DOE SETO Webinar Series

Secure Monitoring and Control of Solar Power Distribution System Through Dynamic Watermarking

Le Xie, Professor, Texas A&M

Team Members:

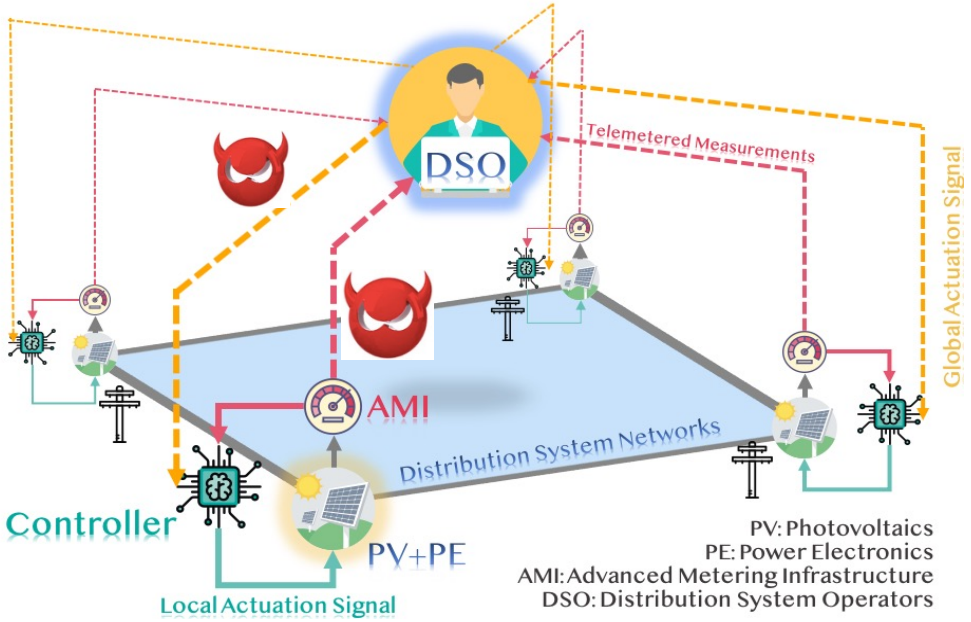
P. R. Kumar, Prasad Enjeti,	**Texas A&M**
Mohammad Shahidehpour, Zuyi Li,	**Illinois Institute of Technology**
Marija Ilic,	**Massachusetts Institute of Technology**
Tianqi Hong,	**Argonne National Laboratory**
Kevin Ding,	**CenterPoint Energy**

Apr. 26. 2023

TEXAS A&M ENGINEERING EXPERIMENT STATION · ILLINOIS INSTITUTE OF TECHNOLOGY · Argonne NATIONAL LABORATORY · CenterPoint Energy

Background

- A PV-dominant distribution grid is a cyber-physical system.
- Attackers can compromise the system by manipulate edge devices.
- Efforts that ***solely*** target at improving the cyber-layer security may not be adequate.
- How to defend a PV-dominant distribution grid against cyber attack?

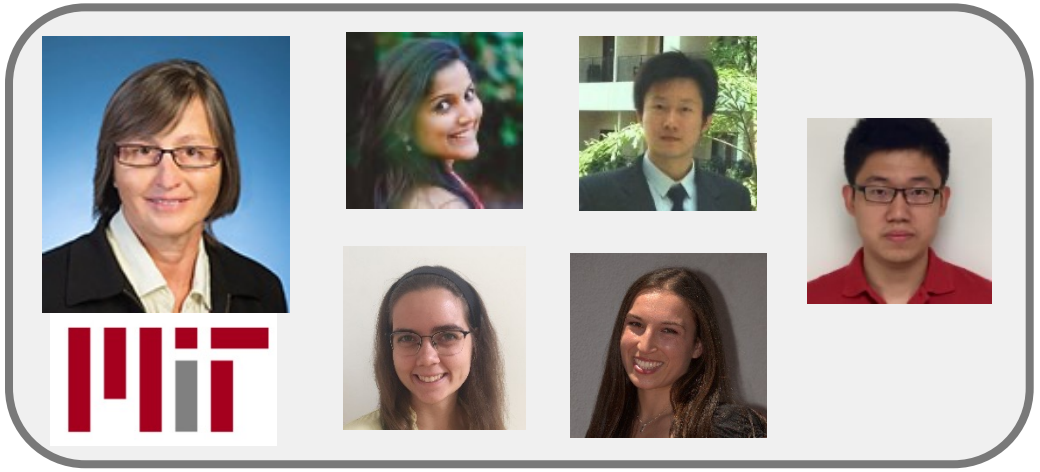


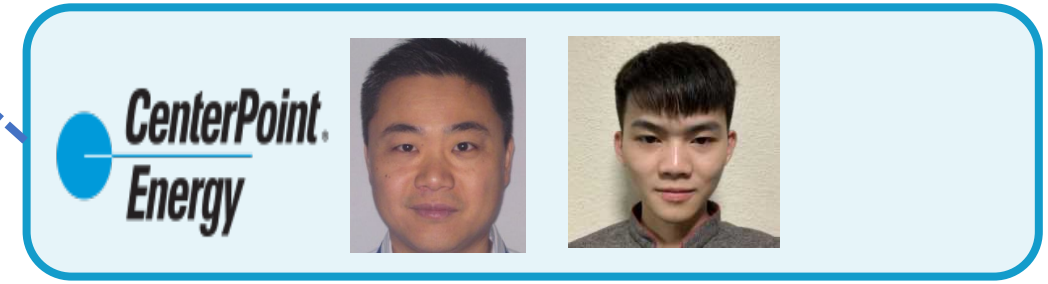
Project Goal

This project aims to:

- provide an end-to-end ***monitoring framework*** of critical microgrid/distribution grid with inverter-interfaced PV;
- design a ***resilient control*** strategy that would function well under normal conditions and function safely during abnormal (attacked) conditions;
- develop and validate the performance of the monitoring capabilities in ***real-world testbed*** configured based on ***realistic distribution system information***.

Research Team





More to be added...

Industry Advisory Board

Burak Ozpineci
Section Head
Oak Ridge National Laboratory
burak@ornl.gov

Patrick Chapman
Vice President
Enphase Energy
pchapman@enphaseenergy.com

Charlies Hanley
Sr. Manager
Sandia National Laboratories
cjhanle@sandia.gov

Wes Baker
Sr. Technical Leader
Electric Power Research Institute
wbaker@epri.com

Ryan Wiechens
Lincoln Lab @ MIT
wiechens@ll.mit.edu

Rajesh Kanungo
CEO
Talasecure
rajesh@talasecure.com

Song Wang
Principal Transmission Planning Engineer
PacifiCorp
Song.Wang@pacificorp.com

Hala Ballouz
President
EPE Consulting
hballouz@epeconsulting.com

Ivan Celanovic
Co-founder & Chief Business Development Officer
Typhoon HIL, Inc.
ivanc@typhoon-hil.com

Yi Liu
Senior Quantitative Engineer ComEd
Yi.Liu@comed.com

Dan Schnitzer, Ph.D.
CEO
SPARKMETER
dan@sparkmeter.io

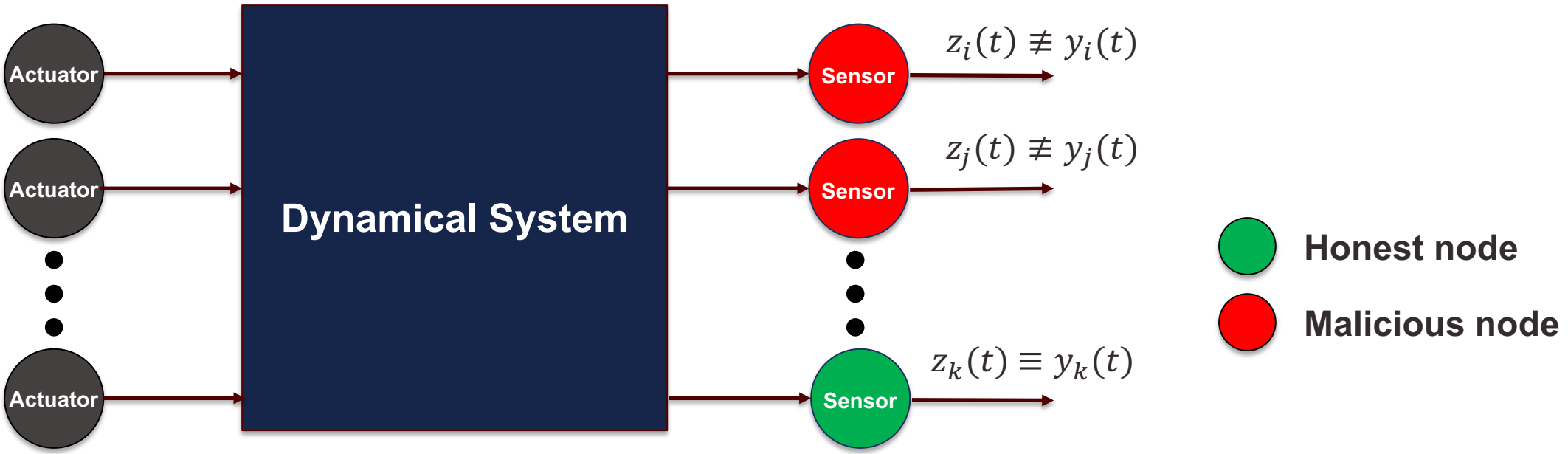
Project Overview

Cyber-Security of Networked Cyber-Physical Systems (CPS)

Satchidanandan, Bharadwaj, and Panganamala R. Kumar. "Dynamic watermarking: Active defense of networked cyber–physical systems." Proceedings of the IEEE 105.2 (2016): 219-240.

