LA-UR-22-31034

Approved for public release; distribution is unlimited.

Title: Towards the Secure Operation of Cyber-Physical Energy Systems (CPES)

Author(s): Ospina Casas, Juan Jose

Intended for: Invited presentation talk for the Research on Computing Systems (ROCS) Joint Group at King Abdullah University of Science and Technology (KAUST).

Issued: 2022-10-19

Towards the Secure Operation of Cyber-Physical Energy Systems (CPES)

Juan Ospina, *Ph.D*.

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

November 8, 2022

LA-UR-XX-XXXXXX

Research on Computing Systems (ROCS)
King Abdullah University of Science and Technology (KAUST)

Acknowledgements - Team

- Venkatesh Venkataramanan (National Renewable Energy Laboratory)
- Charalambos Konstantinou (King Abdullah University of Science and Technology)

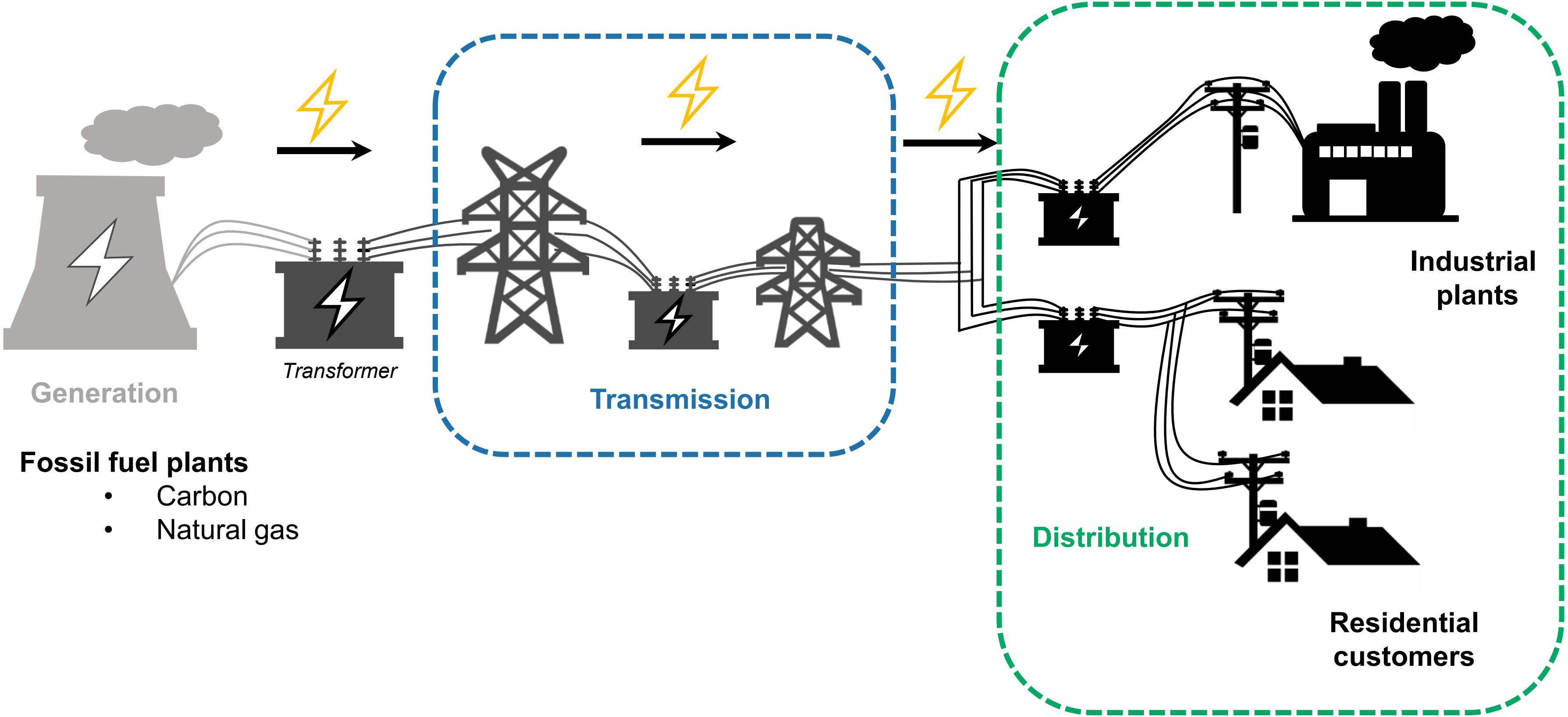
Outline

- Brief Introduction to Electric Power Systems
- Brief Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems

Outline

- Brief Introduction to Electric Power Systems
- Brief Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems

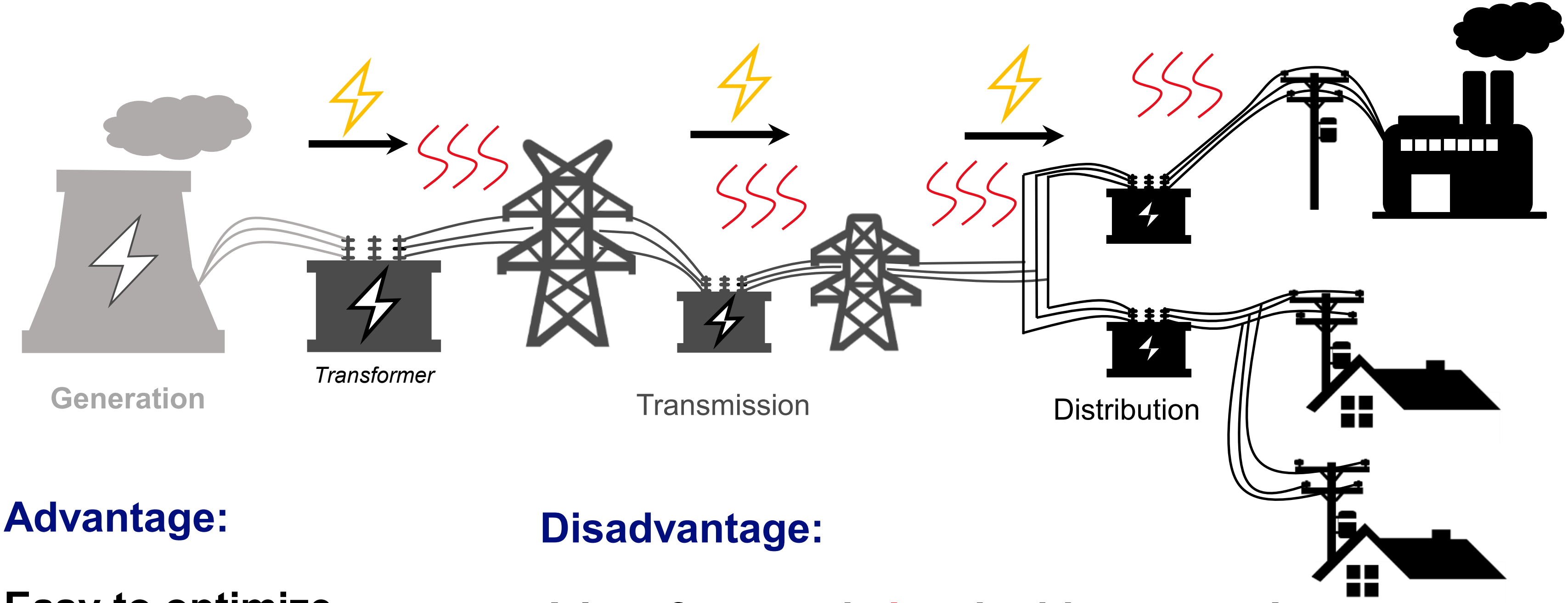
Traditional Power Generation/Consumption



Fossil fuel plants

- Carbon
- Natural gas

Advantages & Disadvantages



Advantage:

Easy to optimize
(All coming from monolithic Generation sites)

Disadvantage:

A lot of energy is lost in this process!

