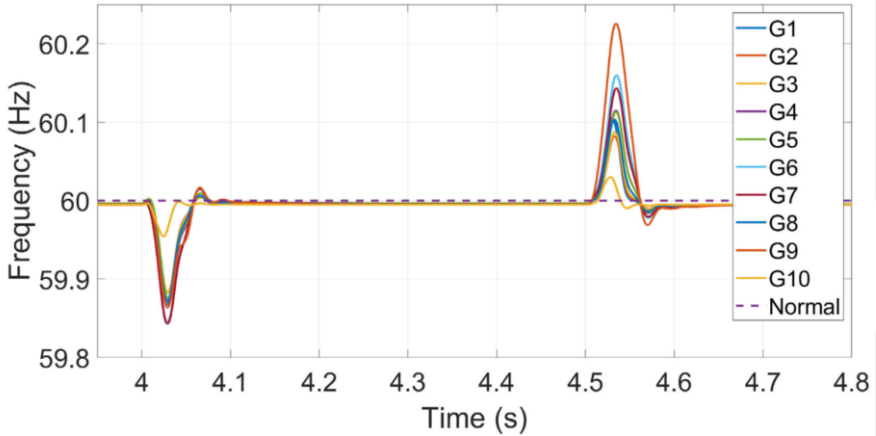
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 2 – Load Changing/Altering Attacks



Frequency variation impact on the power grid with 50% demand increased at bus 29 & 16

Frequency variation impact on the power grid with 50% demand increased at bus 29,16 & 23



Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.

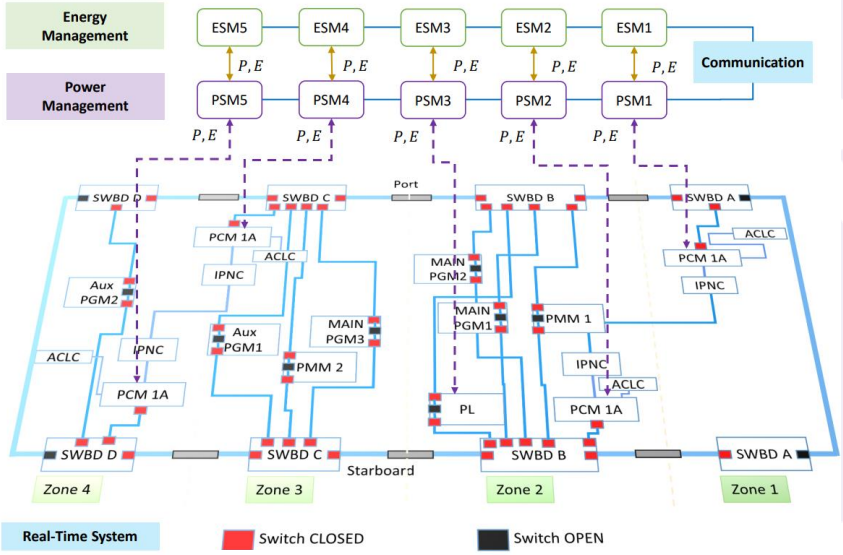
Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 3 - Real-Time Co-Simulation for Shipboard Power Systems

Test system:
- 4-zone Medium-Voltage DC (MVDC) system
- The power system is a 12kVDC-100MW MVDC

Power Storage Management (PSM) Controllers
- Power-sharing among Energy Storage Modules (ESM) during pulse power operations
- Communication using a ring topology
- Communication constraint of $\mathbf{1}ms$

Energy Storage Management (ESM) Controllers
- Charges ESM to pre-defined SOC at completion of each pulse power operation
- Reduces generator output by servicing pulse loads
- Discharging 10MW and Charging 5MW power
- Communication using a star topology
- Communication constraint of $\mathbf{5}ms$

