Integrated Cybersecurity for Power Grid with Inverter-Based Resources

ALI MEHRIZI-SANI

ASSOCIATE PROFESSOR

Resilient Renewable Energy Grid Adaptation Laboratory (REGAL)

Contributing Students:

Ardavan Mohammadhassani, Brady Alexander, Victor Mukora

VT-MPR SEMINAR

March 2023

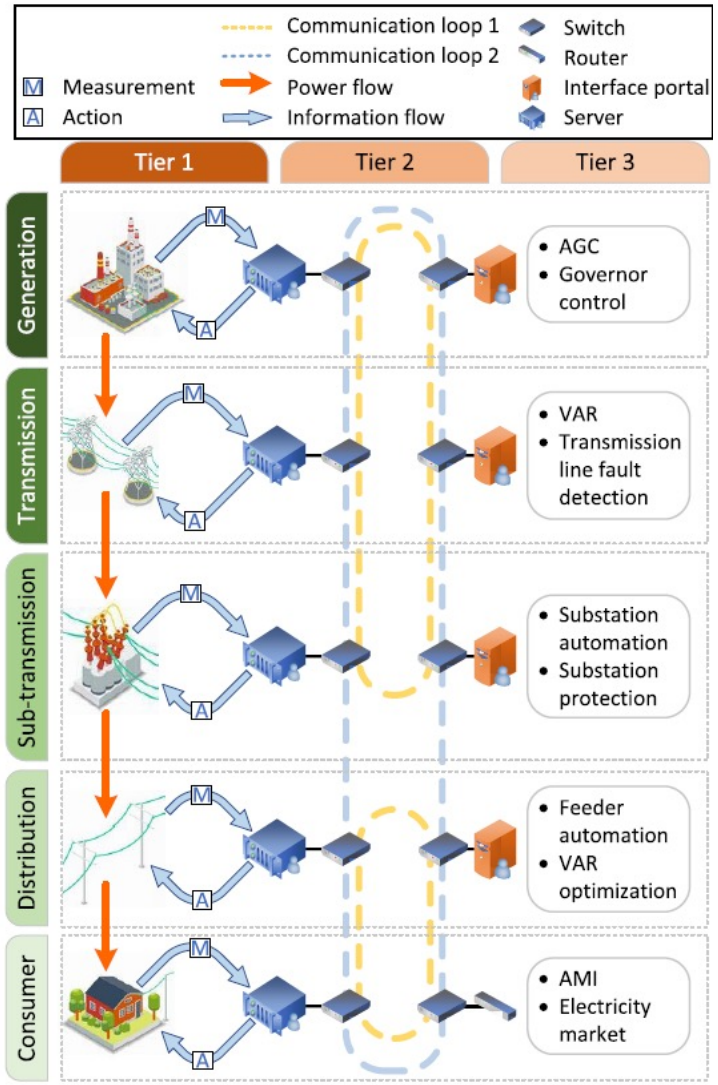
VIRGINIA TECH

POWER AND ENERGY CENTER

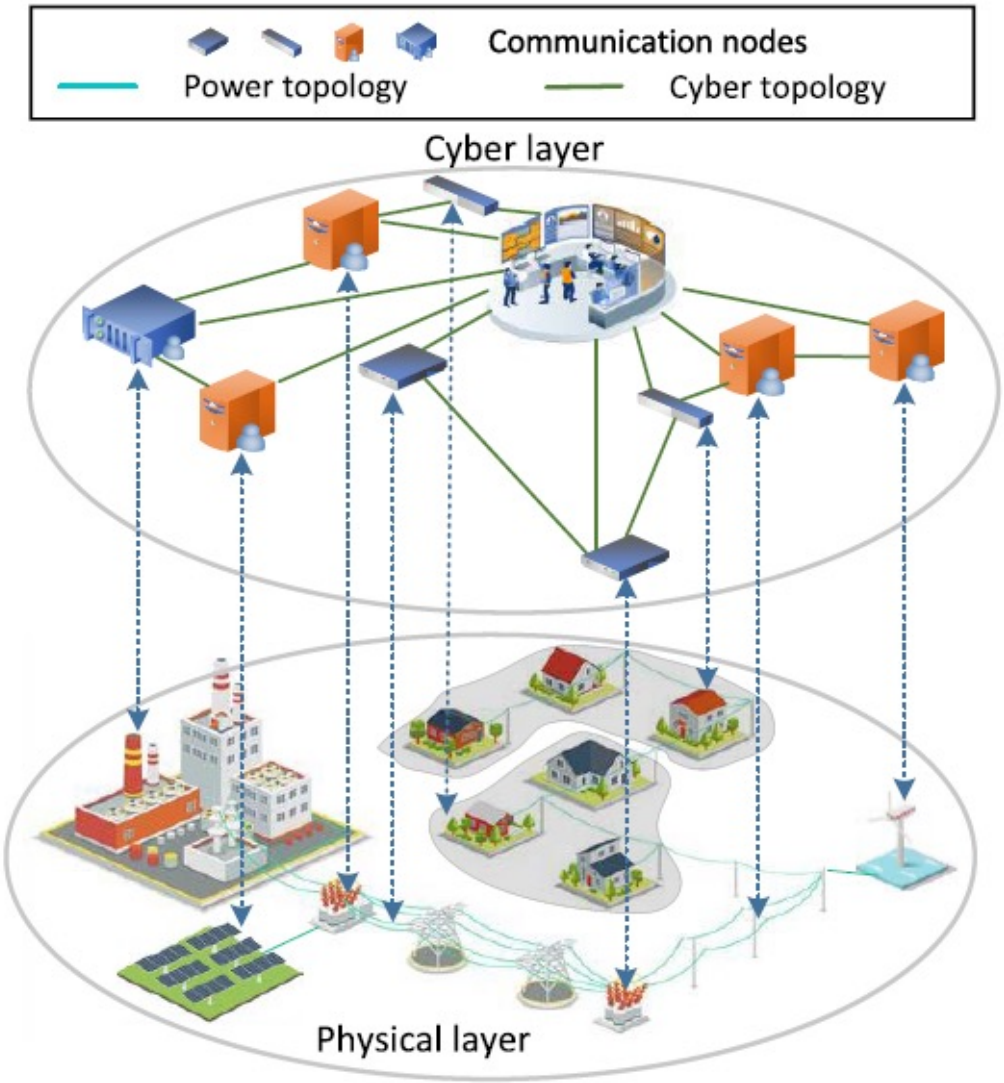
Bradley Department of ECE

his work is supported in part by UNIFI Consortium, in part by Virginia's Commonwealth Cyber Initiative (CCI), in part by NSF award CPS-1837700 .

Cyber-Physical Power System



Structure



One-to-One Mapping

M. Abdelmalak, V. Venkataramanan and R. Macwan, "A survey of cyber-physical power system modeling methods for future energy systems," IEEE Access, vol. 10, 2022.