- Around 2-6% in transmission
- Around 4% in distribution

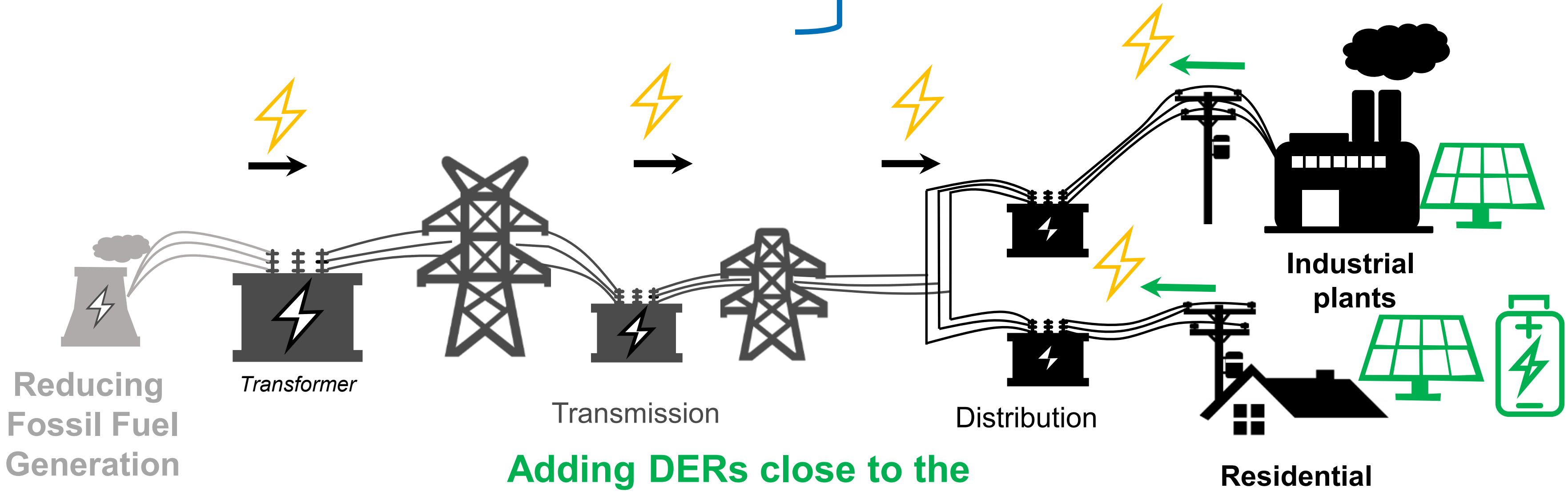
http://insideenergy.org/2015/11/06/lost-in-transmission-how-much-electricity-disappears-between-a-power-plant-and-your-plug/

https://www.eia.gov/energyexplained/us-energy-facts/

Efforts to Reduce Losses and Improve Efficiency

1. Renewable energy sources (RES)
2. Energy storage devices (Batteries)

Distributed Energy Resources (DERs)

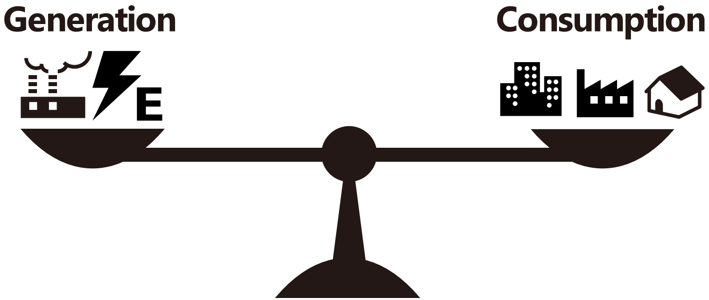


Adding DERs close to the consumption (At the distribution)

Adding DERs (Issue)

- Just adding **DERs everywhere** is not a **realistic** solution
  - A balance between **Generation** & **Consumption** needs to be **always maintained**

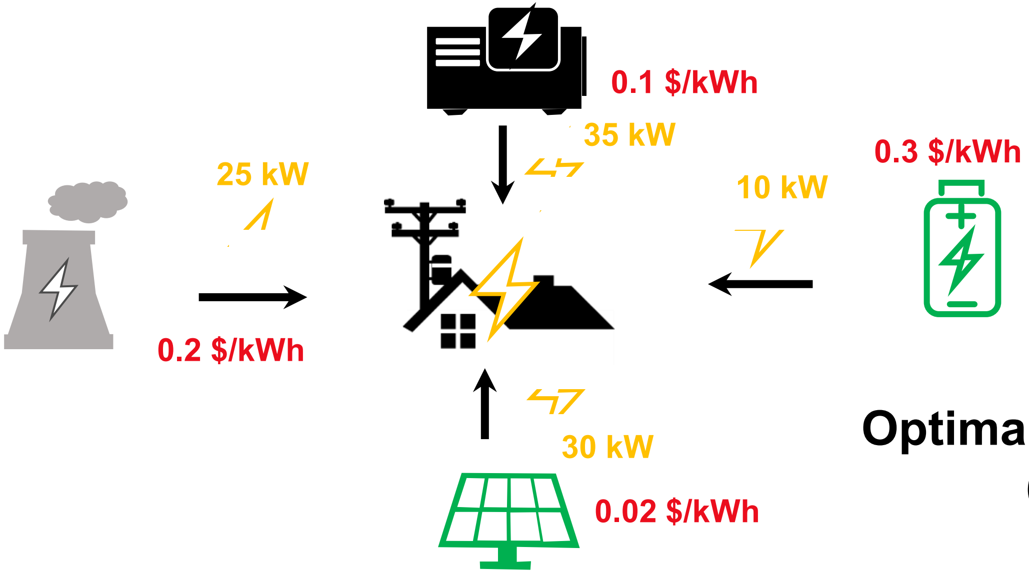
  - **If balanced is not maintained**
    - **Blackouts** can occur
    - **Transformers** can explode
    - **Protection devices** can be triggered



Solution: Optimal control of DERs (Optimization)

We need to **optimize** the **power/energy dispatch** from **DERs**.

Obtain the exact **power** that each **DER** needs to **dispatch.**



Optimal Power Flow (OPF)

Optimizing is not that simple!

Power Flow Formulations:

- Physical models that describe how the **power** flows on the lines.

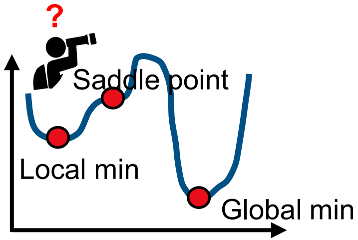
$$P_{ij} = g_{ij}V_i^2 - V_iV_j\left(g_{ij}\cos(\theta_i - \theta_j) + b_{ij}\sin(\theta_i - \theta_j)\right)$$

Bus i Bus j

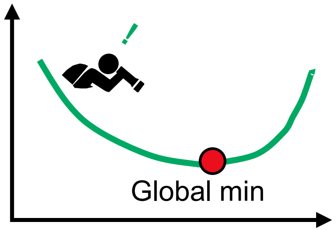
AC Polar

More Accurate

Harder to solve



Non-Convex



Convex

$$P_{ij} = -\frac{1}{x_{ij}}(\theta_j - \theta_i)$$

Bus i Bus j

DC approximation

Less Accurate

Easier to solve

Outline

- Brief Introduction to Electric Power Systems
- Brief Introduction to Cyber-Physical Energy Systems (CPES) & Cybersecurity in Power Systems
- A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems

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

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

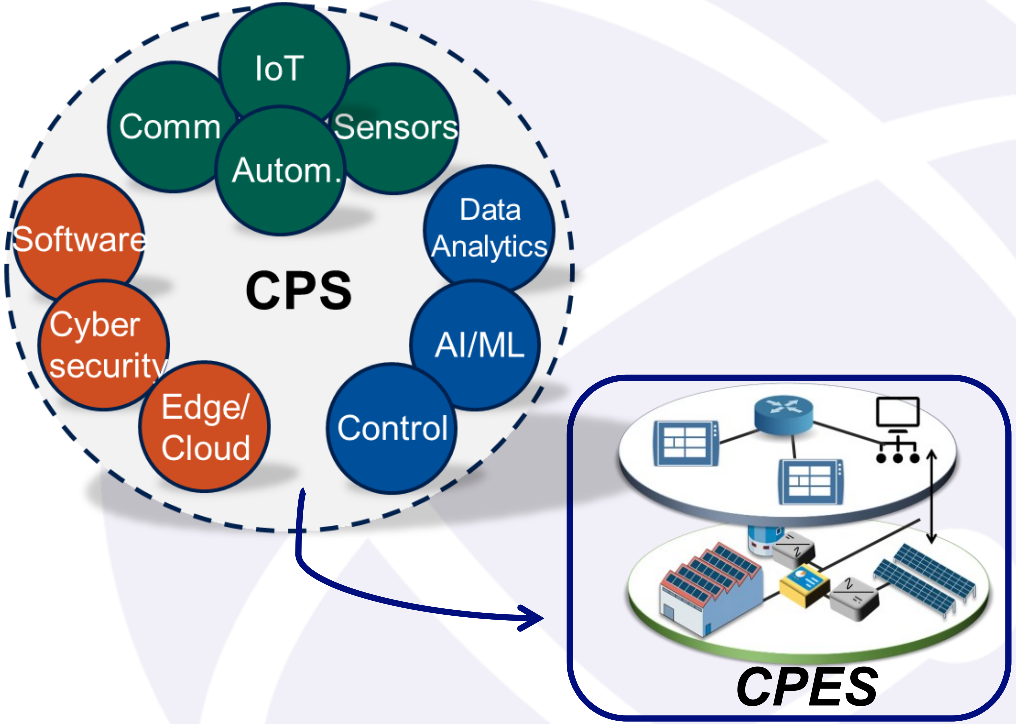
EPS → CPES

- This modernization have **disadvantages**:
  - CPES are 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**

So, what are specifically Cyber-Physical Energy Systems (CPES)?

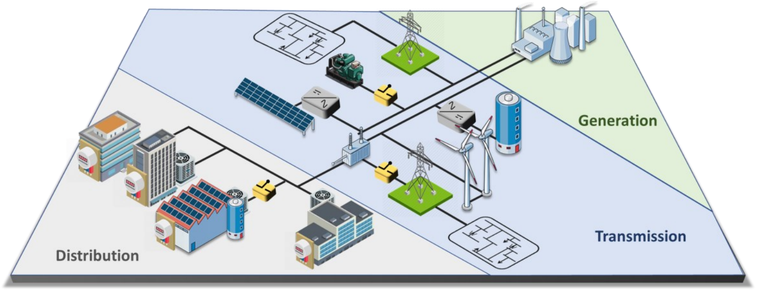
Introduction to Cyber-Physical Energy Systems (CPES)

- **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.

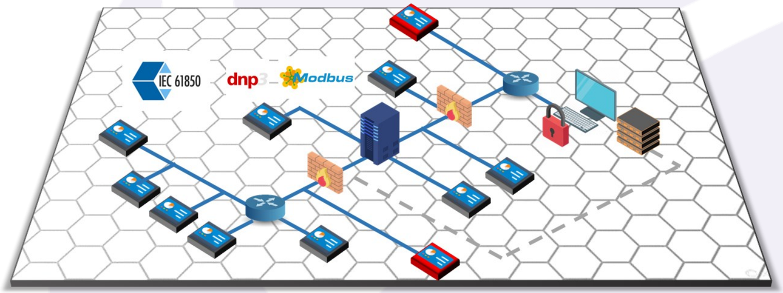


Introduction to Cyber-Physical Energy Systems (CPES)

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



Physical



Cyber

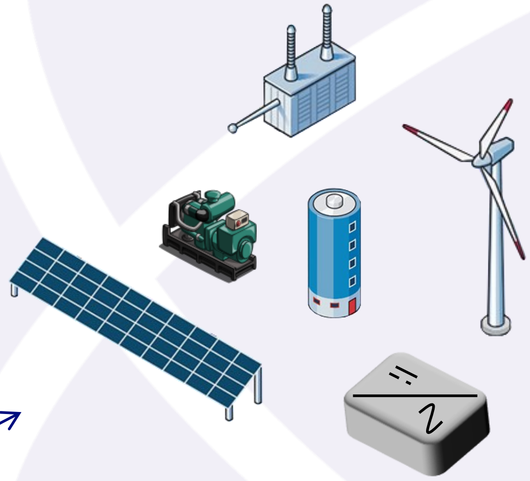
- **Cyber:** computation, communication, and control that are discrete, logical, and switched.
- **Physical:** systems governed by the laws of physics and operating continuously.

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

- **<u>General Definition</u>:** 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

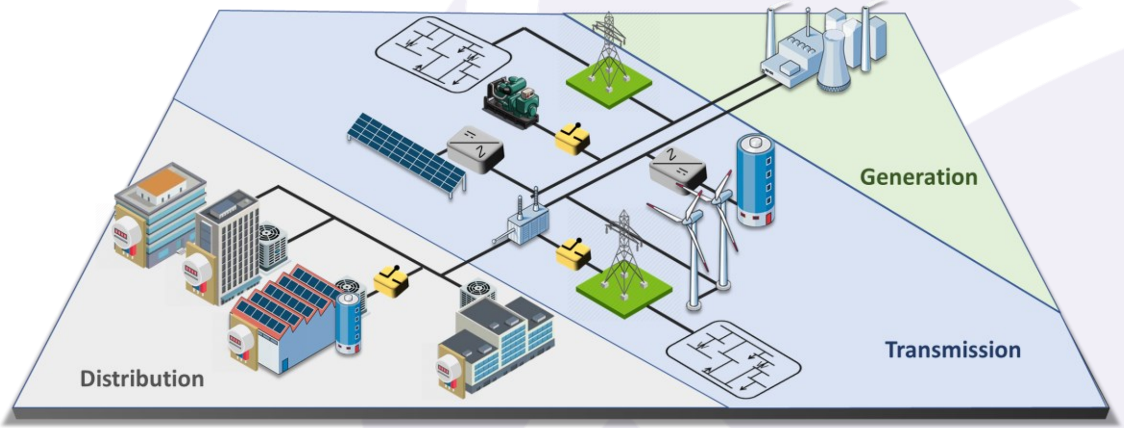
- **Sectors where CPS exist:**
  - Smart Manufacturing
  - Healthcare
  - Robotics
  - Transportation
  - **Electric Power Systems (EPS)**



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

- **General Definition:** composed of **hardware and software components** embedded into the Information Technology (IT) environment.

- Allows the interconnection using common ***communication protocols over digital links.***

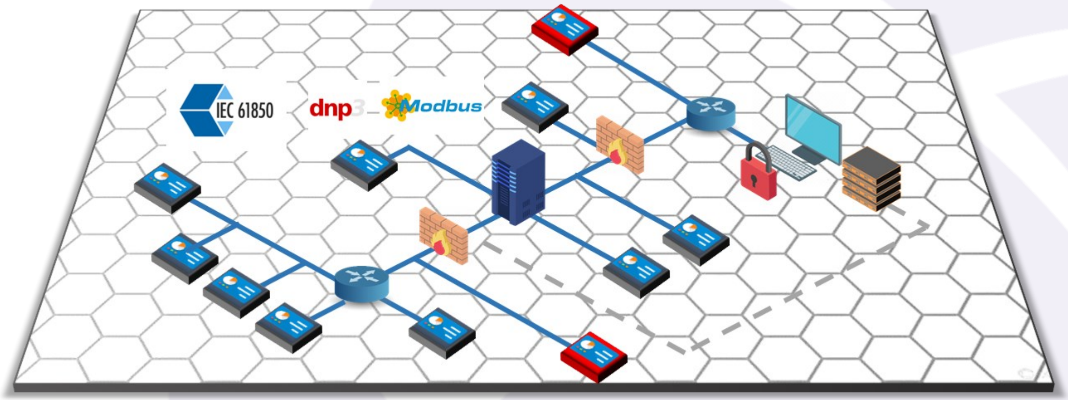
- Allows **sharing resources and data** located across networking nodes.