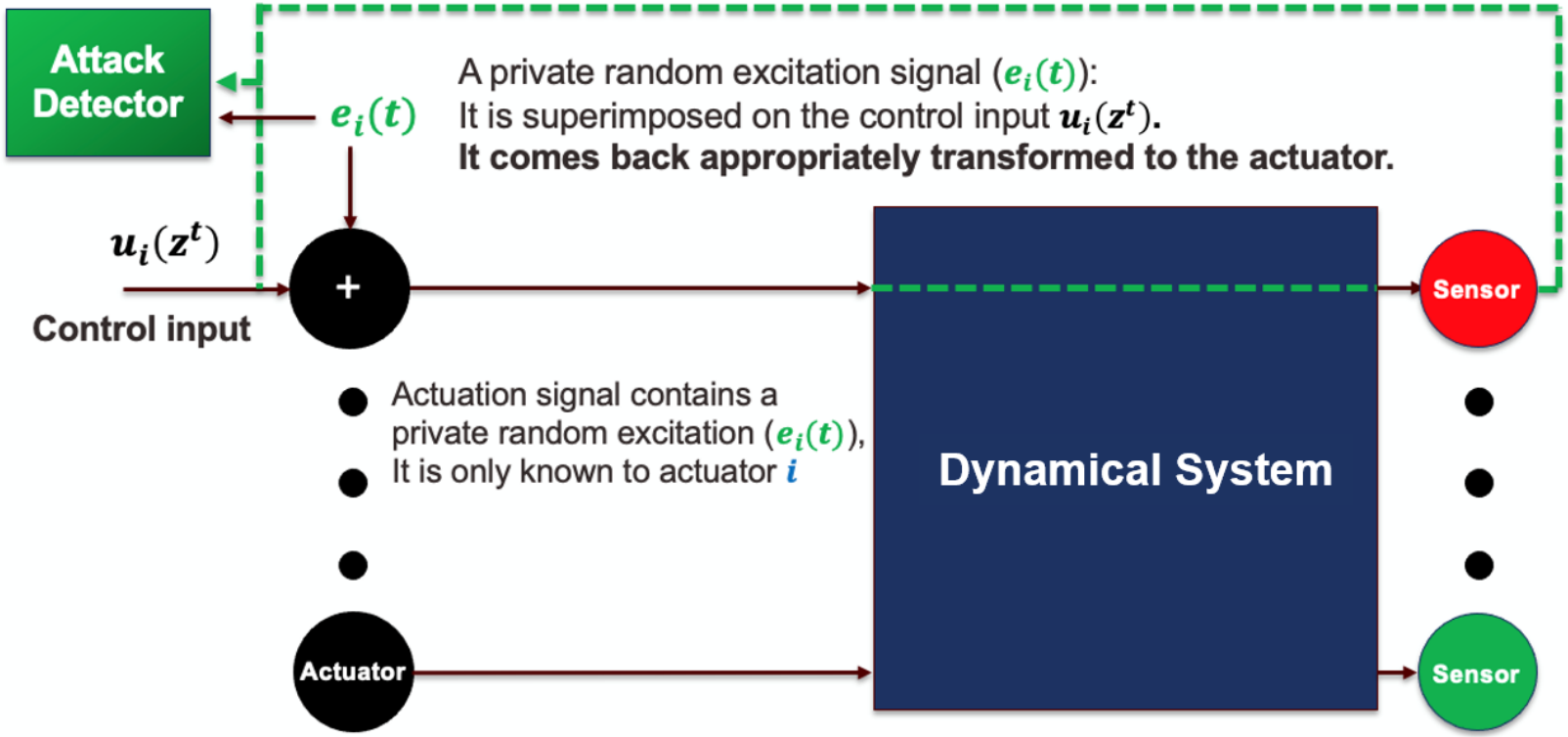
Huang, Tong, et al. "Enabling secure peer-to-peer energy transactions through dynamic watermarking in electric distribution grids: Defending the distribution system against sophisticated cyberattacks with a provable guarantee." IEEE Electrification Magazine 9.3 (2021): 55-64.

Cyber-Physical Systems (CPS) with malicious sensors



- **Some sensors in the system could be malicious.**
- **The false measurements can cause damage to the system.**
  - **Stuxnet (2010)**

The Dynamic Watermarking Method for Detecting Attacks



Why is it called "Watermark" ?
Because it is "Indelible"
like a watermark on a sheet of paper.
It cannot be removed
from the sensor measurement.

- Actuator can check if the private excitation comes back appropriately transformed in the measurements reported by the sensors.

Satchidanandan, Bharadwaj, and Panganamala R. Kumar. "Dynamic watermarking: Active defense of networked cyber–physical systems." Proceedings of the IEEE 105.2 (2016): 219-240.

Huang, Tong, et al. "Enabling secure peer-to-peer energy transactions through dynamic watermarking in electric distribution grids: Defending the distribution system against sophisticated cyberattacks with a provable guarantee." IEEE Electrification Magazine 9.3 (2021): 55-64.

The Dynamic Watermarking Method: A SISO example

- $x(t+1) = ax(t) + bu(t) + w(t+1)$, where $w(t) \sim N(0, {\sigma_w}^2)$ i.i.d.
- DW: $u(t) = u(t) + e(t)$ with $e(t) \sim N(0, {\sigma_e}^2)$ i.i.d.
- Closed-loop system: $x(t+1) = ax(t) + bu(t) + be(t) + w(t+1)$
- Therefore,

$$x(t+1) - ax(t) - bu(t) - be(t) = w(t+1) \sim N(0, {\sigma_w}^2)$$

$$x(t+1) - ax(t) - bu(t) = be(t) + w(t+1) \sim N(0, b^2{\sigma_e}^2 + {\sigma_w}^2)$$

Satchidanandan, Bharadwaj, and Panganamala R. Kumar. "Dynamic watermarking: Active defense of networked cyber–physical systems." Proceedings of the IEEE 105.2 (2016): 219-240.

Huang, Tong, et al. "Enabling secure peer-to-peer energy transactions through dynamic watermarking in electric distribution grids: Defending the distribution system against sophisticated cyberattacks with a provable guarantee." IEEE Electrification Magazine 9.3 (2021): 55-64.

The Dynamic Watermarking Method: Two Tests for Detecting Attacks

- **Two tests are conducted by actuator**

Test 1: $$\left[lim\ \frac{1}{T} \sum_{t=0}^{T-1} \left(z(t+1) - az(t) - bu(t) - be(t) \right)^2 \right] \overset{?}{=} {\sigma_w}^2$$

Test 2: $$\left[lim\ \frac{1}{T} \sum_{t=0}^{T-1} \left(z(t+1) - az(t) - bu(t) \right)^2 \right] \overset{?}{=} b^2 {\sigma_e}^2 + {\sigma_w}^2$$

- **If either test fails, then there is malicious/abnormal sensor information**
  - **System goes into safety mode: Halted, rebooted, manual operation, etc**

- **Trade-off for setting detection threshold**
  - **High threshold results in more Miss Alarms**
  - **Low threshold results in more False Alarms**

Dynamic Watermarking for Transmission Systems

Key Idea:

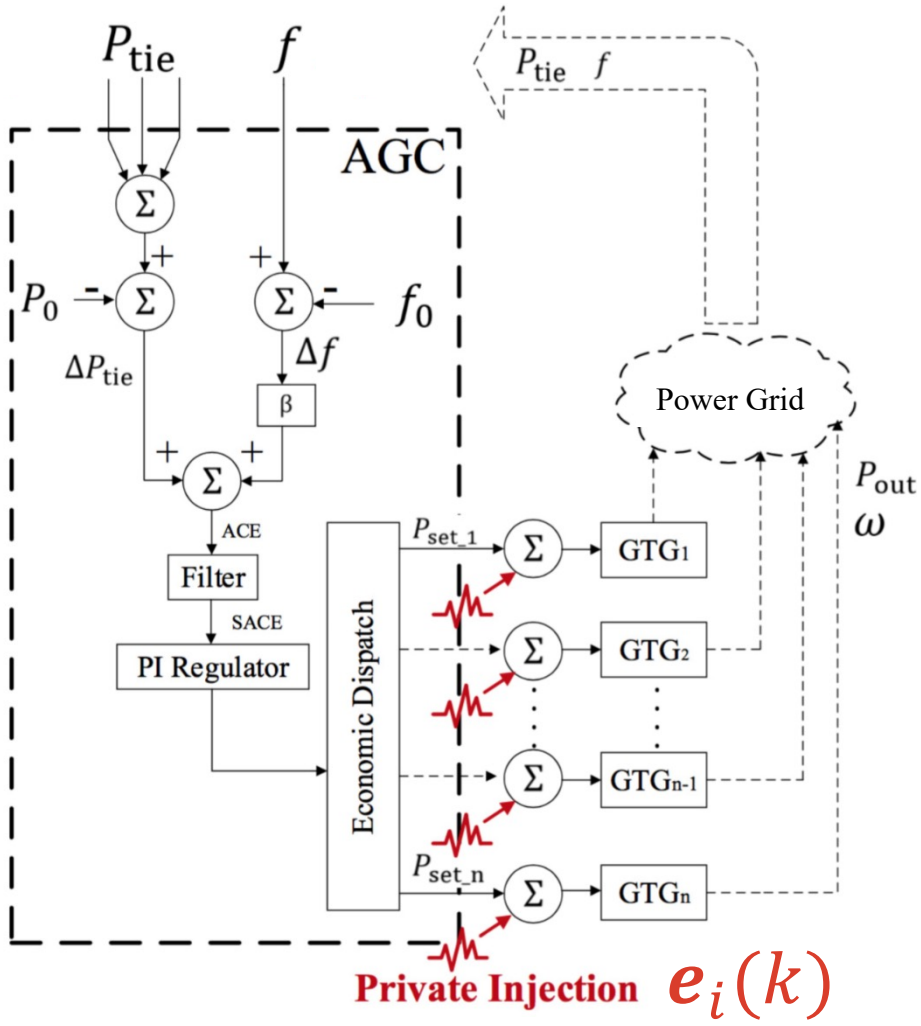
- By injecting a private (*small*) signal at the controller, an *indelible* pattern can be imprinted into the measurement feeding to the generator control.

$$\begin{aligned} \boldsymbol{x}_{\mathrm{d}i}(k+1) =& A_{\mathrm{d}i}\boldsymbol{x}_{\mathrm{d}i}(k) + B_{\mathrm{d}i}^{\mathrm{ref}}\boldsymbol{p}_{si}(k) \\ &+ B_{\mathrm{d}i}^{\mathrm{load}}\boldsymbol{u}_{\mathrm{load}}(k) + \boldsymbol{\gamma}(k+1) \\ \boldsymbol{y}_i(k) =& C_{\mathrm{d}i}\boldsymbol{x}_{\mathrm{d}i}(k) + \boldsymbol{n}(k) \end{aligned}$$

Statistical Connection?

$$\boldsymbol{p}_{si}(k) = \boldsymbol{f}_i(\boldsymbol{y}_i^k) + \boldsymbol{e}_i(k)$$

$\boldsymbol{y}_i(k)$:



Huang, Satchidanandan, Kumar, and **Xie**, "An Online Detection Framework for Cyber Attacks on Automatic Generation Control," *IEEE TPWRS* (2018).

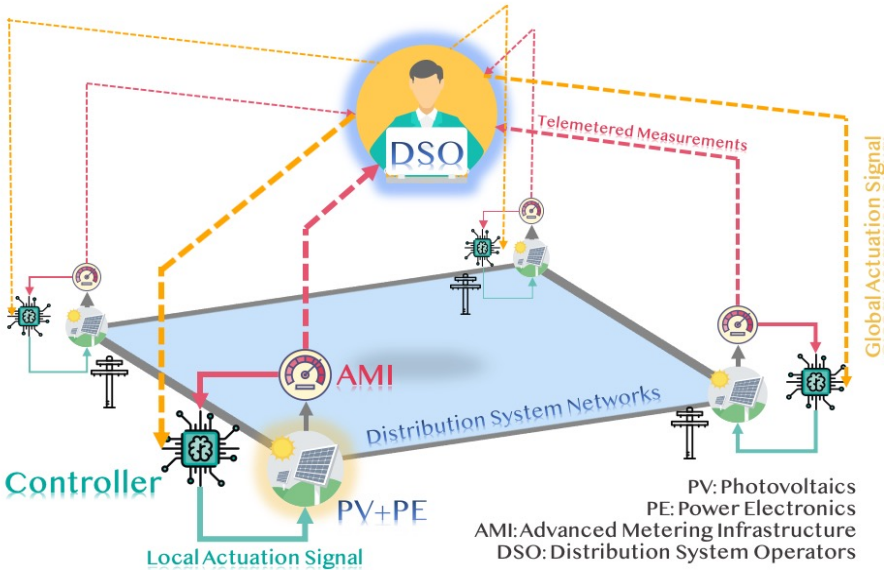
Preliminary Success of the Dynamic Watermarking Method in other cyber-physical systems

- Defending against cyber-attacks on automatic generation control
  - Huang, Tong, et al. "An online detection framework for cyber attacks on automatic generation control." IEEE Transactions on Power Systems 33.6 (2018): 6816-6827.
- Defending against cyber-attacks on a prototype chemical process control systems
  - Kim, Jaewon, Woo-Hyun Ko, and P. R. Kumar. "Cyber-security with dynamic watermarking for process control systems." 2019 AIChE Annual Meeting. AIChE, 2019.
- Defending against cyber-attacks on a prototype autonomous vehicular systems
  - Shangguan, Lantian, et al. "Dynamic watermarking for cybersecurity of autonomous vehicles." IEEE Transactions on Industrial Electronics (2022).
- Defending against cyber-attacks on a prototype two-rotor aerial vehicle control systems
  - Kim, Jaewon, Woo-Hyun Ko, and P. R. Kumar. "Cyber-Security through Dynamic Watermarking for 2-rotor Aerial Vehicle Flight Control Systems." 2021 International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, 2021.

Cyber-Security of Photovoltaic Power Distribution Systems

Our focus: Cyber Physical Security in Solar-rich Distribution Grids

- PV-dominant distribution grids are cyber-physical systems
- Attackers can compromise the system by manipulating inverters at the edges



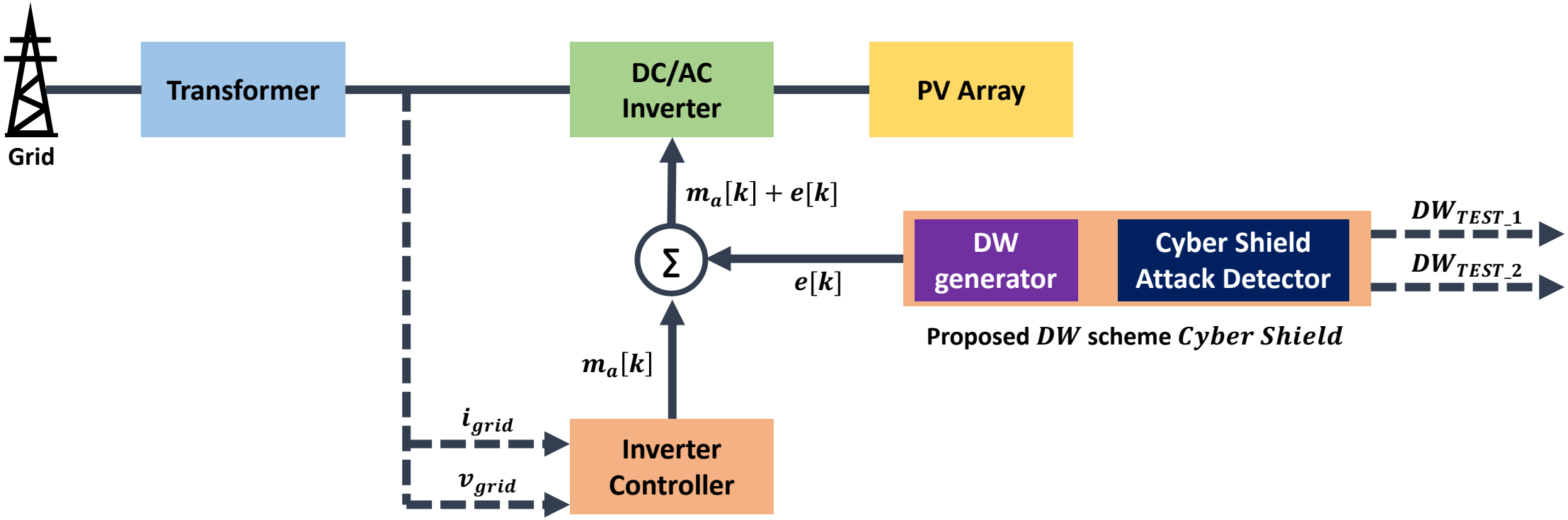
How to defend PV-dominant distribution grids against cyber attack?