Controller Hardware
- Eleven (11) Total Controllers
  - 5 x NI cRIO-9064 (Communication Agents (PSM))
  - 5 x NI sbRIO-9637 (Solver Agents (ESM))
  - 1 x NI sbRIO-9637 (Host Controller: Controls state of all controllers)



sbRIO-9637

cRIO-9064

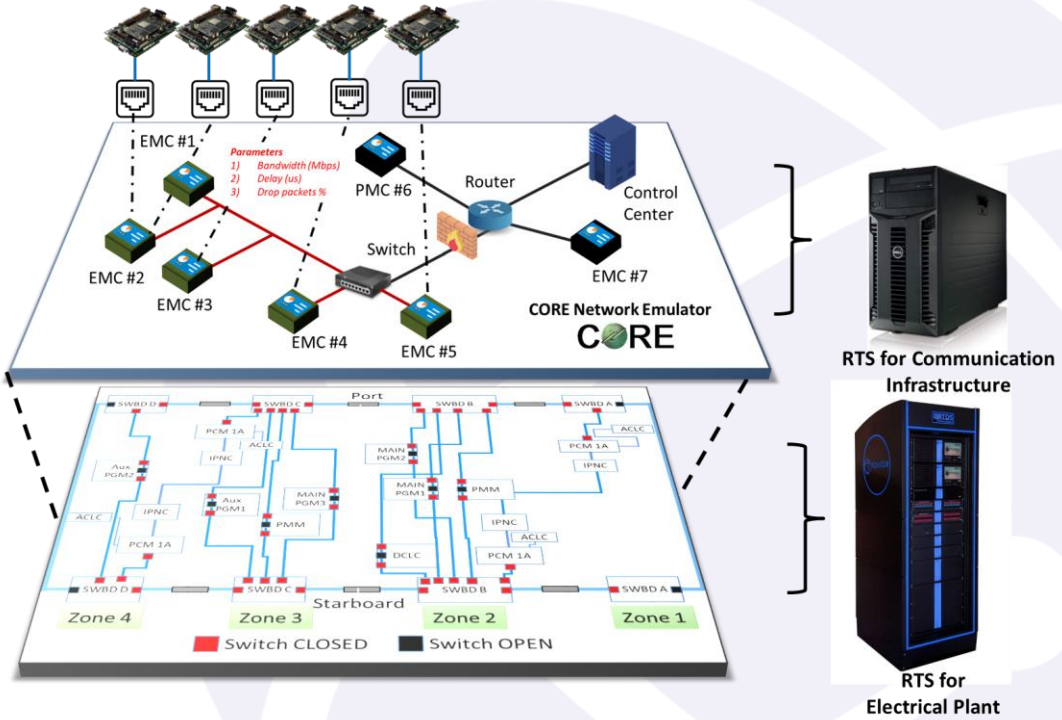
Ogilvie, C., Ospina, J., Konstantinou, C., Vu, T., Stanovich, M., Schoder, K., & Steurer, M. (2020, October). Modeling communication networks in a real-time simulation environment for evaluating controls of shipboard power systems. In 2020 IEEE CyberPELS (CyberPELS) (pp. 1-7). IEEE.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 3 - Real-Time Co-Simulation for Shipboard Power Systems

Cyber-Physical Energy Systems (CPES) Testing Framework

Layers	Modeling	Resources	Metrics
Cyber-System	Emulation	CORE	Packet Loss, Latency
Physical-System	EMT: Real-time	RTDS (RSCAD)	State-of-Charge (SoC) Difference