- ***Real-world CPS*** (e.g., cellular networks, military zones, or SCADA systems) 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 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.

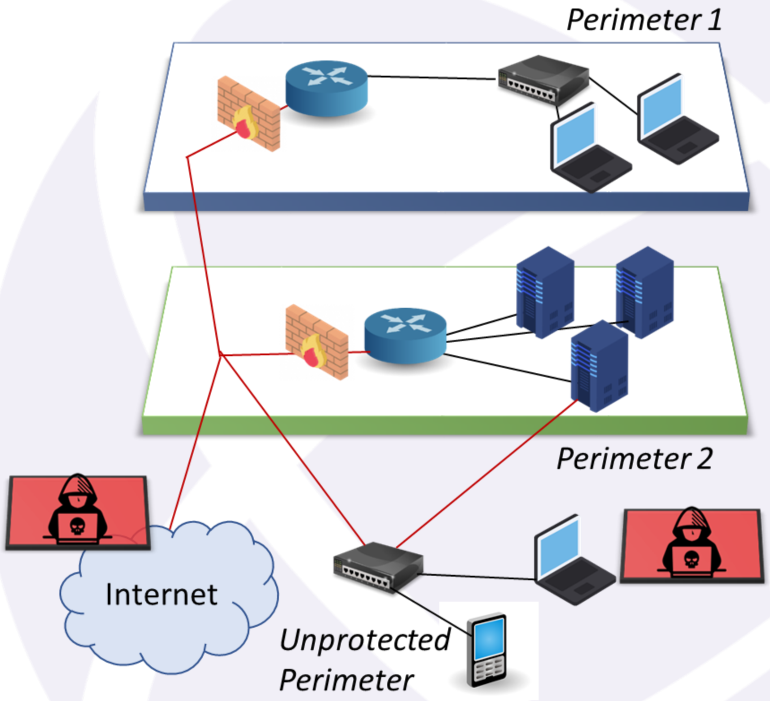
- A technique that removes or reduces a vulnerability

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

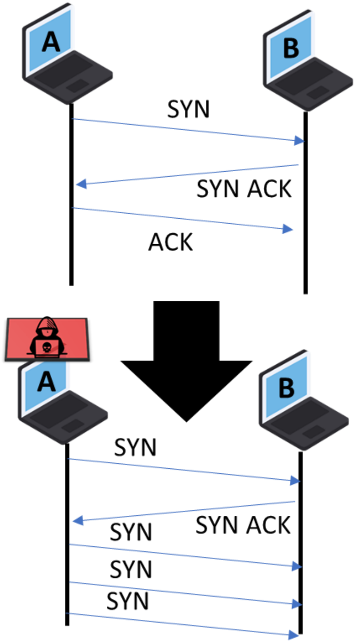
CIA (Confidentiality, Integrity, Accessibility) Triad

- 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)

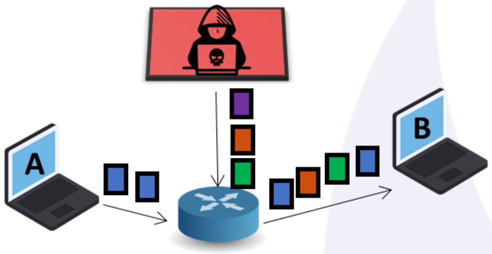
A successful attack violates one or more of these goals.

Introduction to Cybersecurity in Electric Power Systems: Example Cyberattacks

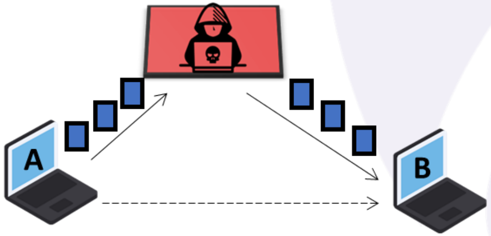
TCP SYN Flooding Attack



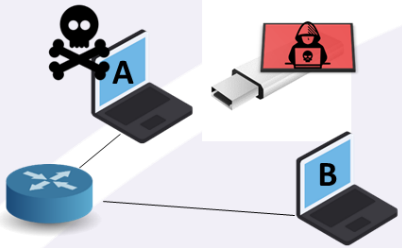
IP Spoofing



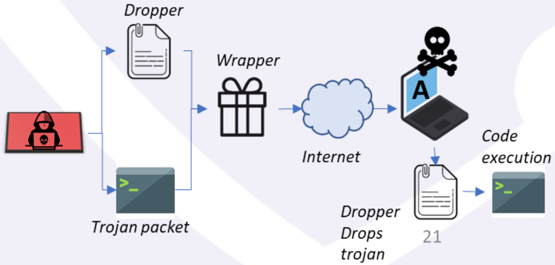
Replay (MiTM)



Malware/Rootkits
(Could be Insider threats)



Trojans



Introduction to Cyber-Physical Energy Systems (CPES): 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

Motivation

Primary motivation(s) for the research conducted:

1. Information and Communication Technologies (ICTs) are creating **new attack vectors** that can affect **reliability** and the way our EPS operate.

- **So, how do we consider ICTs when optimizing EPS/CPES?**

Outline

- Brief Introduction to Electric Power Systems
- Brief Introduction to Cybersecurity in Power Systems & Cyber-Physical Energy Systems (CPES)
- A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems

CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems

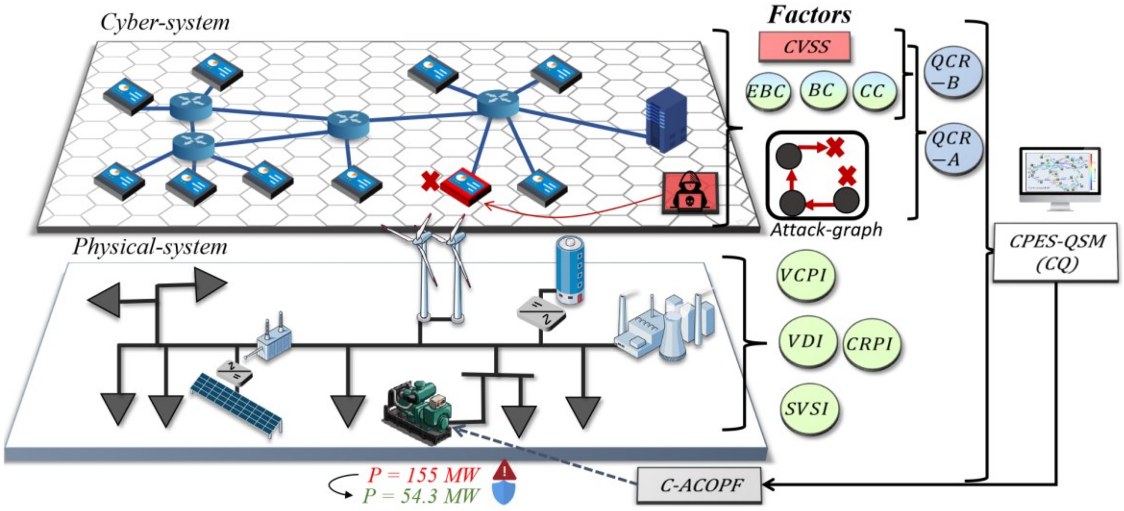
We developed a **process[1]** that:

1) Quantifies the interaction between the **cyber** and **physical** layers in CPES

2) Integrates the **cyber-status** into the operational decisions (OPFs) of the **physical system**.

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems



Overall framework for Cyber-Constrained ACOPF (C-ACOPF) operation based on the Cyber-Physical Energy System Quantitative Security Metric (CPES-QSM).