Cyber-Physical Microgrid

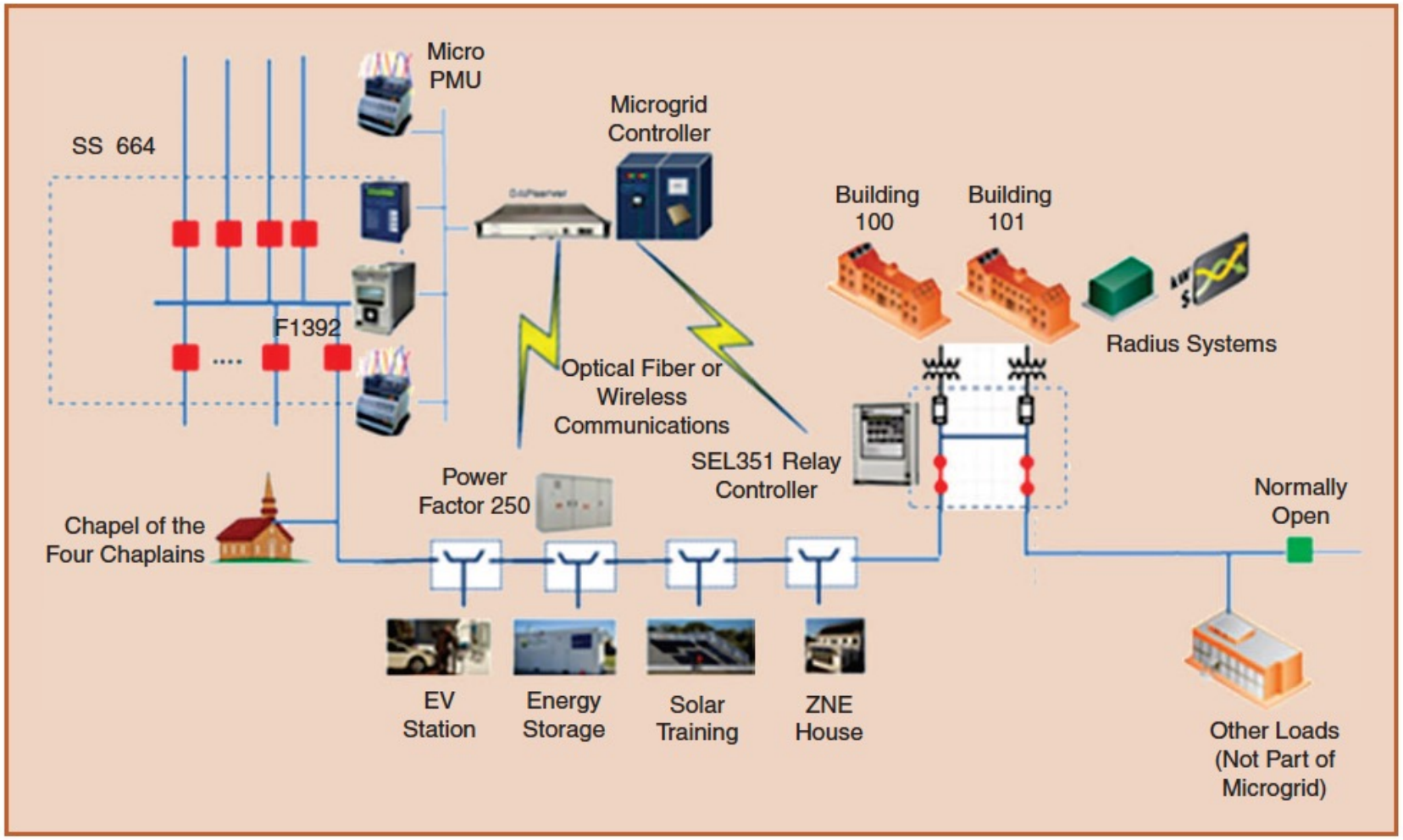


table 1. A summary of loads on GridSTAR microgrid.

Microgrid Assets and Load	Microgrid System	Load (kW) Average Demand	Load (kW) Controllable Load
ZNE House	GridSTAR	4	2
Electric vehicle charging	GridSTAR	10	10
Solar grid storage (RT efficiency)	GridSTAR	20	20
Building 101	GridSTAR	150	75
Building 100	GridSTAR	160	50
Chapel	GridSTAR	16	0
Total		360	187

R. Uluski, J. Kumar, S. S. M. Venkata, D. Vishwakarma, K. Schneider, A. Mehrizi-Sani, R. Terry, and W. Agate, "Microgrid controller design, implementation and deployment–Experiences at The Navy Yard Community at Philadelphia: A journey from conception to implementation," *IEEE Power and Energy Magazine*, vol. 15, no. 4, pp. 50-62, Jul./Aug. 2017.

Cyber-Physical Security in the Power System

- As a cyber-physical system, the power grid is vulnerable to attacks on its structure. Attacks are malicious acts that exploit security vulnerabilities to disrupt power grid operation.
- Most attacks originate in the cyber system since it is more exposed and has more vulnerabilities. Physical attacks can also happen.
- It is imperative that the power grid is protected from cyberattacks to ensure its security and stability are maintained.

Year	Affected System	Type
2001	California ISO	Compromising web servers under development
2007	Estonia's critical infrastructure	Distributed denial of service (DDoS)
2011–	Several U.S. utilities	Exploiting human-machine interface (HMI) by BlackEnergy
2012	Unnamed U.S. Northeast utility	Possibly network scanning and botnets by UglyGorilla
2013–	Several U.S. utilities, vendors	Malware infection (trojan) by Havex
2013	PG&E in Coyote, CA	Telecom cables cut; snipers firing on 17 transformers at a substation (physical attack on the cyber-physical system)
2014	Unnamed U.S. utility	Remote access due to weak password
2015–16	Ukrainian power system	Malware installation, HMI hijacking, and DDoS to customer service

Data from various sources, including DOE's Electric Disturbance Events Annual Summaries at https://www.oe.netl.doe.gov/OE417_annual_summary.aspx. There were 75 sabotage/vandalism reports in 2022.

Cyber-Physical Vulnerabilities in the Power System

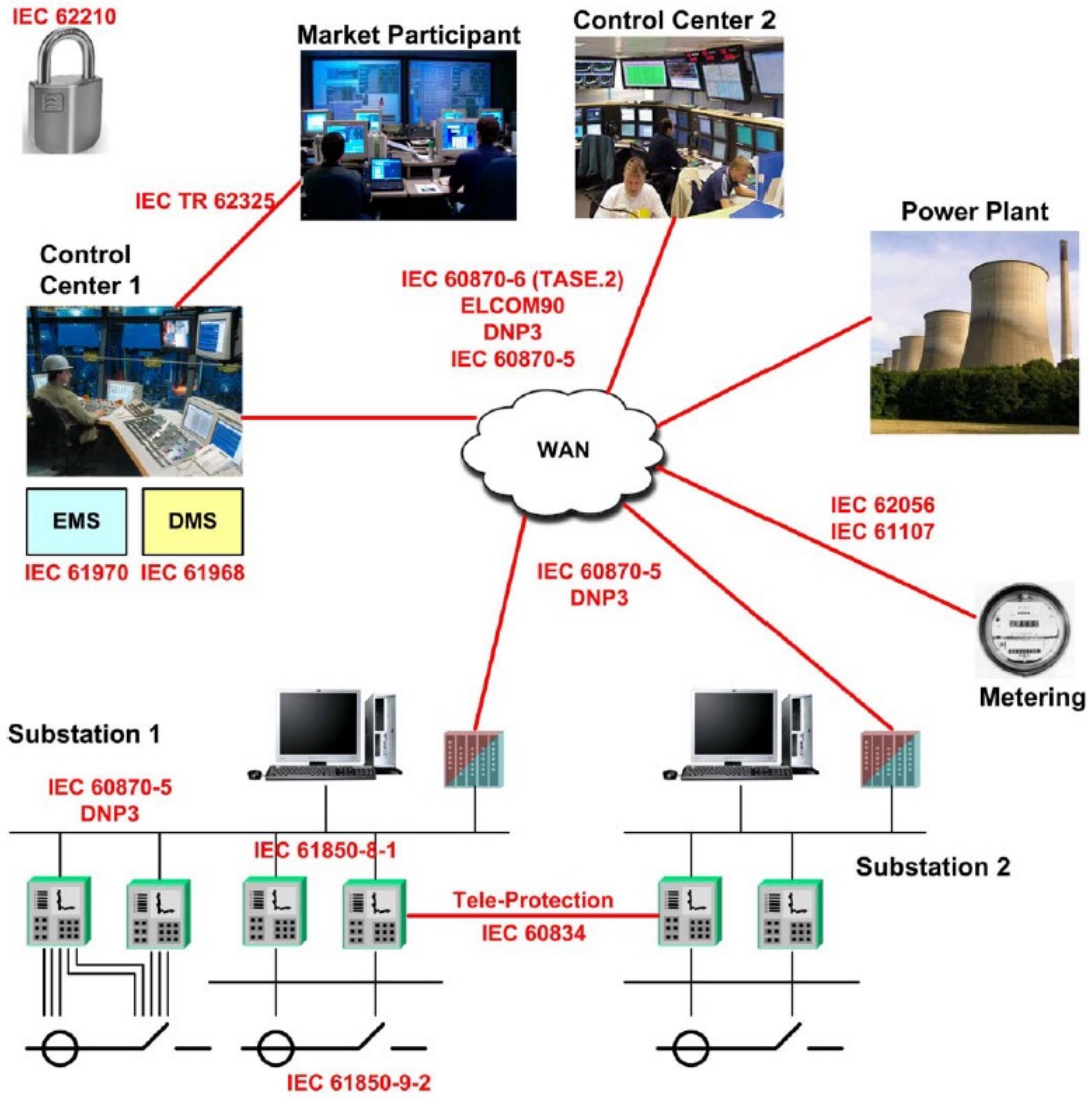
- A power system has vulnerabilities that combine vulnerabilities of the IT system and physical devices.
- The increasing number of vulnerabilities stem from different trends:
  - Wireless communication is gaining popularity for integrating scattered devices. Also, combining wired and wireless communication makes it difficult to design a robust and uniform policy for cybersecurity.
  - Aside from the disparate proprietary protocols, many devices and IBRs are starting to use open protocols such as IEC61850 and DNP3. These protocols have inherent vulnerabilities.
  - Increased communication via the internet can create extra vulnerabilities that can be exploited from the outside world.
  - Increasing internal pervasive communication results in several malicious attacks and unintentional errors.