Our focus: Cyber Physical Security in Solar-rich Distribution Grids

- Cyber-Attack Detection through Dynamic Watermarking based attack detector
- Detection algorithm:
  - Use the system model if the model is given
  - If the model is unknown,

    proper System Identification needed for overcoming the requirement to know the system model
- Experimental validation
- Corrective secondary control (cyber-resilient control)

Dynamic Watermarking-based Detection Algorithm



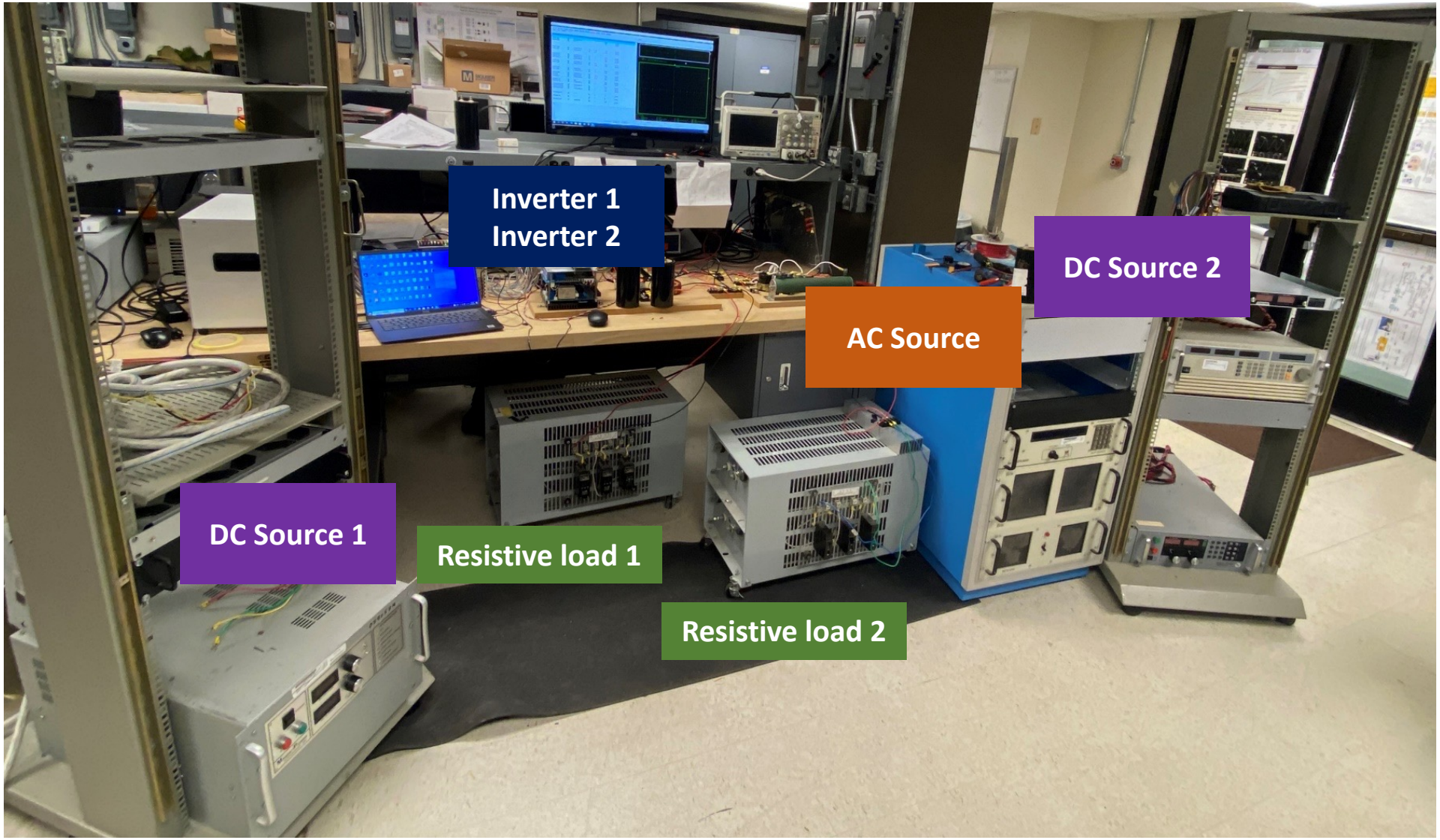
Critical need for Experimental Testing

- Watermarking methodology is fundamentally based on stochastic considerations.
- There is no mathematical model for “noise”.
- Therefore, one needs to test by experimentation.
- Critical issue:

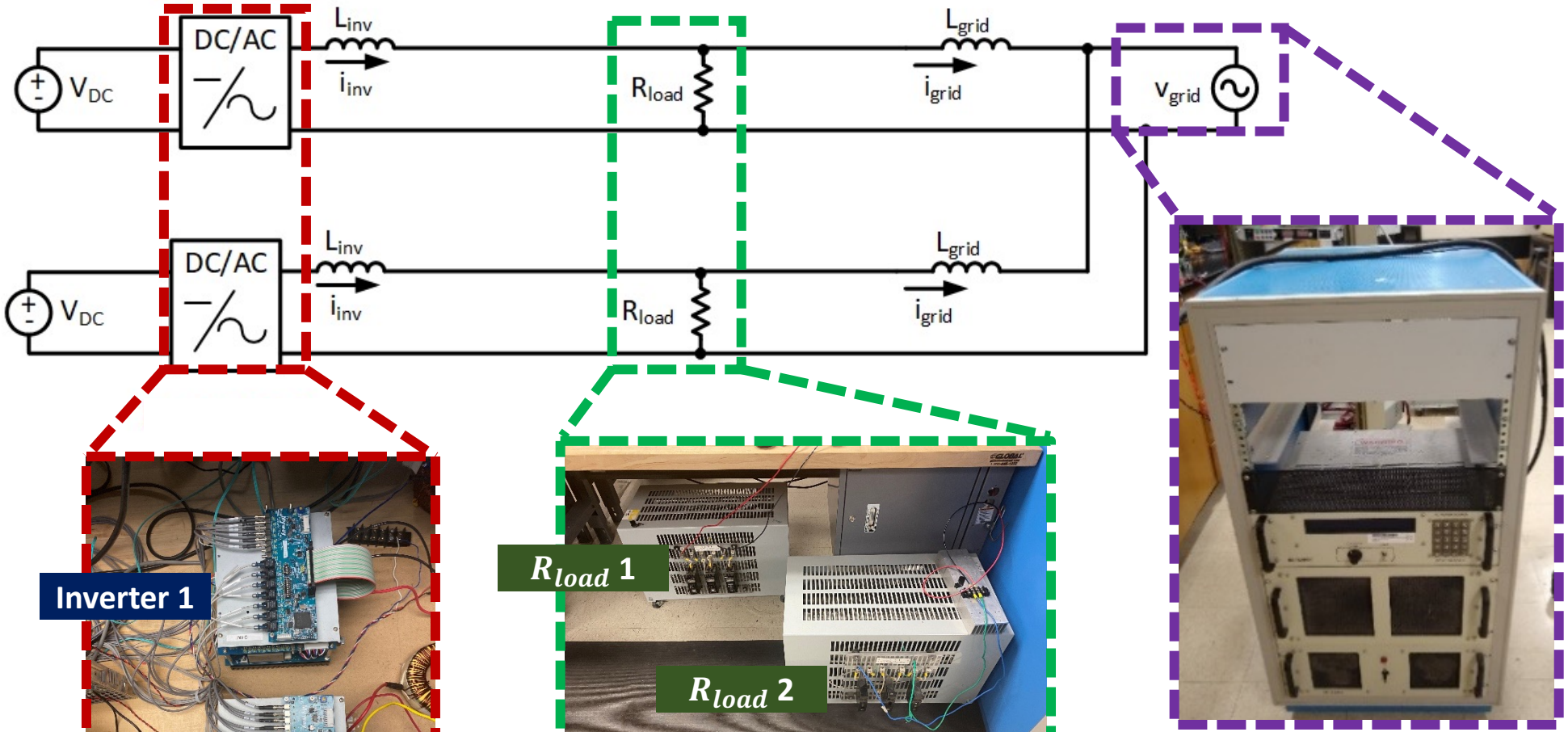
  Does the tiny watermark signal that is superimposed survive passage trough the “noise”?
  - Also, how small can watermark be?
- Therefore, a defense methodology against cyber-attacks that fundamentally relies on stochastic considerations needs experimental validation, not validation by simulation.