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

CPES-QSM: Quantifying the interaction between the cyber and physical layers

Developed a cyber-physical **metric called the Cyber-Physical Energy System Quantitative Security Metric (CPES-QSM)**

- **Quantifies the interaction between the cyber** and **physical** layers **across three domains:**

1. *Electrical*
2. *Cyber-risk*
3. *Network topology (Graph-theory)*

CPES-QSM: Quantifying the interaction between the cyber and physical layers

<u>General Idea</u>:

For each node in the CPES

Electrical *Factors*

Cyber-risk *Factors*

Network topology *(Graph-theory) Factors*

Technique used to combine?

Choquet Integral

CPES-QSM

Informs us about the current ***cyber-physical status*** *of the CPES node.*

- *How 'reliable' or 'unreliable' is this node?*
- *How 'important' is this node?*
- *Is the current status of the system nominal?*

CPES-QSM: Quantifying the interaction between the cyber and physical layers – *The Choquet Integral*

- The **Choquet Integral (CI)** is a *multi-criteria decision-making* approach (MCDM)
- Allows **aggregation of criteria** (i.e., factors) with **different units**.
- It is an aggregation function w.r.t. ***fuzzy measures****.*

Let's see an example to understand how the CI works!

CPES-QSM: Quantifying the interaction between the cyber and physical layers – *The Choquet Integral*

Let's imagine we have **three** criteria (or factors) that we want to combine:

x_1, x_2, x_3

Interaction Index

First step: we need to compute the ***fuzzy measures and λ*** using Equation (1) and (2).

The **fuzzy measures tell you the importance of the subset of criteria. E.g.,*

$$\upsilon(x_1, x_2) = X$$

Where X tells you the weight or 'importance' of the group/subset x_1 and x_2

CPES-QSM: Quantifying the interaction between the cyber and physical layers – *The Choquet Integral*

First step: we need to compute the ***fuzzy measures and λ*** using Equation (1) and (2).

$\boxed{x_1, x_2, x_3}$

$$\lambda + 1 = \prod_{i=1}^{n}(1 + \lambda \nu_i), \quad \text{where} \quad -1 \leq \lambda < 0 \qquad (1)$$

$$\nu(\{x_1, x_2, \ldots, x_n\}) = \frac{1}{\lambda}\left|\prod_{i=1}^{n}(1 + \lambda \nu_i) - 1\right| \qquad (2)$$

1.1 We need to assign 'expert' weights (fuzzy measures) to the individual factors

$$\upsilon(\{\emptyset\}) = 0$$

$$\upsilon(\{x_1\}) = 0.42$$

$$\upsilon(\{x_2\}) = 0.50$$

$$\upsilon(\{x_3\}) = 0.62$$

Then, using (1),
we can solve for $\boldsymbol{\lambda}$

$$\lambda + 1 = (1 + \lambda\upsilon_1)(1 + \lambda\upsilon_2)(1 + \lambda\upsilon_3)$$

$$\lambda + 1 = (1 + \lambda 0.42)(1 + \lambda 0.50)(1 + \lambda 0.62)$$

$$\lambda = -0.748$$

CPES-QSM: Quantifying the interaction between the cyber and physical layers – *The Choquet Integral*

1.2 Now, we can compute the ***fuzzy measures,*** using Eq. (2)

$$\nu(\{x_1, x_2, \ldots, x_n\}) = \frac{1}{\lambda}\left|\prod_{i=1}^{n}(1 + \lambda\nu_i) - 1\right| \quad (2)$$

$$\upsilon(\{x_1, x_2\}) = 0.75$$
$$\upsilon(\{x_1, x_3\}) = 0.82$$
$$\upsilon(\{x_2, x_3\}) = 0.86$$
$$\upsilon(\{x_1, x_2, x_3\}) = 1.0$$

Note: *fuzzy measures only need to be computed* ***once****!*
They determine the 'importance' of the factors and their combinations!

CPES-QSM: Quantifying the interaction between the cyber and physical layers – *The Choquet Integral*

Second step (& final step): we can compute the CI for any value (incoming input value of) x_1, x_2, x_3, using Eq. (3)

fuzzy measures

$$CI_\nu = \sum_{i=1}^{n} [x_i - x_{i-1}] \nu(F_i) \qquad (3)$$

* For our software tool, we use the library ***fmtools v3.0***

[2] https://gitlab.com/juanjospina/quantitative-cyber-metric

CPES-QSM: Quantifying the interaction between the cyber and physical layers

General Idea:

For each node in the CPES

Technique used to combine?

Choquet Integral

Electrical *Factors*

Cyber-risk *Factors*

Network topology *(Graph-theory) Factors*

CPES-QSM

*Informs us about the current **cyber-physical status** of the CPES node.*

- *How 'reliable' or 'unreliable' is this node?*
- *How 'important' is this node?*
- *Is the current status of the system nominal?*

CPES-QSM: Quantifying the interaction between the cyber and physical layers

Factors (criteria) used to calculate the **CPES-QSM**

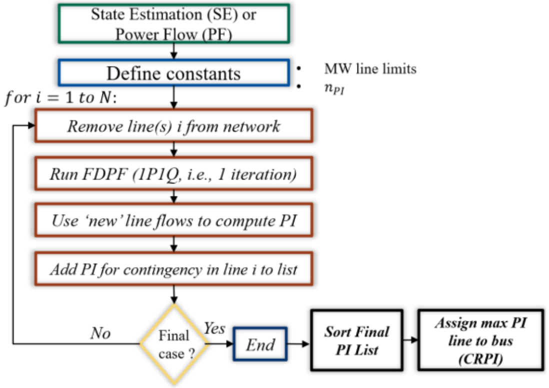
ID	Name	Domain	Environment	Measurement	Formula(s)	Target	Data Source	Report Format
CRPI	Contigency Ranking Performance Index	Electrical	Physical	voltages & angles	Eq. (1)	0	SE, PF, IoTs, SMs, PMUs	decimal
VDI	Voltage Deviation Index	Electrical	Physical	voltage magnitude	Eq. (2)	0	SE, PF, IoTs, SMs, PMUs	decimal
VCPI	Voltage Collapse Prediction Index	Electrical	Physical	voltages/admittance matrix	Eq. (3) - (4)	0	SE, PF, IoTs, SMs, PMUs	decimal
SVSI	Simplified Voltage Stability Index	Electrical	Physical	voltage phasors	Eq. (5) - (7)	0	SE, PF, IoTs, SMs, PMUs	decimal
QCR-B	Quantitative Cyber Risk Base	IT	Cyber	CVSS v3.1 vulnerabilities	Eq. (12) - (13)	≈ 0	cybersecurity assessment	decimal
QCR-A	Quantitative Cyber Risk Attack Graph	IT	Cyber	CVSS v3.1 vulnerabilities	Eq. (13) - (17)	≈ 0	cybersecurity assessment	decimal
BC	Betweenness Centrality	Graph	Network	topology	Eq. (9)	≈ 0	operation center	integer
CC	Closeness Centraility	Graph	Network	topology	Eq. (10)	≈ 0	operation center	integer
EBC	Edge Betweenness Centrality	Graph	Network	topology	Eq. (11)	≈ 0	operation center	integer

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

CPES-QSM: Quantifying the interaction between the cyber and physical layers - *Electrical (Physical) Factors*

Contingency Ranking Performance Index (CRPI)

$$PI_i = \sum_{l, l \neq i}^{N} \left(\frac{P_{l,i}^{flow}}{P_l^{max}}\right)^{2n_{PI}} \quad \text{for } i = 1, \dots, N$$



Voltage Deviation Index (VDI)

$$VDI_k = |1.0 - V_{k(in\ pu)}^{mag}|$$

Voltage Collapse Prediction Index (VCPI)

$$VCPI_k = \left| 1 - \frac{\sum_{m=1; m \neq k}^{N} V_m'}{V_k} \right|$$

**Estimates how close a bus is to voltage collapse*

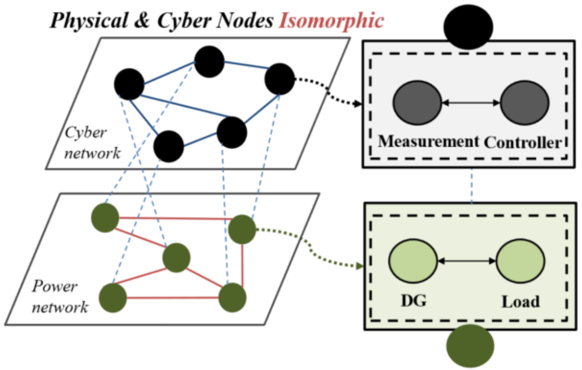
Simplified Voltage Stability Index (SVSI)

$$SVSI_k = \frac{\Delta V_k}{\beta V_k}$$

Determines how stable a bus in the system is in terms of voltage collapse.