Domain	Common Vulnerability
Application Software	Poor Code Quality
	Inadequate Configuration Management
	Poor Permissions and Access Management
	Inadequate Patch Management
	Inadequate Data Integrity Checking
	Inadequate Error Handling
	Inadequate Database Protection
Communication Network	Inadequate Segregation and Segmentation
	Inadequate Access Control
	Weak Intrusion Detection and Prevention
	Weak Encryption Mechanism
	Inadequate Sensitive Data Protection
	Inadequate Network Monitoring and Auditing
	Inadequate Anomaly Tracking
Field Devices	Unprotected Physical Access
	Improper Device Configuration
	Inadequate Firmware Protection
	Lack of Tamper-resistance Hardware
	Weak Authentication and Authorization

Z. Li, M. Shahidehpour and F. Aminifar, "Cybersecurity in Distributed Power Systems," Proceedings of the IEEE, vol. 105, no. 7, pp. 1367-1388, Jul. 2017.

Power System Communication Standards/Protocols

- Communication systems are typically designed to cover a subsystem (generation, transmission, and distribution) ather than the whole system.
- Communication exists in levels such as data sharing among the devices in a distribution substation to share data between the distribution system and the central controller. Typical devices for power system communication are smart meters, remote terminal units (RTU), and protective relays.
- Communication standards and protocols are primarily designed to enable interoperability among different devices from various vendors.
- The most common open protocols for power system communication are Modbus, DNP3, IEC 61850, OPC UA, TASE.2, IEC 60870-5-101, and IEC 60870-5-104. Power system entities may also use enterprise protocols and/or proprietary protocols.



S. Mohagheghi, J. Stoupis and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," IEEE/PES Power Systems Conference and Exposition, 2009, pp. 1-9.

Summary of Open Protocol Security Specifications

	Modbus	Modbus-F2009	Modbus-S2015	Modbus-A2018	OPC UA	TASE.2
Authentication	✗	Signature	Signature	Challenge-response	Password-based, X.509, WSS	✗
Authorization	✗	✗	✗	✗	✗	✗
Integrity	✗	SHA-2	SHA-2	Checksum	Signature	✗
Confidentiality	✗	✗	Encryption	Encryption	Encryption	✗

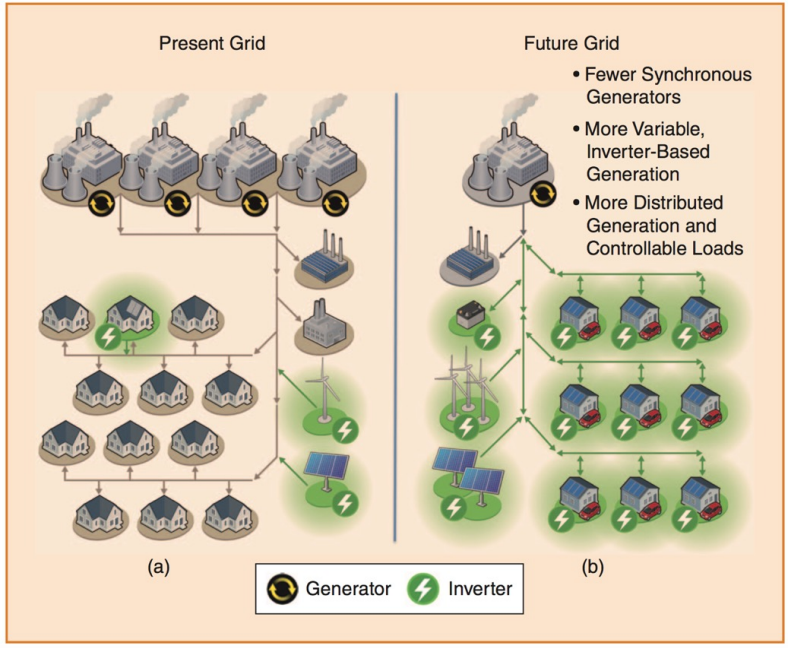
	DNP3	DNPSec	DNP3 SA	IEC 61850
Authentication	✗	HMAC	Challenge-response	✗
Authorization	✗	✗	✗	✗
Integrity	✗	SHA-1	SHA-2	Checksum
Confidentiality	✗	Encryption	✗	✗

A. Volkova, M. Niedermeier, R. Basmadjian and H. de Meer, "Security Challenges in Control Network Protocols: A Survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 619-639, Firstquarter 2019.

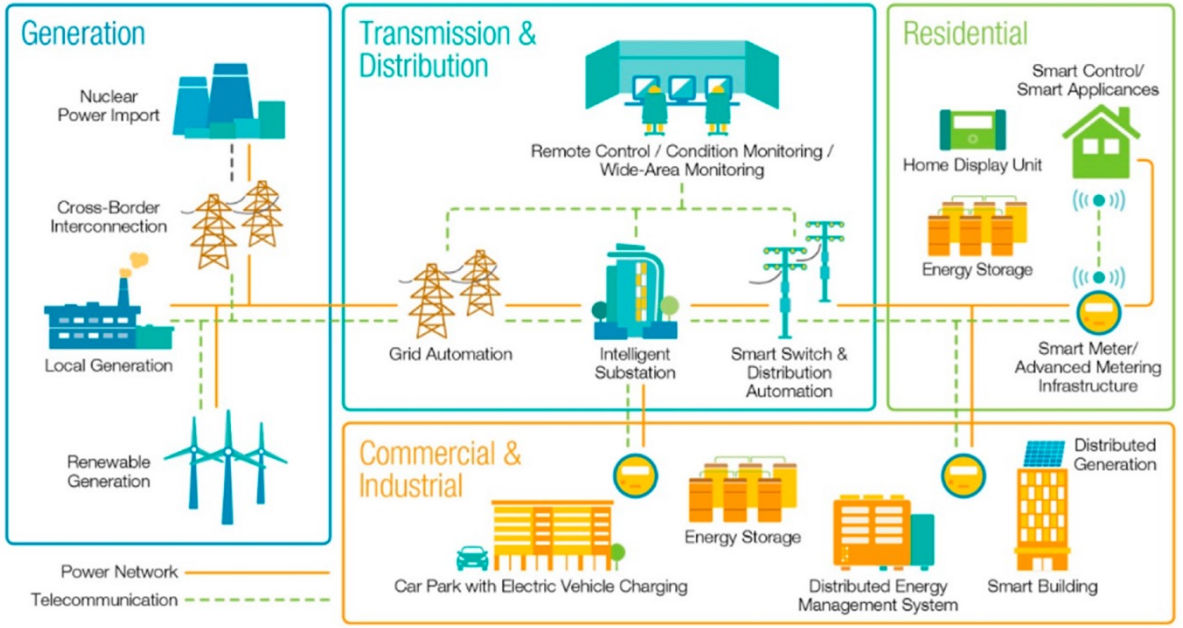
Toward a Decentralized, “Lots of X” Power System

- The power grid is becoming more decentralized:
  - More renewables are being integrated in the power grid: fewer synchronous generators and more IBRs.
  - Lack of inertia makes the grid more sensitive to disturbances.
  - Fast and reliable communication systems are necessary for stable operation and control of the grid.

- The increased amount of communication as well as more IBRs means that the cyber-physical attack surface of the grid is increasing.