Defending against attacks on Two-Inverter Connected System

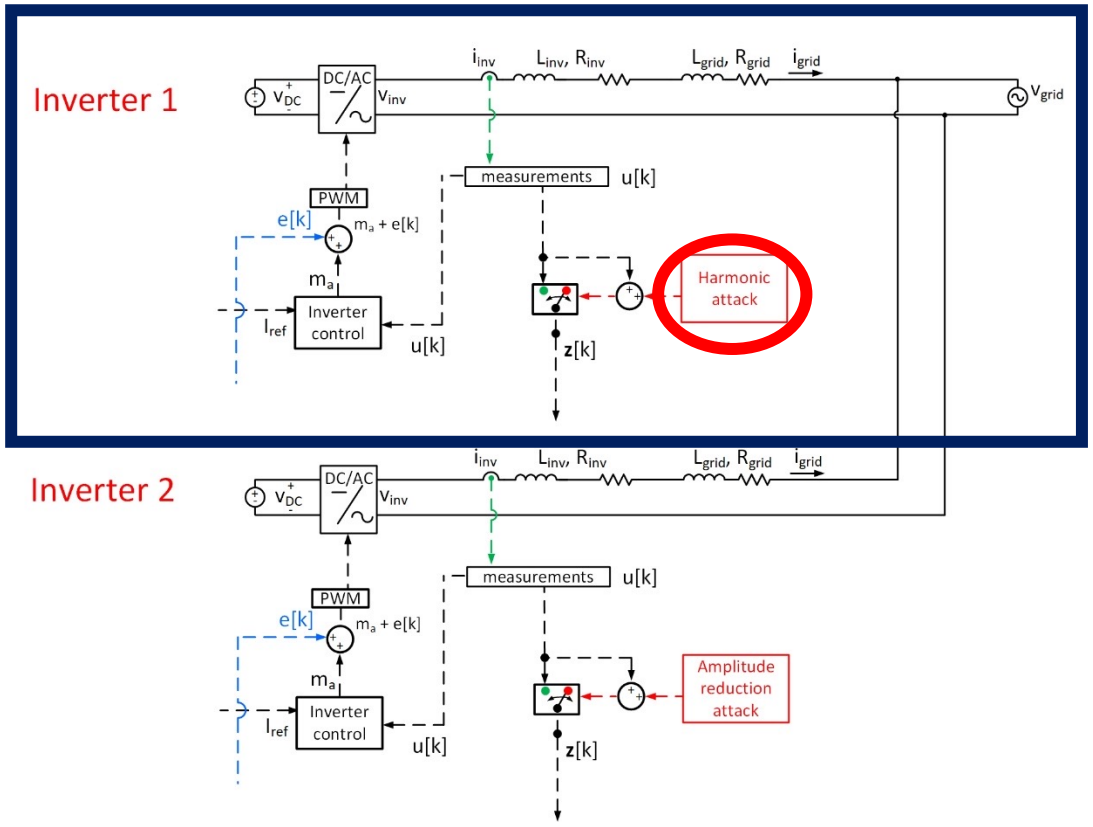
Two inverter system Lab set-up

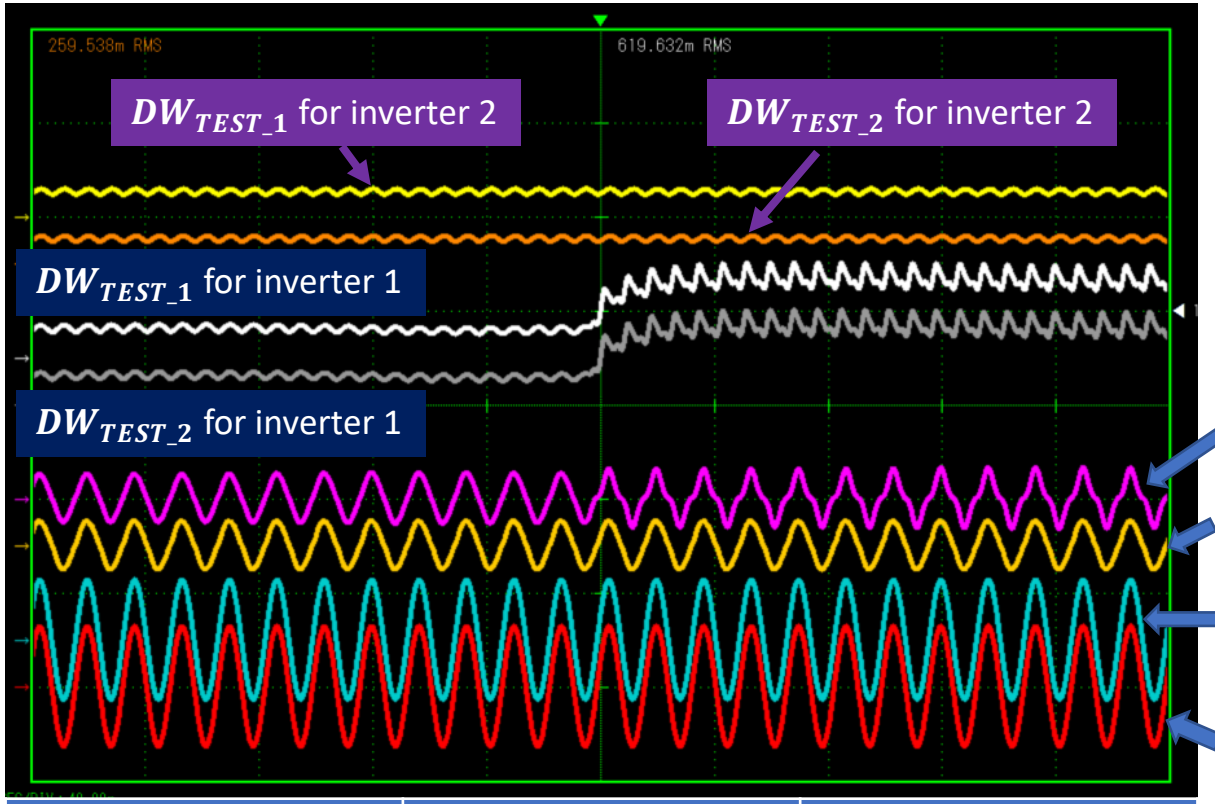


Two inverter system Lab set-up



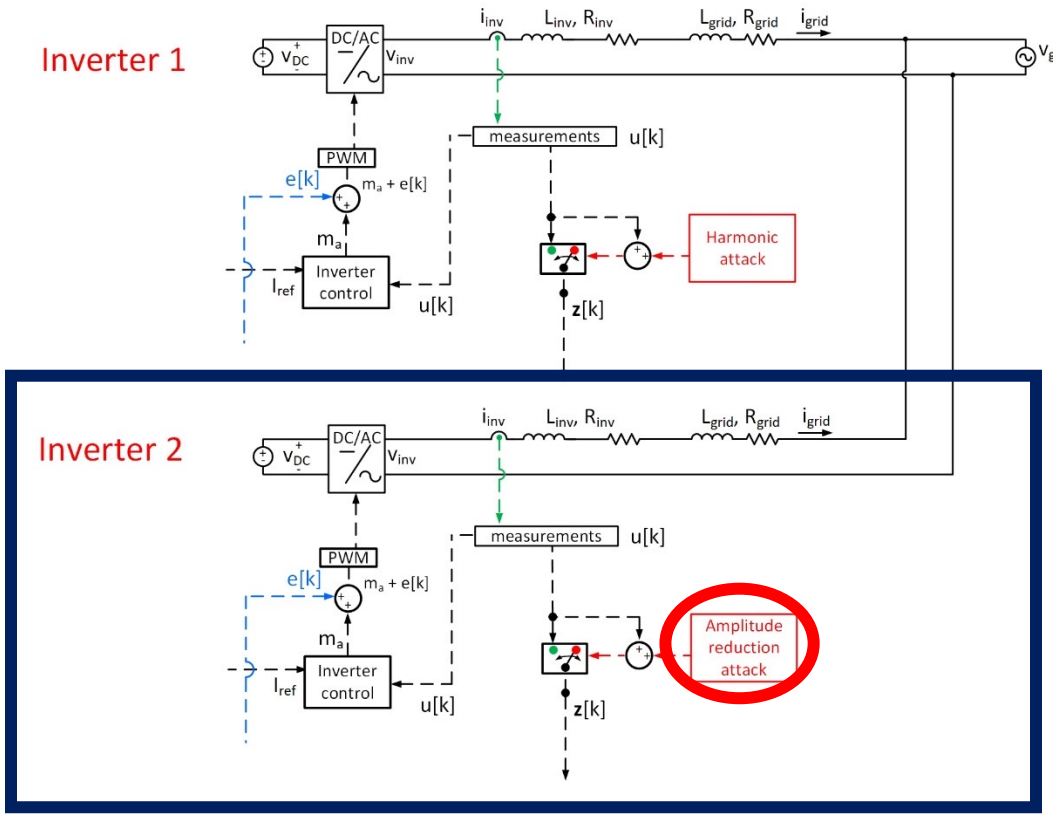
Harmonics Injection Attack on Inverter 1