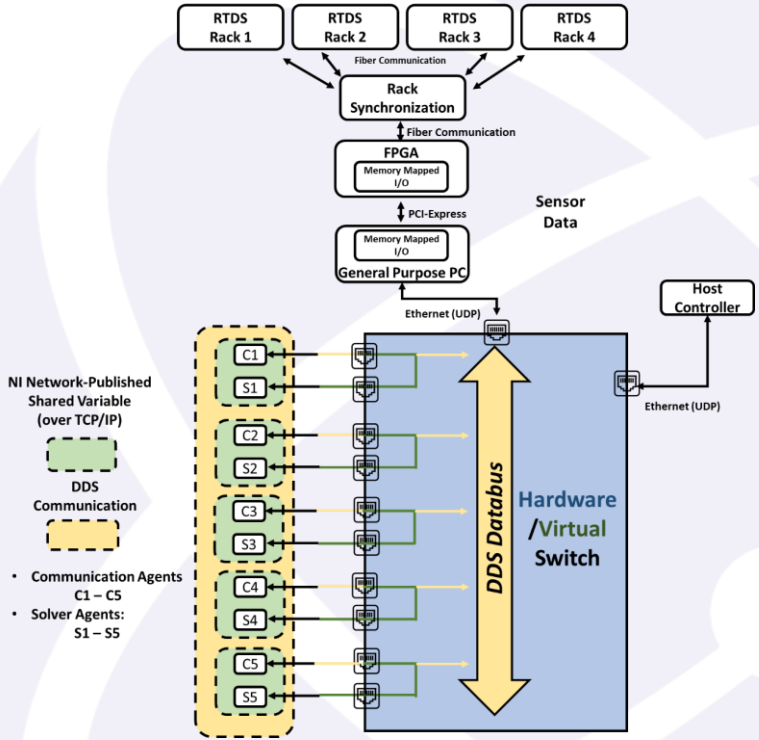
(No threat model)



Ogilvie, C., Ospina, J., Konstantinou, C., Vu, T., Stanovich, M., Schoder, K., & Steurer, M. (2020, October). Modeling communication networks in a real-time simulation environment for evaluating controls of shipboard power systems. In 2020 IEEE CyberPELS (CyberPELS) (pp. 1-7). IEEE.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 3 - Real-Time Co-Simulation for Shipboard Power Systems

- **Communication Agents (C1 → C5)**
  - Communicate through Data Distribution Service (DDS) publish-subscribe model
- **Solver Agents (S1 → S5)**
  - Communication with corresponding communication agent using NI network-published shared variable over TCP/IP
  - Correspond Comm. Agent: C1↔S1, C2 ↔S2, C3↔S3, C4 ↔S4, C5 ↔S5
- ***Distributed Power & Energy Management System:**
  - Distributed Crow Search Algorithm (DCSA) – Energy Optimization
  - Distributed MPC based on Alternating direction method of multipliers (ADMM) [*]

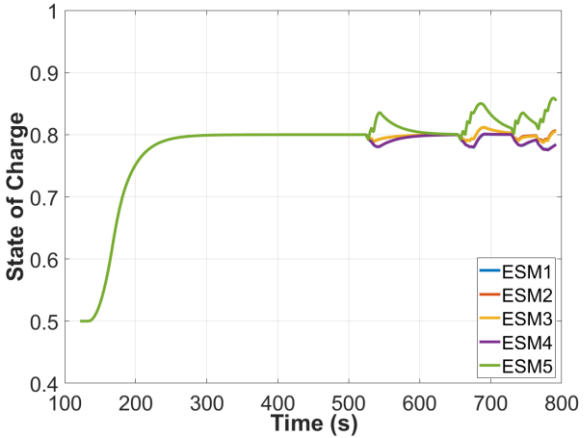


Ogilvie, C., Ospina, J., Konstantinou, C., Vu, T., Stanovich, M., Schoder, K., & Steurer, M. (2020, October). Modeling communication networks in a real-time simulation environment for evaluating controls of shipboard power systems. In 2020 IEEE CyberPELS (CyberPELS) (pp. 1-7). IEEE.

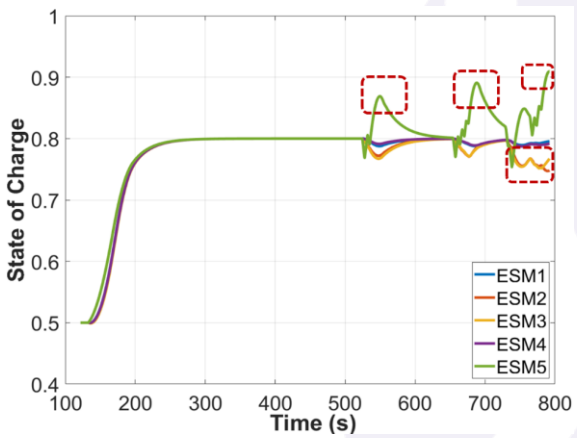
[*] T. V. Vu et al., "Large-scale distributed control for MVDC ship power systems," in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018, pp. 3431–3436.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 3 - Real-Time Co-Simulation for Shipboard Power Systems