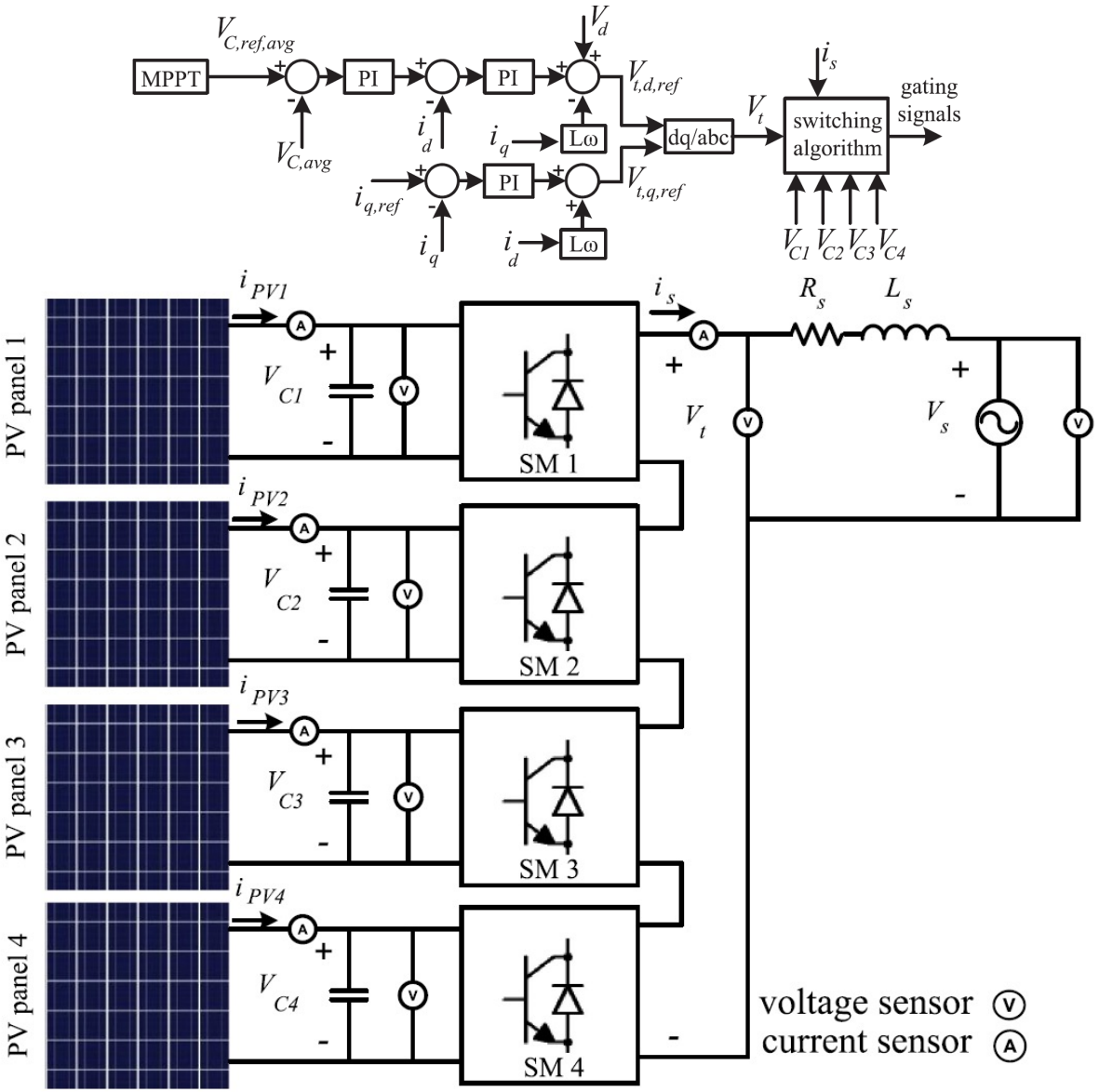


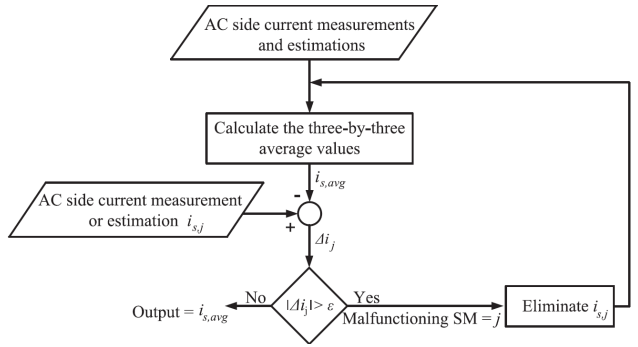
B. Kroposki, B. Johnson;,Y. Zhang, et al., “Achieving a 100% renewable grid,” Power & Energy M., 2017.



D. Muyizere, L. K. Letting, and B. B. Munyazikwiye, “Effects of communication signal delay on the power grid: A review,” Energies, vol. 11, no. 6, Mar. 2022.

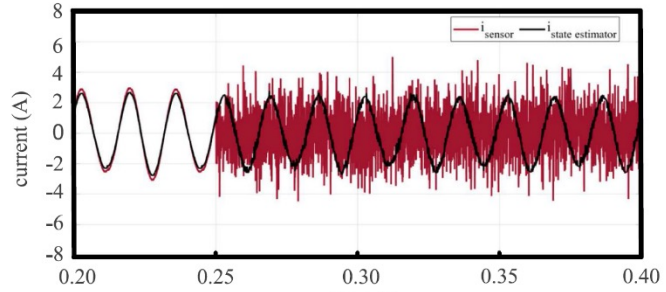
Sensor Attacks on CHB-Based IBRs



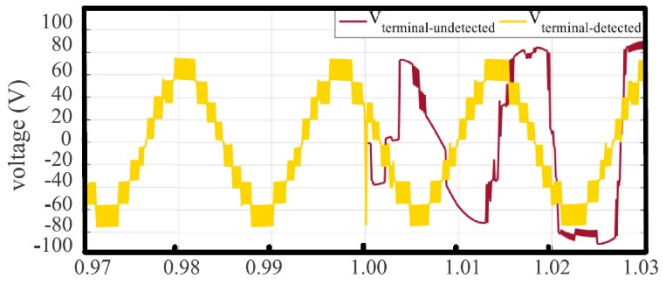


$$V_{C,j,calc} = \frac{V_t - \sum_{i=1,i\neq j}^{4} M_i V_{C,i}}{M_j}$$

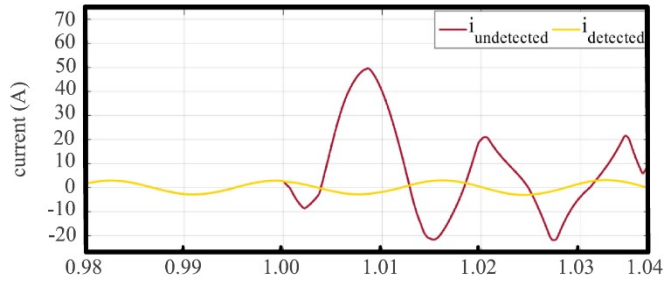
$$i_{PV,j,calc} = C_j \frac{dV_{C,j}}{dt} + M_j i_s$$



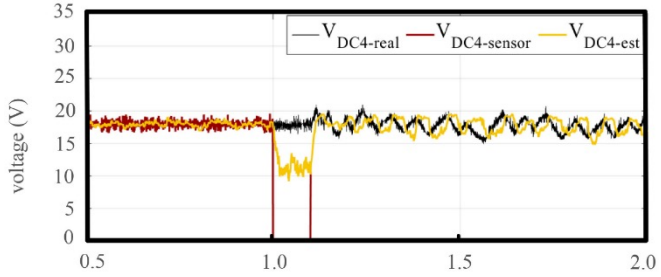
Corrected and uncorrected AC current after an attack on the AC current sensor.



Corrected and uncorrected AC voltage after an attack on DC voltage sensor 4.



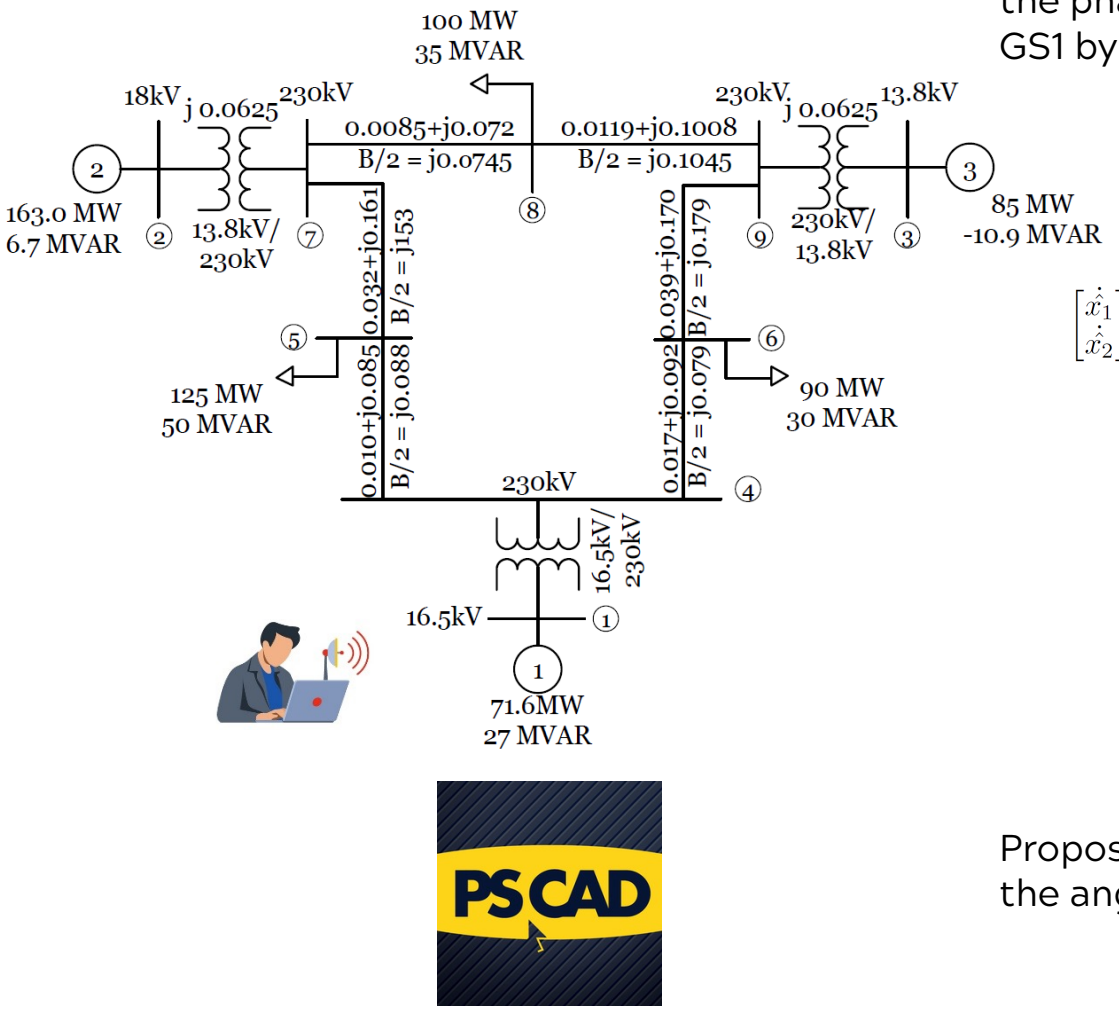
Corrected and uncorrected AC current after an attack on DC voltage sensor 4.