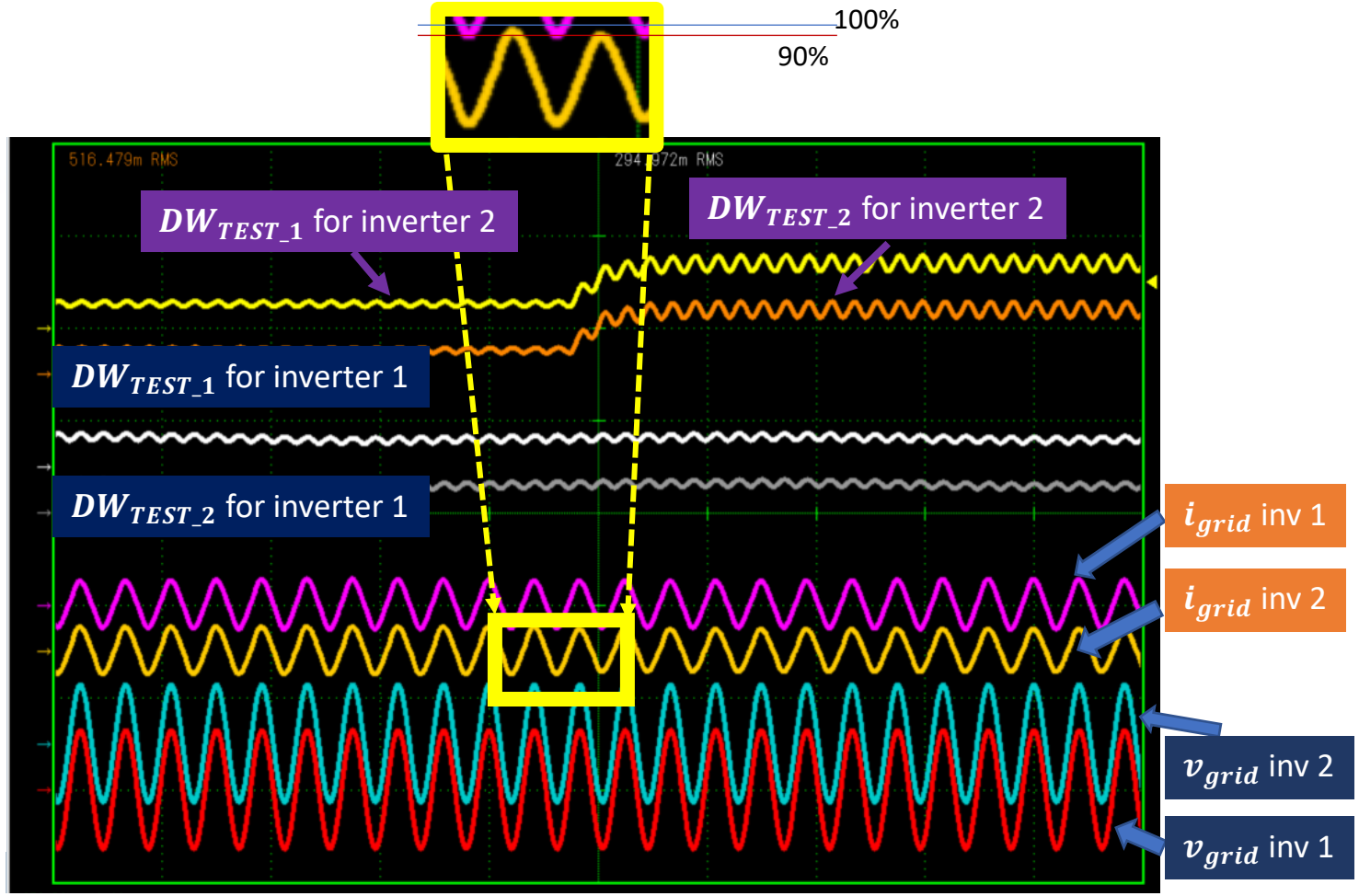




Inverter	Test Variances before attack	Test Variances after attack
1	298×10^{-3}	619×10^{-3}
2	259×10^{-3}	259×10^{-3}

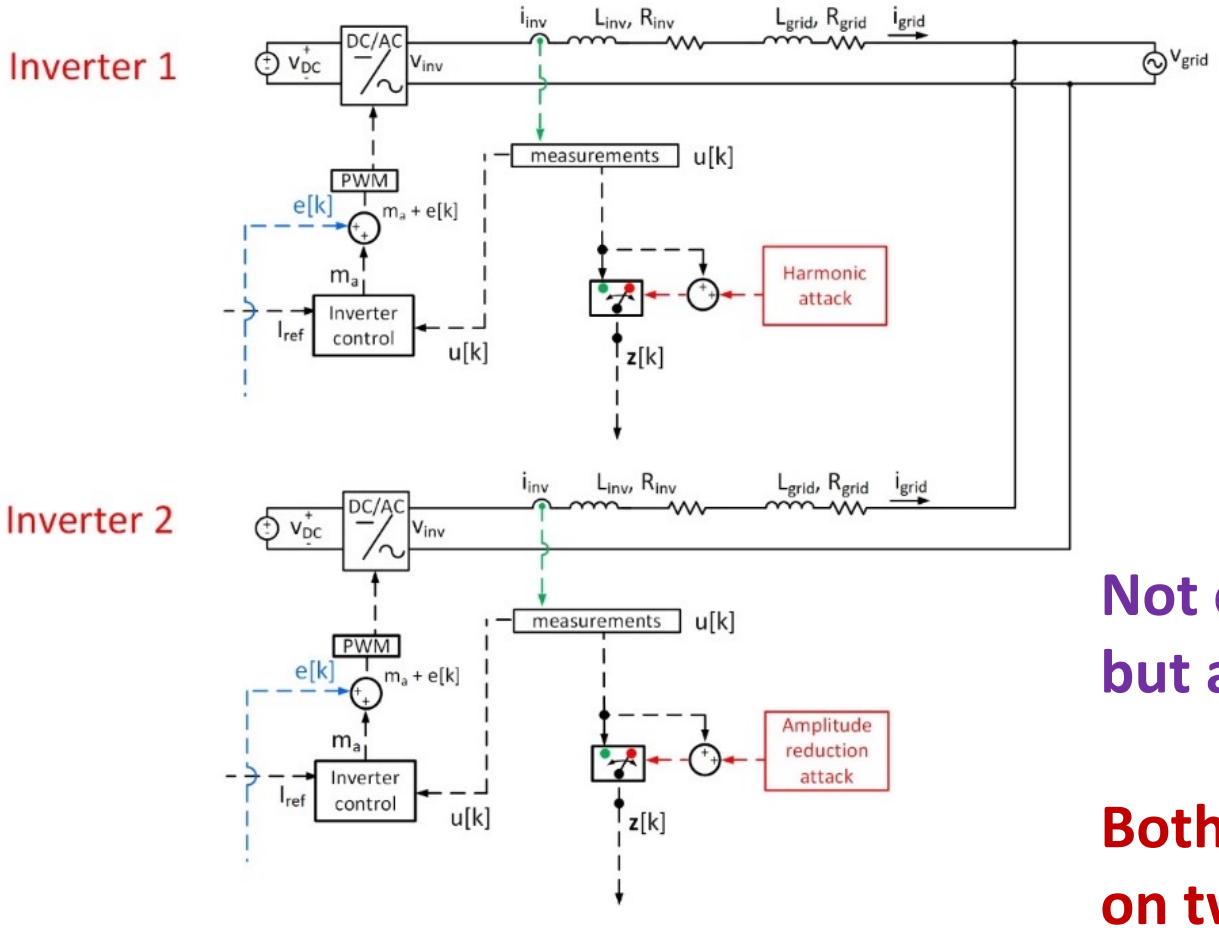
Amplitude Reduction Attack on Inverter 2