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

CPES-QSM: Quantifying the interaction between the cyber and physical layers - *Network topology (Graph-theory)*



Betweenness Centrality (BC)

$$BC(v) = \sum_{s \neq t \neq v \in \mathcal{V}} \frac{\sigma(s,t|v)}{\sigma(s,t)}$$

Closeness Centrality (CC)

$$CC(v) = \frac{n-1}{\sum_{u=1}^{n-1} d(u,v)}$$

Edge Betweenness Centrality (EBC)

$$EBC(e) = \sum_{s \neq t \in \mathcal{V}} \frac{\sigma(s,t|e)}{\sigma(s,t)}$$

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

CPES-QSM: Quantifying the interaction between the cyber and physical layers - *Cyber Factors*

$$\boxed{QCR_{B/A} = P \times I,}$$

QCR – Quantitative cyber-risk
P – Probability of attack
I – Impact of the attack

EXPLOITABILITY METRICS IN COMMON VULNERABILITY SCORING SYSTEM VERSION V3.1 (CVSS V3.1)

Score System	Metric	Abb.	Metric Value	Numerical Value
CVSS v3.1	Attack Vector	AV	Network	0.85
			Adjacent network	0.62
			Local network	0.55
			Physical	0.2
	Attack Complexity	AC	Low	0.77
			High	0.44
	User Interaction	UI	None	0.85
			Required	0.62
	Privileges Required	PR	None	0.85
			Low	0.62 if S = Unchanged 0.68 if S = Changed
			High	0.27 if S = Unchanged 0.50 if S = Changed

Quantitative Cyber Risk Base Model (QCR-B)

$$P = AV \times AC \times UI \times PR$$

$$I = (BC + CC + EBC) \times P^{\%}_{g/l}$$

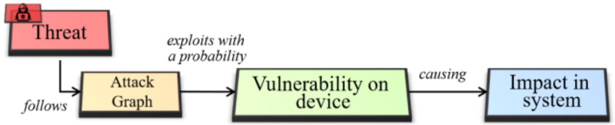
$P^{\%}_{g/l}$ is the generation or load percentage of the total generation or load in the system.

Quantitative Cyber Risk Attack Graph-based Model (QCR-A)

$$\left.\begin{aligned} P_n^{leading} &= \prod_{i=1}^{n-1} P_i \\ P_n^{ag} &= P_n^{leading} \times P_n \end{aligned}\right\} \textit{Serial}$$

$$\left.\begin{aligned} P_n^{leading} &= 1 - \prod_{i=1}^{n-1} (1 - P_i) \\ P_n^{ag} &= P_n^{leading} \times P_n \end{aligned}\right\} \textit{Parallel}$$

$$I = (BC + CC + EBC) \times P^{\%}_{g/l}$$



[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

CPES-QSM: Integrate the cyber-status into the operational decisions (OPFs) of the physical system.

Now, let's see how we use the **CPES-QSM** to 'alter' the OPF of a CPES.

Traditional ACOPF

Minimize cost

$$\min \sum_{k \in G} c_{2k} (\Re(S_k^g))^2 + c_{1k} (\Re(S_k^g)) + c_{0k}$$

Subject to the following ***constraints***

Power flows in lines

$$\boxed{\begin{aligned} S_{ij} &= (Y_{ij} + Y_{ij}^c)^* |V_i|^2 - Y_{ij}^* V_i V_j^*, \ \forall (i,j) \in E \\ S_{ji} &= (Y_{ij} + Y_{ji}^c)^* |V_j|^2 - Y_{ij}^* V_i^* V_j, \ \forall (i,j) \in E \end{aligned}}$$

Reference

$$\boxed{\theta_r = 0, \ \forall r \in R}$$

Generators limits

$$\boxed{S_k^{gl} \leq S_k^g \leq S_k^{gu}, \ \forall k \in G}$$

Voltage limits

$$\boxed{v_i^l \leq |V_i| \leq v_i^u, \ \forall i \in N}$$

Power balance (KCL)

$$\boxed{\sum_{k \in G_i} S_k^g - \sum_{k \in L_i} S_k^d - \sum_{k \in S_i} (Y_k^s)^* |V_i|^2 = \sum_{(i,j) \in E_i \cup E_i^R} S_{ij} \ , \forall i \in N}$$

Power limits in lines

$$\boxed{|S_{ij}| \leq s_{ij}^u, \ \forall (i,j) \in E \cup E_R}$$

Current limits in lines

$$\boxed{|I_{ij}| \leq i_{ij}^u, \ \forall (i,j) \in E \cup E_R}$$

Voltage angle diffs. limits

$$\boxed{\theta_{ij}^{\Delta l} \leq \angle (V_i V_j^*) \leq \theta_{ij}^{\Delta u}, \ \forall (i,j) \in E}$$

CPES-QSM: Integrate the cyber-status into the operational decisions (OPFs) of the physical system.

Now, let's see how we use the **CPES-QSM** to 'alter' the OPF of a CPES.

Cyber-Constrained ACOPF

$$
\begin{aligned}
\min \quad & C(x) \\
\text{s.t.} \quad & G(x) = 0 \\
& \boxed{H(x) \leq l} \\
& x_{min} \leq x \leq x_{max}
\end{aligned}
\quad \longrightarrow \quad
\begin{aligned}
& (1-\zeta)P_k^{gl} \leq P_k^g \leq \alpha P_k^{gu}, \ \forall k \in G \\
& (1-\zeta)Q_k^{gl} \leq Q_k^g \leq \alpha Q_k^{gu}, \ \forall k \in G
\end{aligned}
$$

$$
\alpha(\rho, CQ_k, \zeta) = \begin{cases} 0, & \text{if } CQ_k \geq \rho \text{ for } \zeta = 1 \\ (\frac{P_k^{gl}}{P_k^{gu}}, 1), & \text{if } CQ_k \geq \rho \text{ for } \zeta = 0 \\ 1, & \text{if } CQ_k < \rho \text{ for } \zeta = 0 \end{cases}
$$

CPES-QSM

new cyber-physical variables

ρ - *Threshold defined by experts/user. If CPES-QSM is higher, then node is considered '**unreliable**'*

α - *Value that adjust the upper generation of the 'unreliable' generator*

ζ - *Binary variable that determines if generator k must be disabled or just curtailed (adjust generation)*

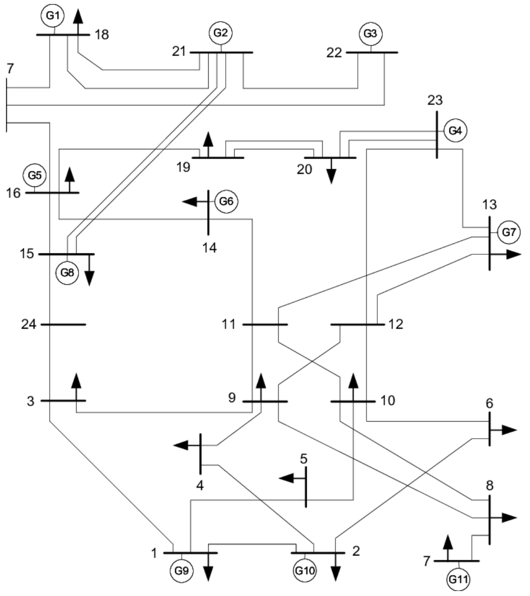
CPES-QSM: Integrate the cyber-status into the operational decisions (OPFs) of the physical system.