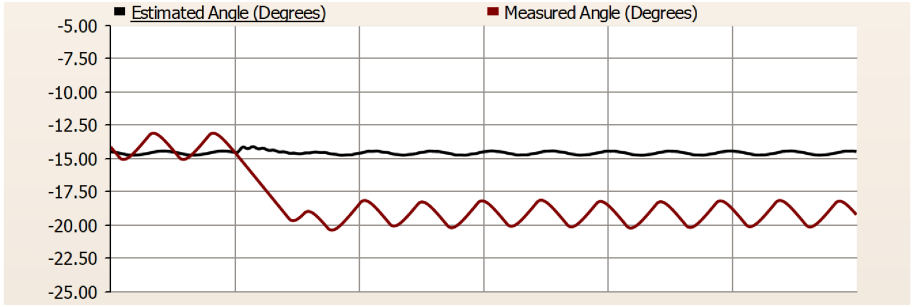
Corrected and uncorrected DC voltage after an attack on DC voltage sensor 4.

A. Teymouri and A. Mehrizi-Sani, “Sensor malfunction and mitigation strategy for a multilevel photovoltaic converter,” IEEE Trans. Energy Convers., vol. 35, no. 2, Jun. 2022.

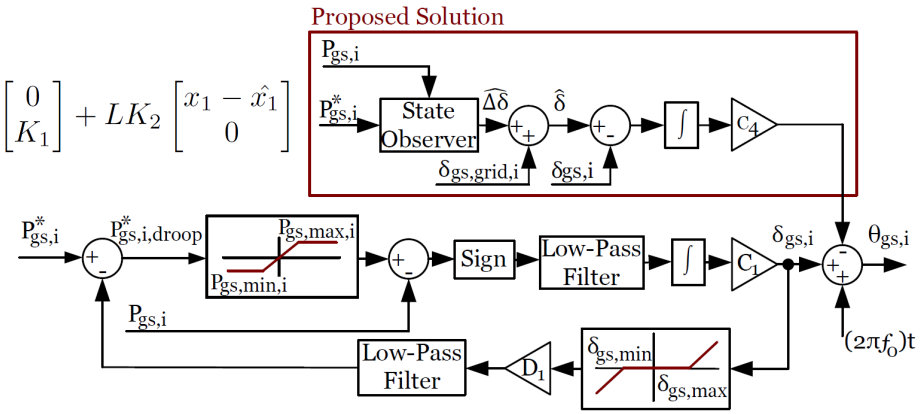
GPS Spoofing Attacks on Power Sharing for IBRs



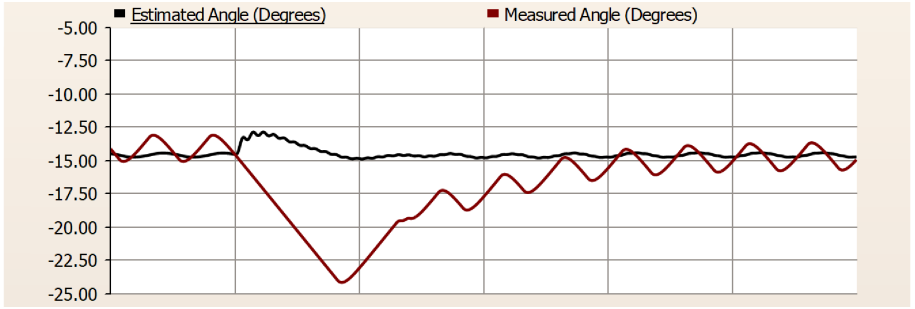
GPS spoofing attack shifts the phase reference for GS1 by about 5 degrees.



$$\begin{bmatrix} \dot{\hat{x}}_1 \\ \dot{\hat{x}}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -K_1K_2 & 0 \end{bmatrix} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \end{bmatrix} + P^*_{gs,i} \begin{bmatrix} 0 \\ K_1 \end{bmatrix} + LK_2 \begin{bmatrix} x_1 - \hat{x}_1 \\ 0 \end{bmatrix}$$



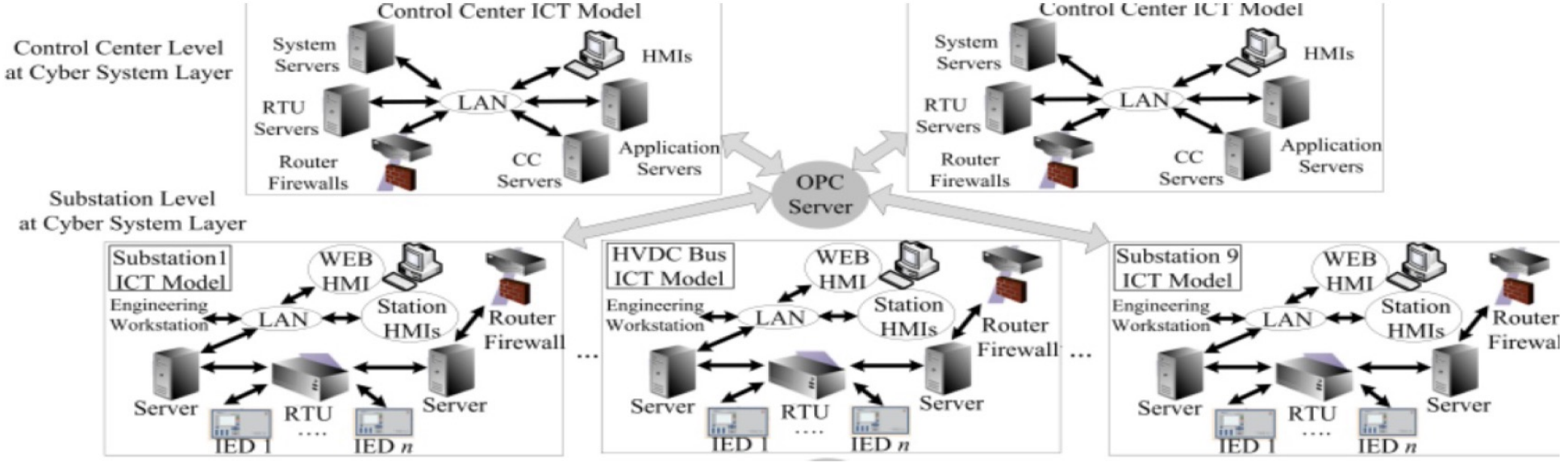
Proposed solution corrects the angle at GS 1.