Inverter	Test Variances before attack	Test Variances after attack
1	294×10^{-3}	294×10^{-3}
2	259×10^{-3}	708×10^{-3}

Multi-Inverter System LAB set-up:
Grid Tied PV System: Attack on Two Inverter Connected System

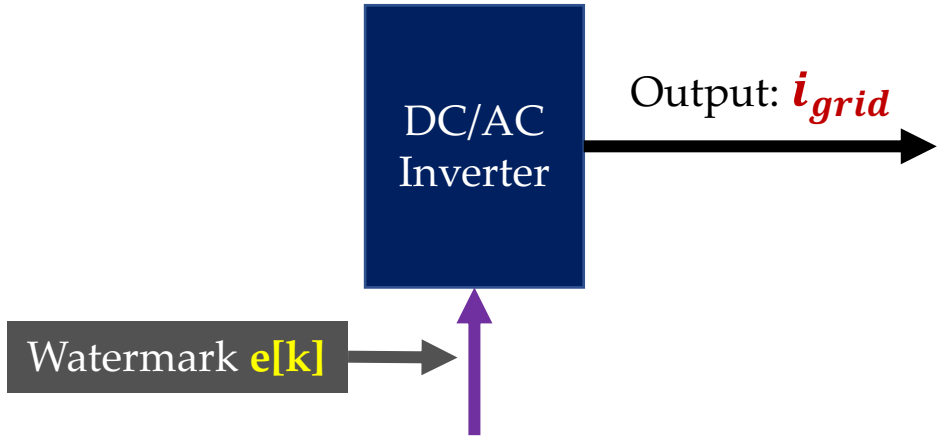


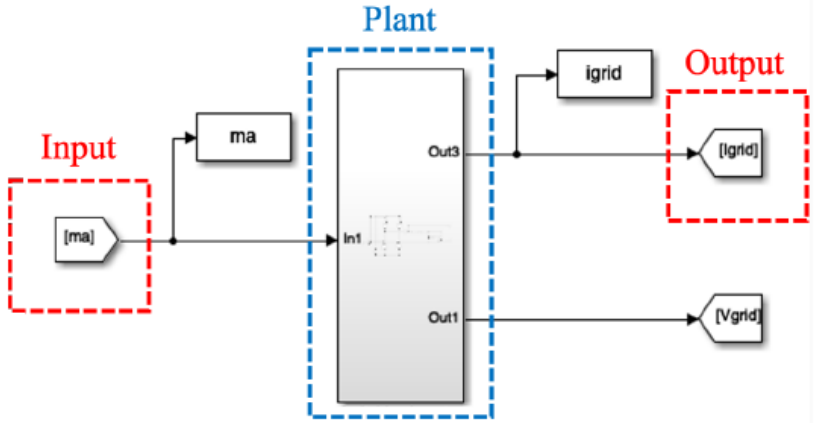
Not only detect cyber-attacks
but also, we can identify the attack location

Both simulation and experimental validation on two inverter connected system

Overcoming the requirement to know the system model

Overcoming the requirement to know the system model





Input and output data collection of a switching inverter

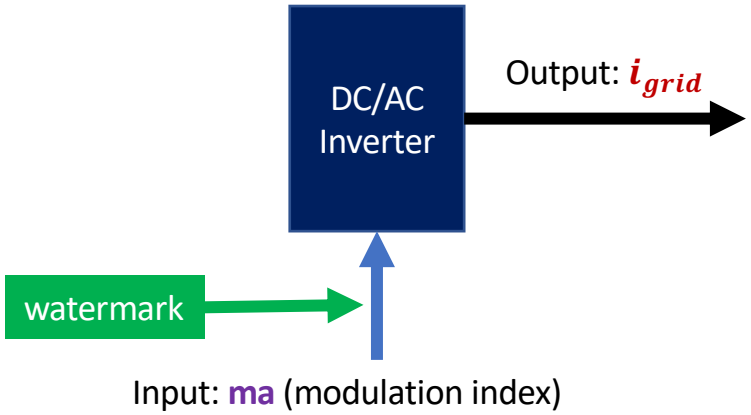
- **Generally, an accurate model of the system is unknown because of the non-linearity of the system as well as the complexity of the connected power grid.**
  - **Therefore, proper system identification methodology is essential not only for controlling the system but also for analyzing the effects of external disturbances and possible faults in the system.**

The form of the prediction model we identify it as follows:

$$\boldsymbol{f(x[k-N:k], u[k-M:k], A_N, B_M) =}$$
$$\boldsymbol{\alpha_0 \cdot x[k] + \alpha_1 \cdot x[k-1] + \cdots + \alpha_N \cdot x[k-N] +}$$
$$\boldsymbol{\beta_0 \cdot u[k] + \beta_1 \cdot u[k-1] + \cdots + \beta_M \cdot x[k-M]}$$

x is the system output i_{grid},
u is the system input m_a, and
$A_N := [\alpha_0\ \alpha_1\ \cdots\ \alpha_N]^T$, $B_M := [\beta_0\ \beta_1\ \cdots\ \beta_M]^T$ are the parameters associated with the input and output of the prediction model.

System Identification of DC/AC Inverter System: Input m_a / Output i_{grid}



$$\boldsymbol{x}[\boldsymbol{k}+\boldsymbol{1}] = \boldsymbol{A}\,\boldsymbol{x}[\boldsymbol{k}] + \boldsymbol{B}\,\boldsymbol{u}[\boldsymbol{k}]$$

$$\boldsymbol{I_{grid}}[k+1] = a_1 \cdot \boldsymbol{I_{grid}}[k] + a_2 \cdot \boldsymbol{I_{grid}}[k-1] + a_3 \cdot \boldsymbol{I_{grid}}[k-2] + a_4 \cdot \boldsymbol{I_{grid}}[k-3] +$$

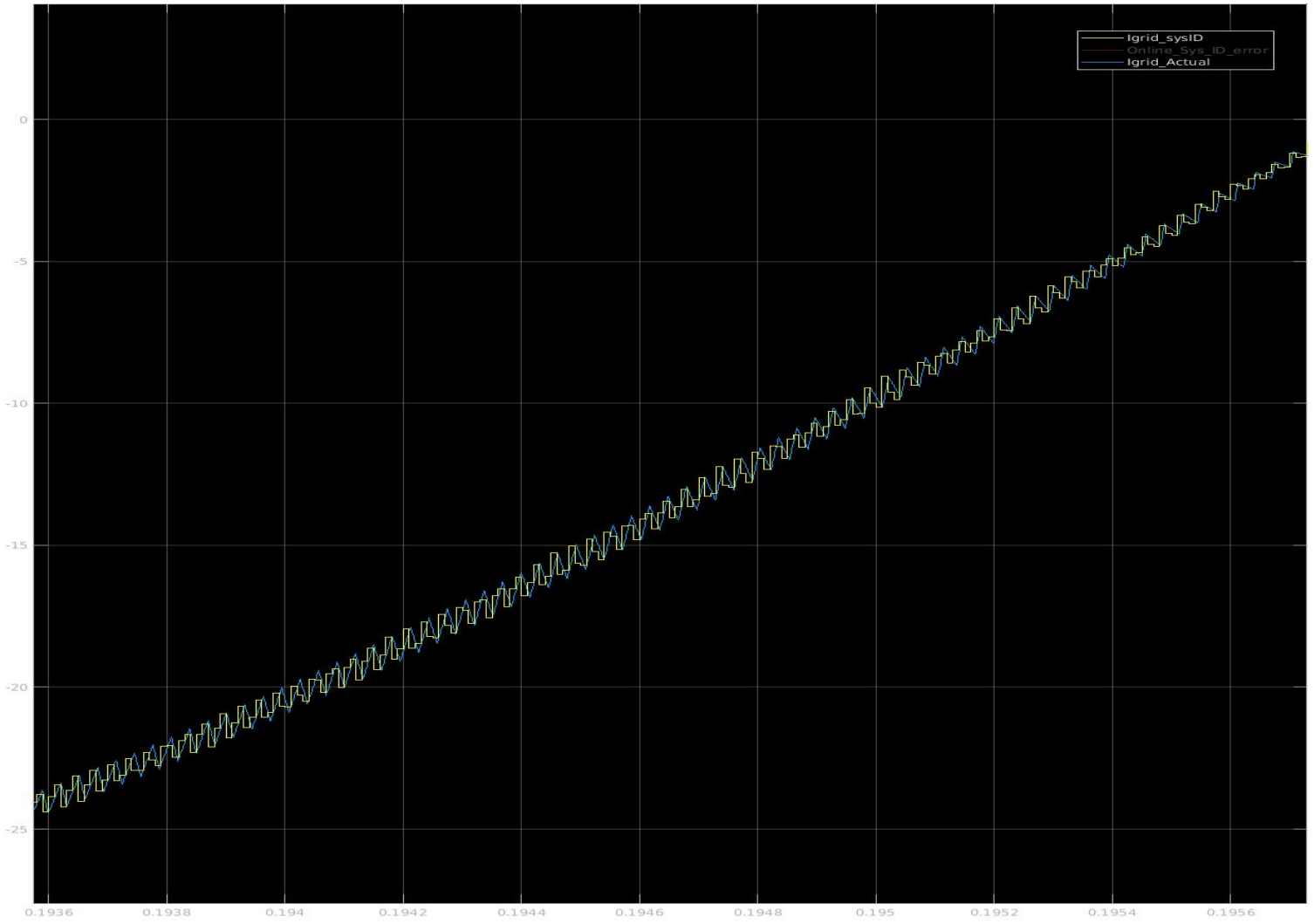
$$b_1 \cdot \boldsymbol{ma}[k] + b_2 \cdot \boldsymbol{ma}[k-1] + b_3 \cdot \boldsymbol{ma}[k-2] + b_4 \cdot \boldsymbol{ma}[k-3]$$