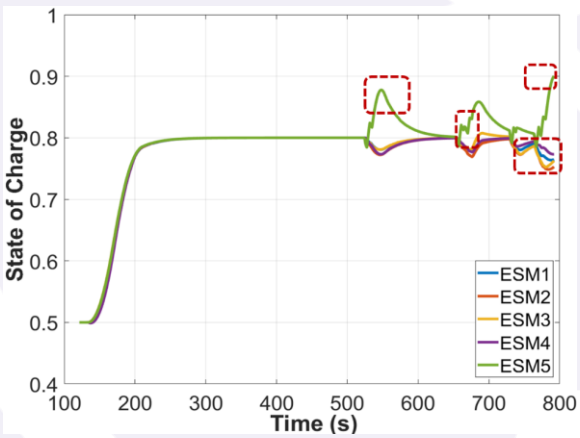
Virtual-based switch – No Delay



Virtual-based switch – 100 ms delay



Virtual-based switch – 10% packet loss



Ogilvie, C., Ospina, J., Konstantinou, C., Vu, T., Stanovich, M., Schoder, K., & Steurer, M. (2020, October). Modeling communication networks in a real-time simulation environment for evaluating controls of shipboard power systems. In 2020 IEEE CyberPELS (CyberPELS) (pp. 1-7). IEEE.

Co-Simulation of Cyber-Physical Energy Systems (CPES): Case 3 - Real-Time Co-Simulation for Shipboard Power Systems

Percent Difference

$$PD_i(\%) = \frac{x_1^i - x_2^i}{\frac{1}{2}\left(x_1^i + x_2^i\right)} * 100$$

- x_1, x_2, Two time-series signals being compared
- n, Total sample size of the signals

Case Study Scenario	SOC	Avg. PD (%)	Max. PD (%)
Hardware-based Switch Run #1 vs. Virtual-based Switch Run #1	ESM 1	0.034	0.218
	ESM 2	0.091	0.225
	ESM 3	0.01	0.248
	ESM 4	0.004	0.225
	ESM 5	0.049	0.375
Hardware-based Switch Run #1 vs. Virtual-based Switch Run #1 [10ms Delay all Cont.]	ESM 1	0.564	1.728
	ESM 2	1.666	3.617
	ESM 3	1.607	3.478
	ESM 4	0.59	1.907
	ESM 5	4.779	9.557
Virtual-based Switch Run #1 vs. Virtual-based Switch Run #1 [100 ms Delay all Cont.]	ESM 1	0.727	2.169
	ESM 2	3.731	7.589
	ESM 3	2.392	5.535
	ESM 4	0.491	1.860
	ESM 5	3.114	8.285
Virtual-based Switch Run #1 vs. Virtual-based Switch Run #1 [10% Packet Loss all Cont.]	ESM 1	1.249	2.498
	ESM 2	3.418	7.154
	ESM 3	2.692	5.852
	ESM 4	0.692	3.566
	ESM 5	2.613	5.668

Ogilvie, C., Ospina, J., Konstantinou, C., Vu, T., Stanovich, M., Schoder, K., & Steurer, M. (2020, October). Modeling communication networks in a real-time simulation environment for evaluating controls of shipboard power systems. In 2020 IEEE CyberPELS (CyberPELS) (pp. 1-7). IEEE.

Conclusion

- The use of a framework (such as the one presented) has many advantages in the research of CPES such as:
  - Clear **understanding** of the:
    - **Models** used (modeling techniques used in the research)
    - **Resources** used (Offline, real-time, etc.)
    - **Metrics** used (cyber, physical, etc.)
  - Clear **threat models** (specifically designed to investigate system vulnerabilities)
  - Provides a (somewhat) **standard approach** to perform:
    - Cybersecurity studies
    - Novel control & optimization techniques (closer to reality)
    - Development of secure authentication techniques
    - Study system's performance and behavior

Contact:

Email(s):

- jjospina@lanl.gov
- juanospinacasas@gmail.com

Personal website

Thank you very much for your time.

Questions?