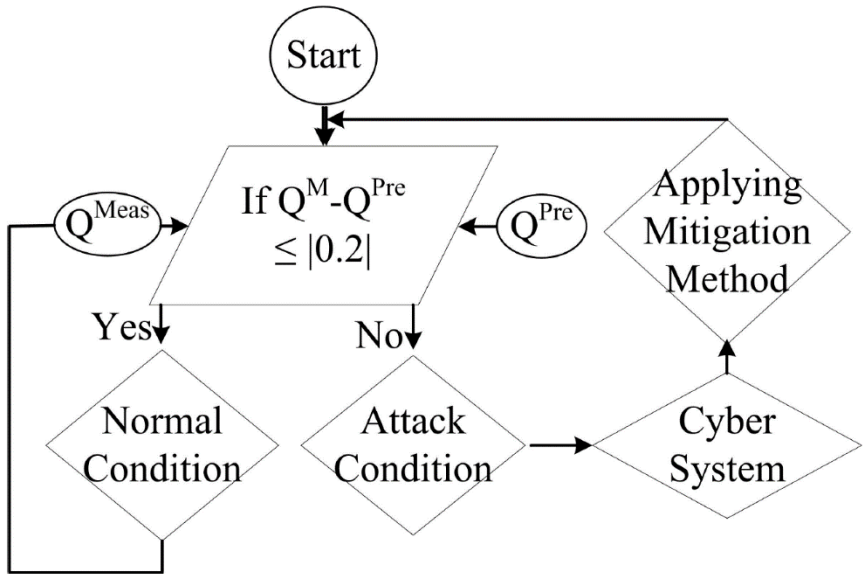


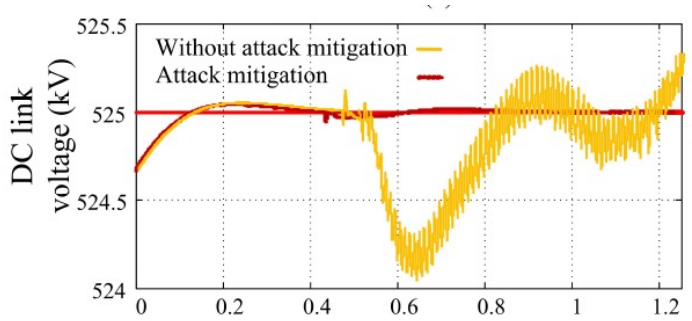
B. Alexander, A. Mohammadhassani, and Ali Mehrizi-Sani, “Resilient Power Sharing in a 100% Inverter-Based Power System Under GPS Spoofing Attacks,” IEEE Power Energy Soc. General Meeting (PESGM), 2023.

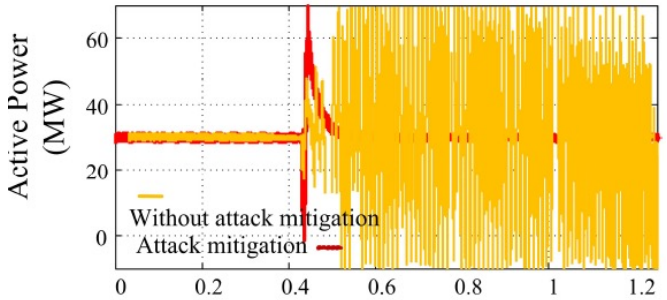
T. Meyers and B. Mather, "Empirical evaluation of GPS clock accuracy for isochronous droop-based inverters," IEEE Energy Convers. Cong. Expo. (ECCE), 2021.

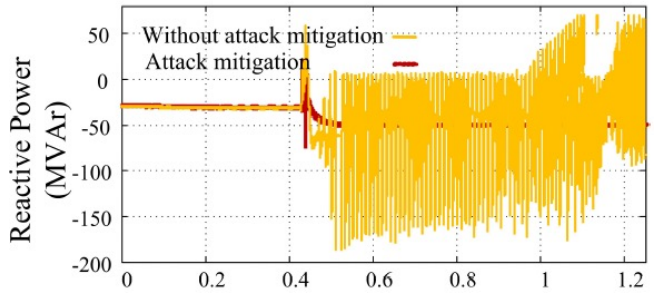
Cyber Vulnerability and Security in HVDC







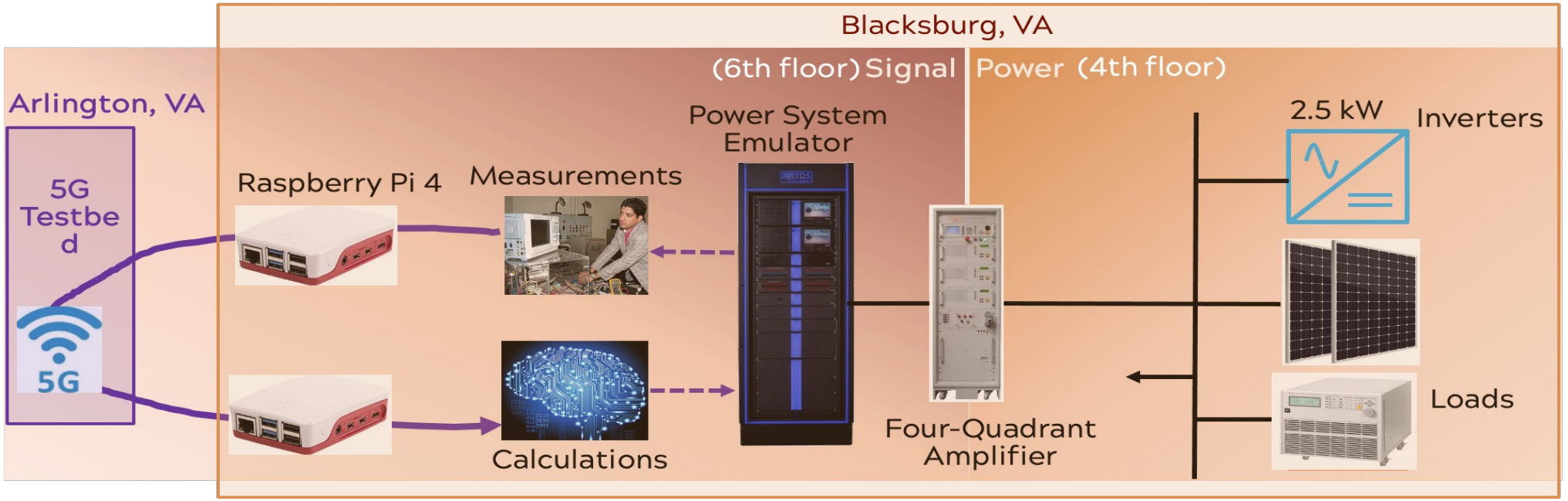




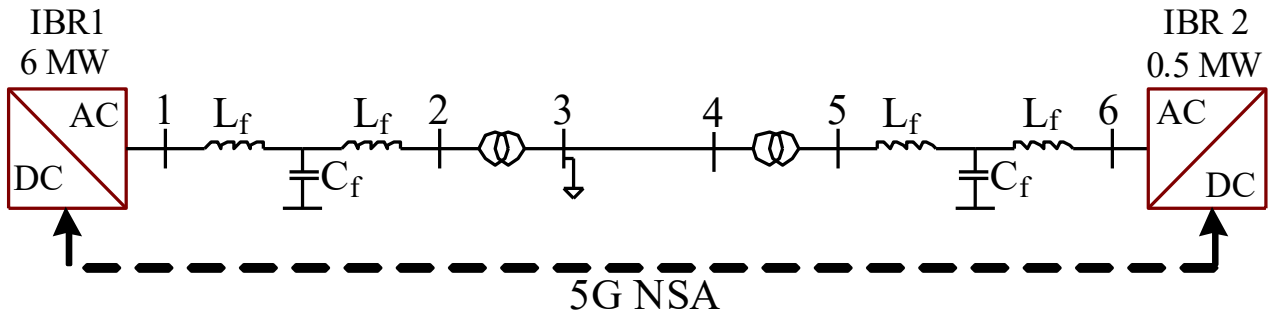
A. Gholami, M. Mousavi, A. K. Srivastava, and A. Mehrizi-Sani, "Cyber-physical vulnerability security analysis of power grid with HVDC line," North American Power Symp. (NAPS), 2019.

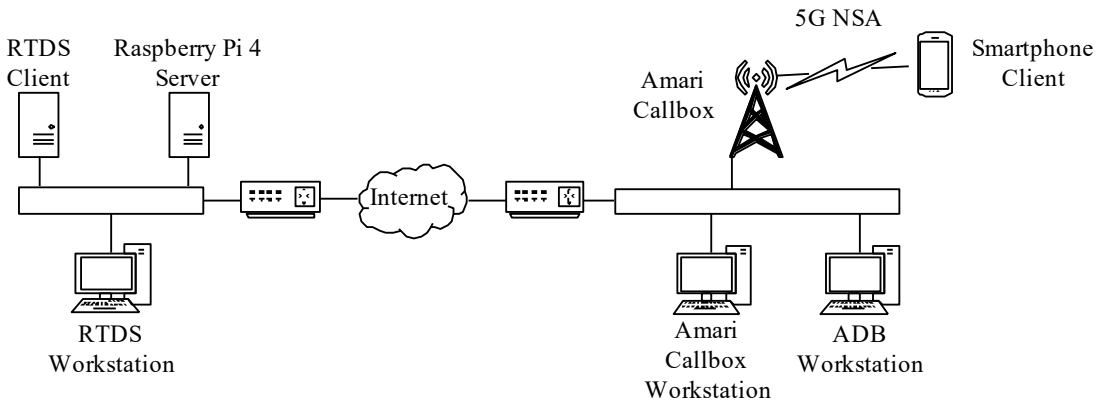
VT Power Grid Testbed for Cybersecurity Design

- The power grid testbed at VT provides various capabilities to design high-performance and cybersecure control systems for inverter-based power systems.
- This testbed consists of a real-time simulation setup using RTDS units offering communication via protocols such as Modbus, DNP3, and IEC 61850, which is connected to a microgrid testbed consisting of devices such as inverters via four-quadrant amplifier as well as a 5G testbed in Arlington, VA.
- Cyber risk assessment using the VT power grid testbed allows for the design of secure communication protocols to and cybersecure controllers to minimize the risk and maximize the performance of the power system.