- By ***Cyber-constraining*** the generation in 'unreliable' nodes, the OPF solution provides a **more 'secure' solution**
- **The new solution** relies on the generation of more **reliable nodes** at the **cost of more expensive generation** that yields a **higher traditional cost**
- The final **Cyber-Constrained ACOPF (C-ACOPF) solution** makes the CPES **more secure** in terms of cyber-physical security **while sacrificing cost**

Co-Optimization of Cyber-Physical Energy Systems (CPES) – Cyber-Constrained ACOPF

Experimental Setup

IEEE RTS-24



Test #1

Traditional ACOPF (T-ACOPF)
vs.
Cyber-Constrained ACOPF (C-ACOPF)

Test #2

Effects of Cyberattacks in T-ACOPF and C-ACOPF Formulations

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

Co-Optimization of Cyber-Physical Energy Systems (CPES) – Test #1: T-ACOPF vs. C-ACOPF

C-ACOPF Setup

Factors for CPES-QSM	'Expert' Weights
CRPI (x_1)	*0.26*
QCR-B (x_2)	*0.55*
VDI (x_3)	*0.61*
SVSI (x_4)	*0.65*
VCPI (x_5)	*0.66*

$$\lambda = -0.983$$

$2^5 = 32$ total ***fuzzy measures***

$$\upsilon(\{x_1, x_2\}) = 0.669$$
$$\upsilon(\{x_1, x_3\}) = 0.714$$
$$\upsilon(\{x_1, x_3\}) = 0.743$$
$$\vdots$$

Quantitative Cyber Risk Base Model (QCR-B)
Probability and Impact

Cyber Layer :

Bus #15 (Gen #5): {AV: *Network*, PR: *None*, AC: *Low*, UI: *None*} ***unreliable***
Other buses: {AV: *Local*, PR: *High*, AC: *High*, UI: *Required*} ***reliable***

****OPF optimizations are solved using PandaPower solver (i.e., the primal-dual interior point method from the Python Interior Point Solver (PIPS))***

[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

Co-Optimization of Cyber-Physical Energy Systems (CPES) – Test #1: T-ACOPF vs. C-ACOPF Results

T-ACOPF

Cost = $49,903.54

Gen #	Bus #	P (MW)	Q (MVAR)	$\|V\|_{pu}$	$\angle V$
0	0	192.00	13.42	1.050	-7.38
1	1	192.00	10.86	1.050	-7.47
2	6	131.60	66.68	1.022	-17.84
3	13	0.00	172.03	1.049	1.02
4	14	215.0	110.00	1.042	10.03
5	15	155.00	80.00	1.046	8.98
6	17	400.00	69.02	1.050	14.83
7	20	400.00	-12.42	1.050	15.64
8	21	300.00	-39.00	1.050	21.27
9	22	660.00	70.37	1.050	9.80
10 (slack)	12	258.54	53.05	1.020	0.00

C-ACOPF

Cost = $53,621.13

Gen #	Bus #	P (MW)	Q (MVAR)	$\|V\|_{pu}$	$\angle V$
0	0	192.00	12.55	1.050	-8.33
1	1	192.00	10.54	1.050	-8.40
2	6	141.64	64.54	1.024	-17.76
3	13	0.00	146.10	1.044	-0.79
4	14	215.0	110.00	1.042	7.47
5	15	54.30	80.00	1.044	6.32
6	17	400.00	73.54	1.050	12.22
7	20	400.00	-10.61	1.050	13.05
8	21	300.00	-38.39	1.050	18.67
9	22	660.00	68.44	1.050	8.40
10 (slack)	12	344.70	43.15	1.021	0.00

****OPF optimizations are solved using PandaPower solver (i.e., the primal-dual interior point method from the Python Interior Point Solver (PIPS))***

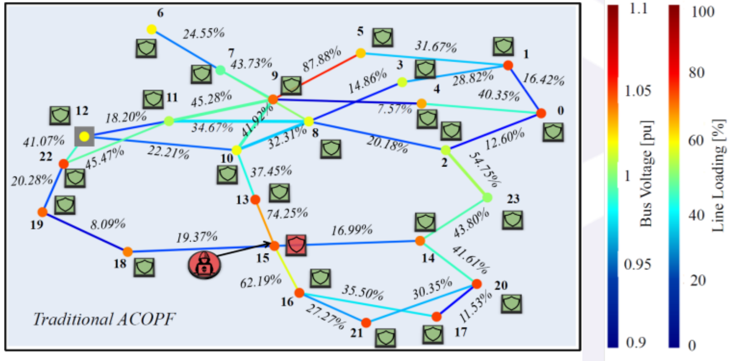
[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

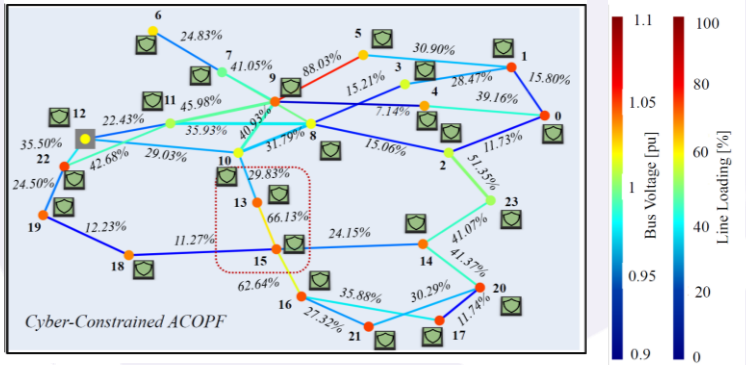
Co-Optimization of Cyber-Physical Energy Systems (CPES) – Test #1: T-ACOPF vs. C-ACOPF Results

$\rho = 0.2$

CPES-QSM

Bus #	CRPI		QCR-B		VDI		SVSI		VCPI		*CQ*	
Case	T	C	T	C	T	C	T	C	T	C	T	C
0	0.11	0.11	0.0	0.0	0.05	0.05	0.0	0.0	0.0	0.0	0.05	0.05
1	0.22	0.22	0.0	0.0	0.05	0.05	0.0	0.0	0.0	0.0	0.08	0.08
2	0.12	0.12	0.03	0.03	0.01	0.01	0.02	0.0	0.01	0.01	0.05	0.04
3	0.11	0.11	0.02	0.02	0.02	0.02	0.01	0.0	0.02	0.02	0.04	0.04
4	0.11	0.11	0.01	0.01	0.03	0.03	0.01	0.01	0.01	0.01	0.05	0.05
5	0.47	0.47	0.02	0.01	0.03	0.03	0.01	0.01	0.02	0.02	0.14	0.14
6	0.09	0.09	0.01	0.01	0.05	0.05	0.0	0.0	0.03	0.03	0.04	0.04
7	0.11	0.11	0.02	0.02	0.01	0.01	0.02	0.02	0.03	0.03	0.05	0.05
8	0.12	0.12	0.03	0.03	0.02	0.02	0.01	0.01	0.01	0.01	0.04	0.04
9	0.47	0.47	0.03	0.03	0.05	0.05	0.03	0.03	0.02	0.02	0.15	0.15
10	0.19	0.19	0.03	0.03	0.02	0.02	0.01	0.01	0.02	0.02	0.07	0.07
11	0.40	0.40	0.02	0.02	0.01	0.01	0.0	0.0	0.02	0.02	0.12	0.12
12	0.53	0.53	0.01	0.01	0.02	0.02	0.0	0.0	0.0	0.0	0.15	0.15
13	0.23	0.23	0.0	0.0	0.04	0.04	0.0	0.0	0.01	0.01	0.08	0.08
14	1.0	1.0	0.02	0.0	0.04	0.04	0.0	0.0	0.0	0.0	0.27	0.27
15	0.50	0.50	0.20	0.07	0.05	0.04	0.0	0.0	0.0	0.0	0.21	0.16
16	0.41	0.41	0.02	0.02	0.05	0.05	0.03	0.03	0.0	0.0	0.13	0.13
17	0.1	0.1	0.02	0.02	0.05	0.05	0.0	0.0	0.0	0.0	0.05	0.05
18	0.50	0.50	0.02	0.02	0.04	0.04	0.03	0.02	0.0	0.0	0.15	0.15
19	0.1	0.1	0.02	0.02	0.04	0.04	0.03	0.03	0.0	0.0	0.05	0.05
20	0.31	0.31	0.04	0.04	0.05	0.05	0.0	0.0	0.0	0.0	0.10	0.10
21	0.14	0.14	0.0	0.0	0.05	0.05	0.0	0.0	0.0	0.0	0.06	0.06
22	0.53	0.53	0.02	0.02	0.05	0.05	0.0	0.0	0.01	0.01	0.16	0.16
23	1.0	1.0	0.02	0.02	0.01	0.01	0.01	0.01	0.02	0.02	0.27	0.27