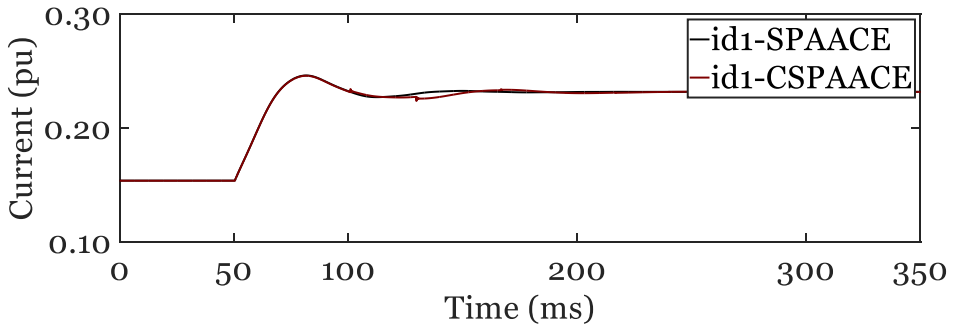


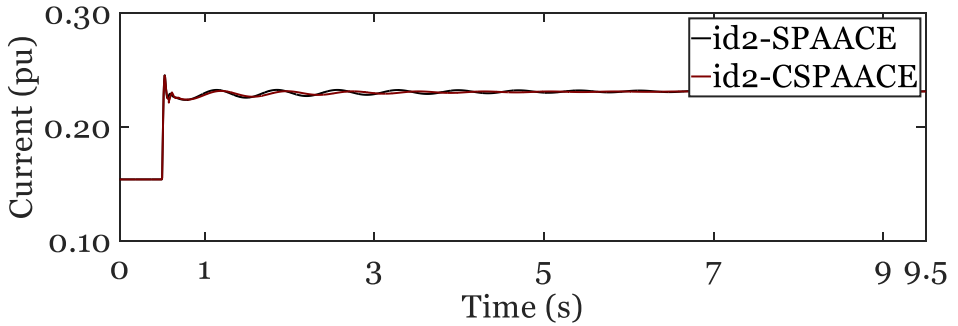
5G Communication in the VT Power Grid Testbed:





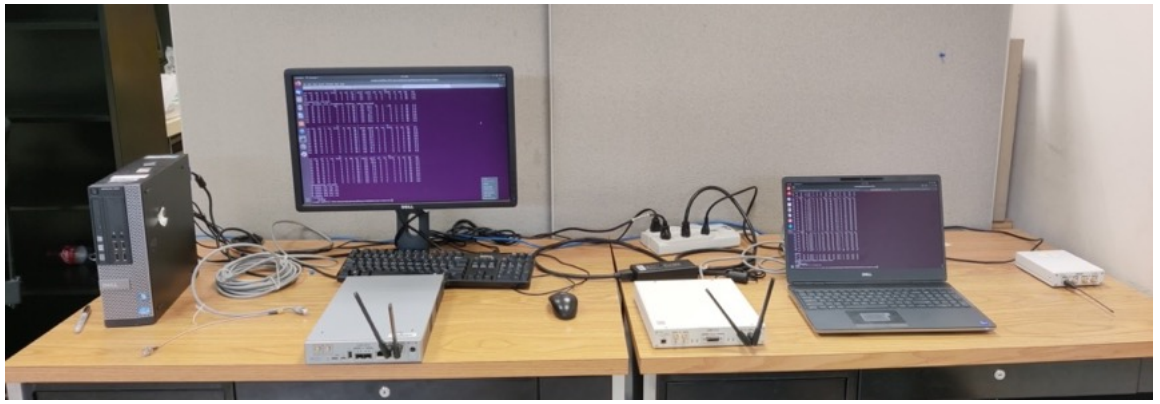
- The 5G testbed at the Commonwealth Cyber Initiative (CCI) is used to provide 5G non-standalone (NSA) connectivity to RTDS.
- The 5G user equipment (UE) is a Samsung Galaxy S20 phone, while the testbed base station is emulated using Amari Callbox technology.
- A TCP/IP interface is designed using socket programming to connect the UE to RTDS and establish duplex communication.
- A client program is designed for the UE in JAVA while a server program is designed for RTDS in Python.
- The minimum roundtrip latency is 28 ms.

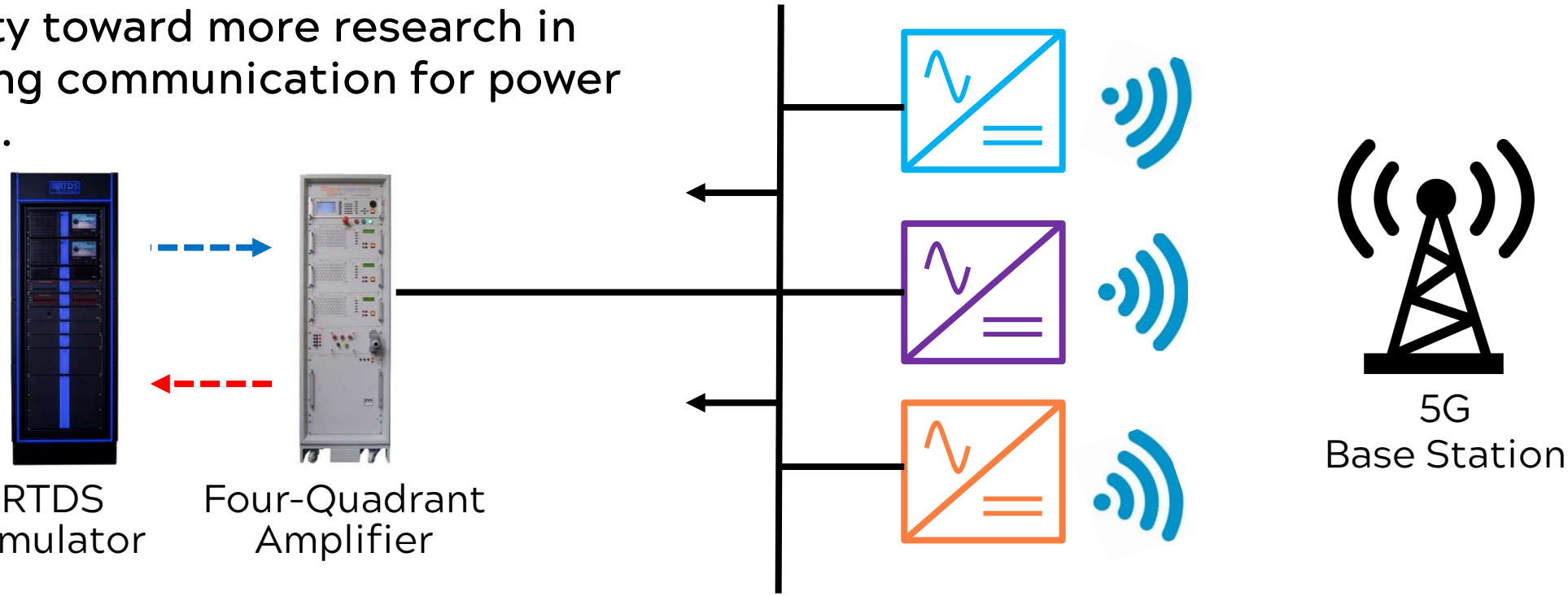




5G Communication in the VT Power Grid Testbed

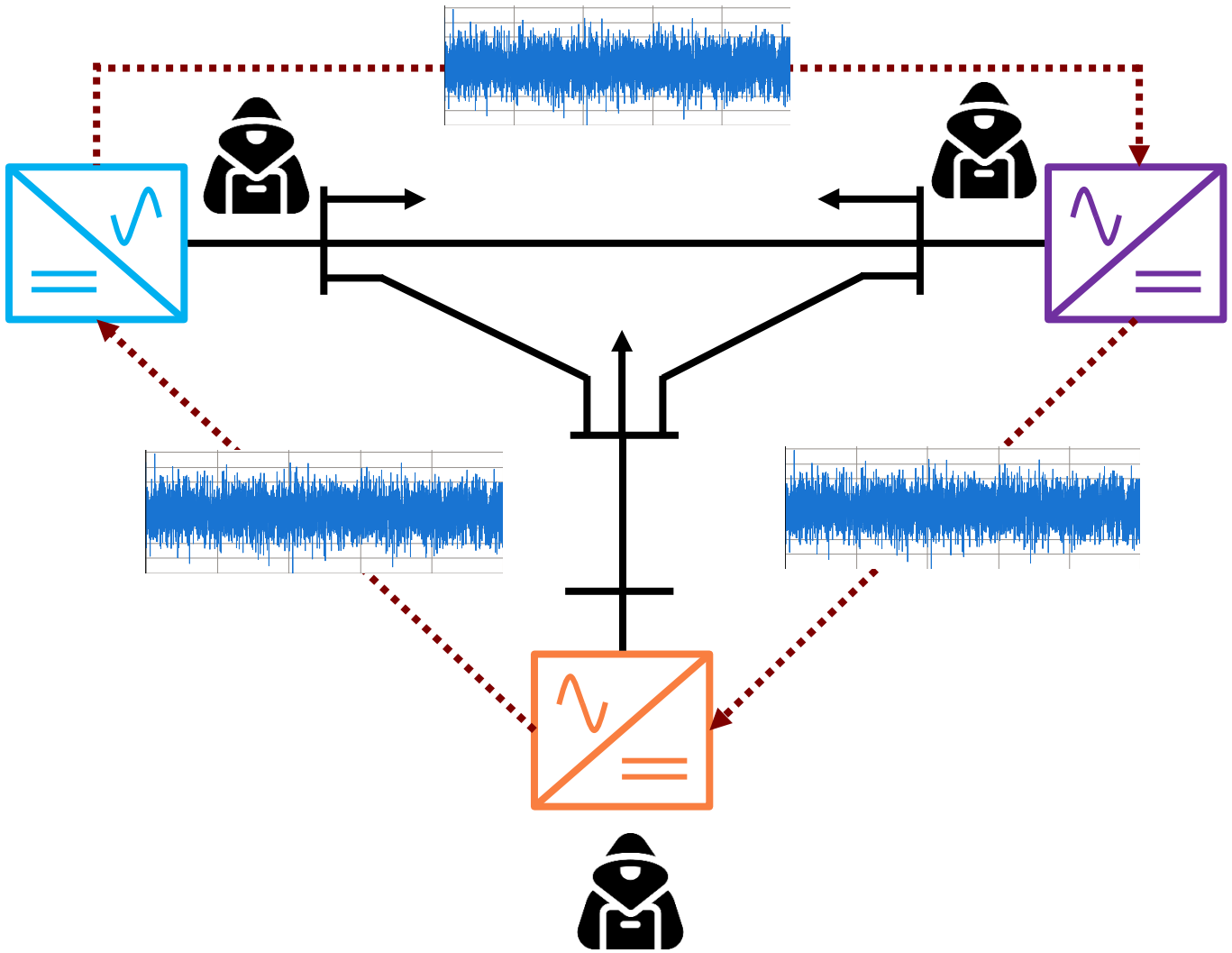
- An in-house 5G testbed is under development by Wireless@VT, which can be used for direct connection between devices in the VT Power Grid testbed.
- This 5G testbed provides more functionalities than the CCI testbed as well as a lower latency and more flexibility toward more research in improving communication for power systems.





Ongoing Research: Signal Reconstruction for Control

- In distributed control, IBRs communicate signals to improve system performance.
- The communicated signals typically have a similar shape during microgrid disturbances.
- 5G-based distributed control can become victim to noisy operating conditions, which can be caused by environmental conditions or cyber attacks.
- These disturbed signals can be properly reconstructed to correct signals by using autocorrelation and cross-correlation-based measurements.



Ongoing Research: Signal Reconstruction for Control

Algorithm 1: SDP-based Reconstruction Algorithm.

Inputs: The autocorrelation and cross-correlation measurements b_m for $0 \leq m < M$, the signal lengths L_1 and L_2.

Outputs: Signal estimates $\hat{\mathbf{x}}_1$ and $\hat{\mathbf{x}}_2$.

- Obtain the $(L_1 + L_2) \times (L_1 + L_2)$ matrix $\hat{\mathbf{X}}$ by solving

$$\begin{aligned} \text{find} \quad & \mathbf{X}, \\ \text{subject to} \quad & \text{trace}(\mathbf{A}_m \mathbf{X}) = b_m \text{ for } 0 \leq m < M, \\ & \mathbf{X} \succcurlyeq 0. \end{aligned} \tag{7}$$

- Calculate the best rank-one approximation of $\hat{\mathbf{X}}$ through SVD, and get $\hat{\mathbf{x}}\hat{\mathbf{x}}^\star$.
- Return $\hat{\mathbf{x}}_1 = (\hat{x}[0], \hat{x}[1], \ldots, \hat{x}[L_1 - 1])^T$ and $\hat{\mathbf{x}}_2 = (\hat{x}[L_1], \hat{x}[L_1 + 1], \ldots, \hat{x}[L_1 + L_2 - 1])^T$.

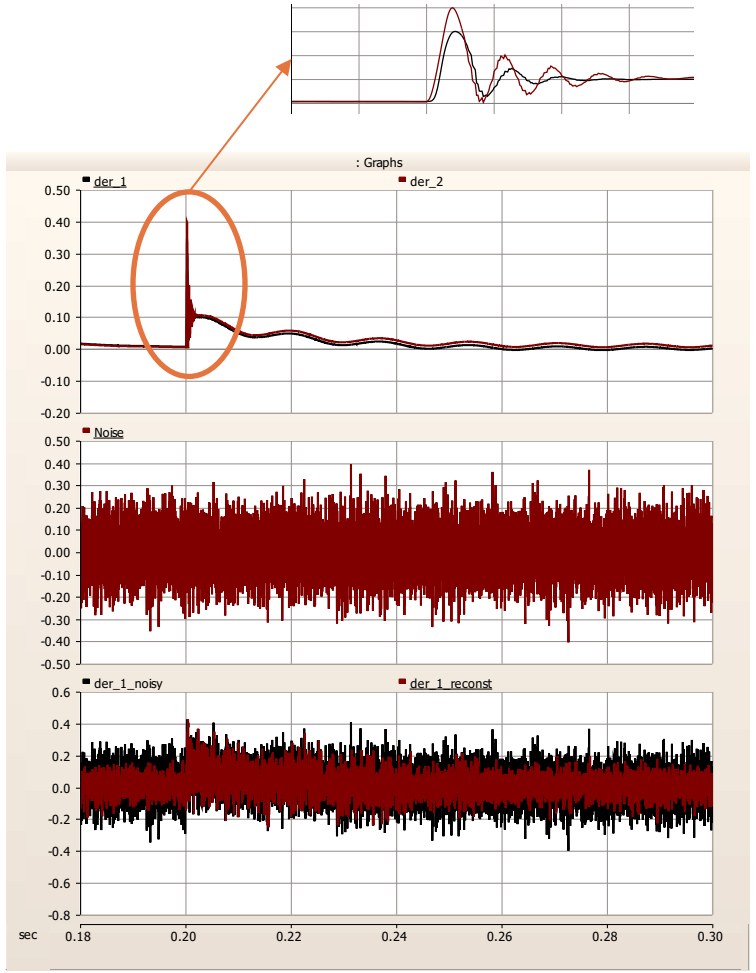
$$a_1[m] = \sum_{n=0}^{L_1-1} x_1[n] x_1^\star[n-m]$$

$$a_2[m] = \sum_{n=0}^{L_2-1} x_2[n] x_2^\star[n-m]$$

$$a_{12}[m] = \sum_{n=0}^{L_1-1} x_1[n] x_2^\star[n-m]$$

$$a_{21}[m] = \sum_{n=0}^{L_2-1} x_2[n] x_1^\star[n-m]$$

- In our work, semidefinite programming (SDP) is used to reconstruct noisy signals using their autocorrelation and cross-correlation measurements with locally measured signals and/or with each other.
- Autocorrelation and cross-correlation may become susceptible to noise when sample batches are small and noise is powerful but SDP can be designed to be resilient toward noise.



Noise reduction in remote signal der_1_noisy using its autocorrelation and cross-correlation with local signal der_2 via SDP reconstruction.

Integrated Cybersecurity for Power System Control with Inverters

Ali mehrizi-Sani

mehrizi@VT.EDU
mehriziSANI.COM

VIRGINIA TECH

POWER AND ENERGY CENTER