[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

Co-Optimization of Cyber-Physical Energy Systems (CPES) – Test #2: Effects of Cyberattacks T-ACOPF vs. C-ACOPF

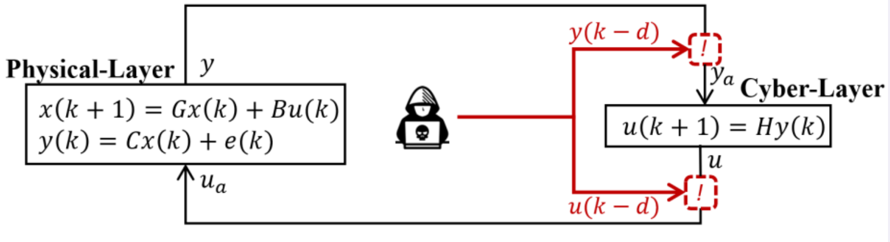
Data Availability Attack (DAA) threat

capable of exploiting the vulnerabilities of the affected node(s) by making them unresponsive via the delay of control and measurements

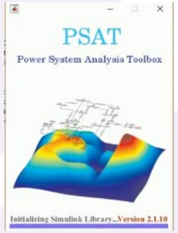
Threat Model [3]

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

Time delay attack that targets **Generator at bus #15**, by making it **inoperable** for **5 seconds**



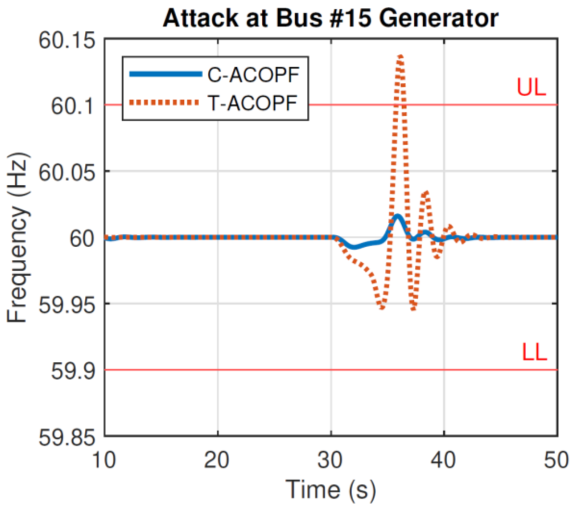
The **time-domain simulation** of the **IEEE RTS-24 test system** used for this analysis is performed using the **Power System Analysis Toolbox (PSAT)**



[3] I. Zografopoulos, J. Ospina, X. Liu and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," in IEEE Access, vol. 9, pp. 29775-29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

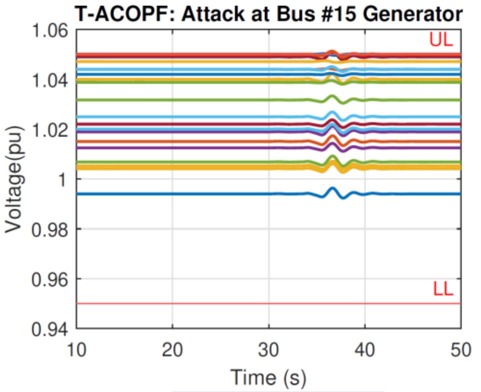
Co-Optimization of Cyber-Physical Energy Systems (CPES) – Test #2: Effects of Cyberattacks T-ACOPF vs. C-ACOPF Results

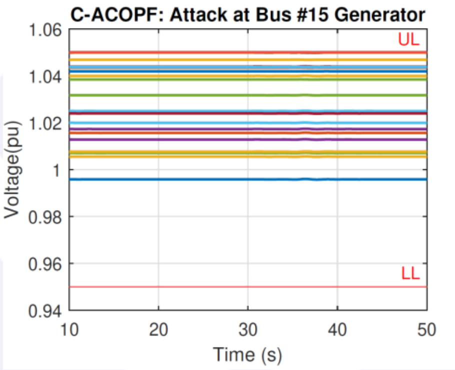
Frequency response



***Frequency response** comparison for both T-ACOPF and C-ACOPF solutions when a DAA cyberattack is used to compromise the generator at bus #15*

Voltage response





[1] J. Ospina, V. Venkataramanan and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," in *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3210402.

Conclusion

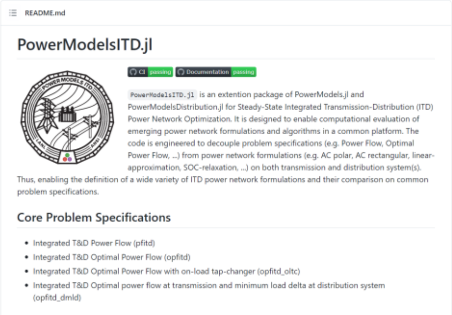
- There are ways to improve the (cyber) security of modern CPES
  - A quantitative cyber-physical security metric for CPES (**CPES-QSM**)
    - Provides a quantitative value to the **cyber** and **physical** status of the operating CPES
    - Considers various factors from the **Electrical**, **Cyber**, and **Graph-theory** domains.
  - A cyber-constrained ACOPF (C-ACOPF) formulation
    - Produces a **more secure operating point**
    - Considers **vulnerabilities existing in IoT, ICT, and OT**

Code available at:

https://gitlab.com/juanjospina/quantitative-cyber-metric

Future Work(s)

- **Exploring the scalability** of the **proposed approach** by
  - Evaluating its performance in **large-scale integrated transmission-distribution(T&D) systems** using tools such as ***PowerModelsITD.jl*.***
  - Explore the **stability** of the **CI** will be examined for the case when a **large number of factors** are considered simultaneously.


README.md

PowerModelsITD.jl

CI passing | Documentation passing

`PowerModelsITD.jl` is an extention package of PowerModels.jl and PowerModelsDistribution.jl for Steady-State Integrated Transmission-Distribution (ITD) Power Network Optimization. It is designed to enable computational evaluation of emerging power network formulations and algorithms in a common platform. The code is engineered to decouple problem specifications (e.g. Power Flow, Optimal Power Flow, ...) from power network formulations (e.g. AC polar, AC rectangular, linear-approximation, SOC-relaxation, ...) on both transmission and distribution system(s). Thus, enabling the definition of a wide variety of ITD power network formulations and their comparison on common problem specifications.

Core Problem Specifications

- Integrated T&D Power Flow (pfitd)
- Integrated T&D Optimal Power Flow (opfitd)
- Integrated T&D Optimal Power Flow with on-load tap-changer (opfitd_oltc)
- Integrated T&D Optimal power flow at transmission and minimum load delta at distribution system (opfitd_dmld)

* https://github.com/lanl-ansi/PowerModelsITD.jl

Thank you for your time.

Questions?

Contact:

Email(s):

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