$$A = [\, a_1 \; a_2 \; a_3 \; a_4 \,]$$

$$B = [\, b_1 \; b_2 \; b_3 \; b_4 \,]$$

System Identification

Output error of the identified model

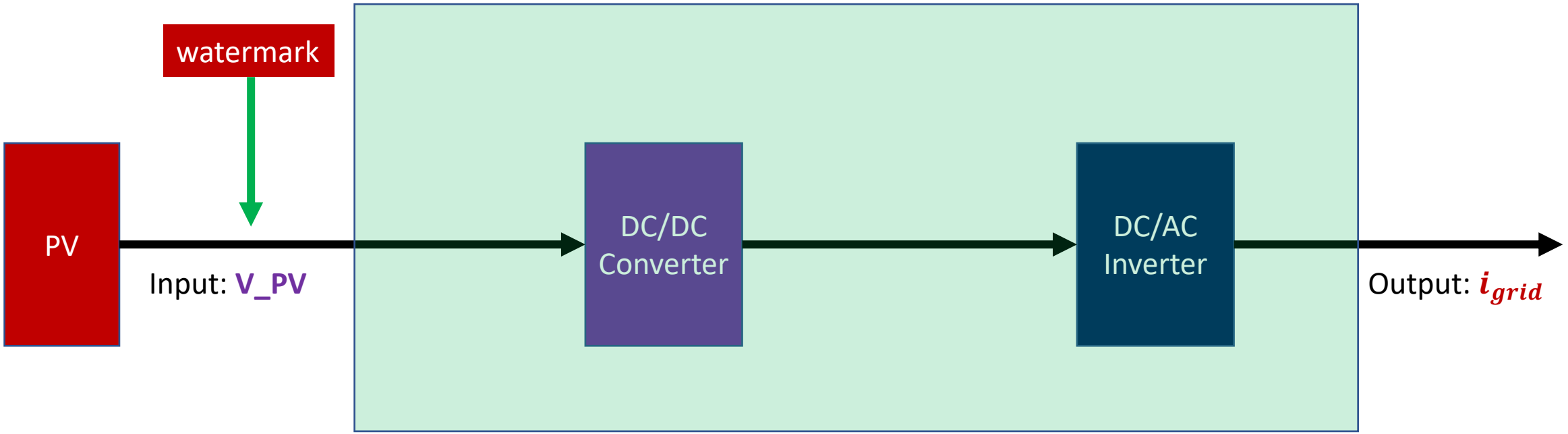


On-line (real-time)
System Identification

Yellow: System ID

Blue: Actual system output

System Identification of PV System: Input v_{pv} / Output i_{grid}



$$i_{grid}[k+1] = a_1 \cdot i_{grid}[k] + a_2 \cdot i_{grid}[k-1] + a_3 \cdot i_{grid}[k-2] + a_4 \cdot i_{grid}[k-3] +$$

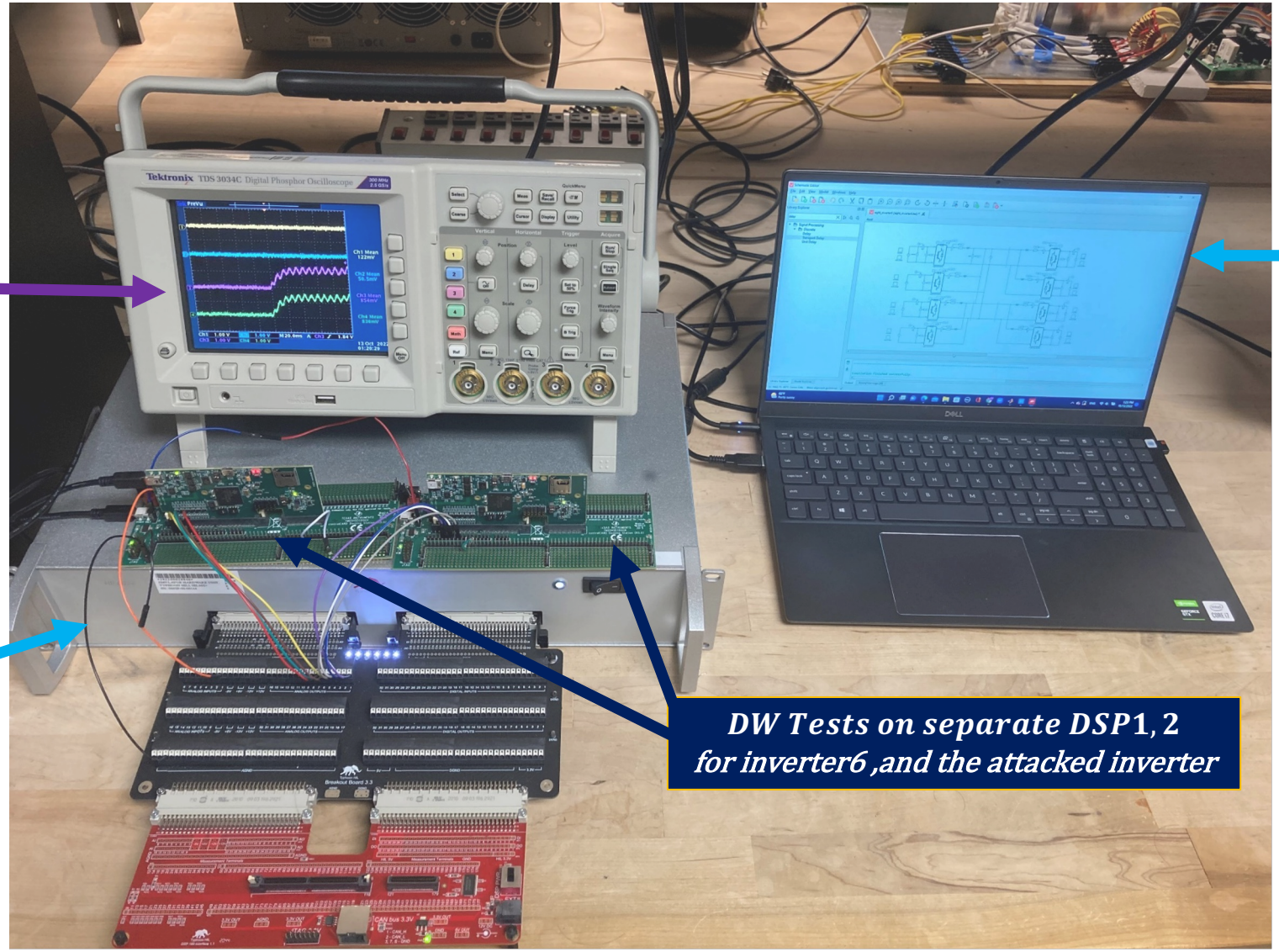
$$b_1 \cdot v_{pv}[k] + b_2 \cdot v_{pv}[k-1] + b_3 \cdot v_{pv}[k-2] + b_4 \cdot v_{pv}[k-3]$$

$$A = [\, a_1 \; a_2 \; a_3 \; a_4 \,]$$

$$B = [\, b_1 \; b_2 \; b_3 \; b_4 \,]$$

Hardware-in-the-loop experiments and Commercial grid connected Inverter experiments

Grid-connected multi-inverter system in Typhoon HIL Hardware setup



Oscioscilloscope DW Tests

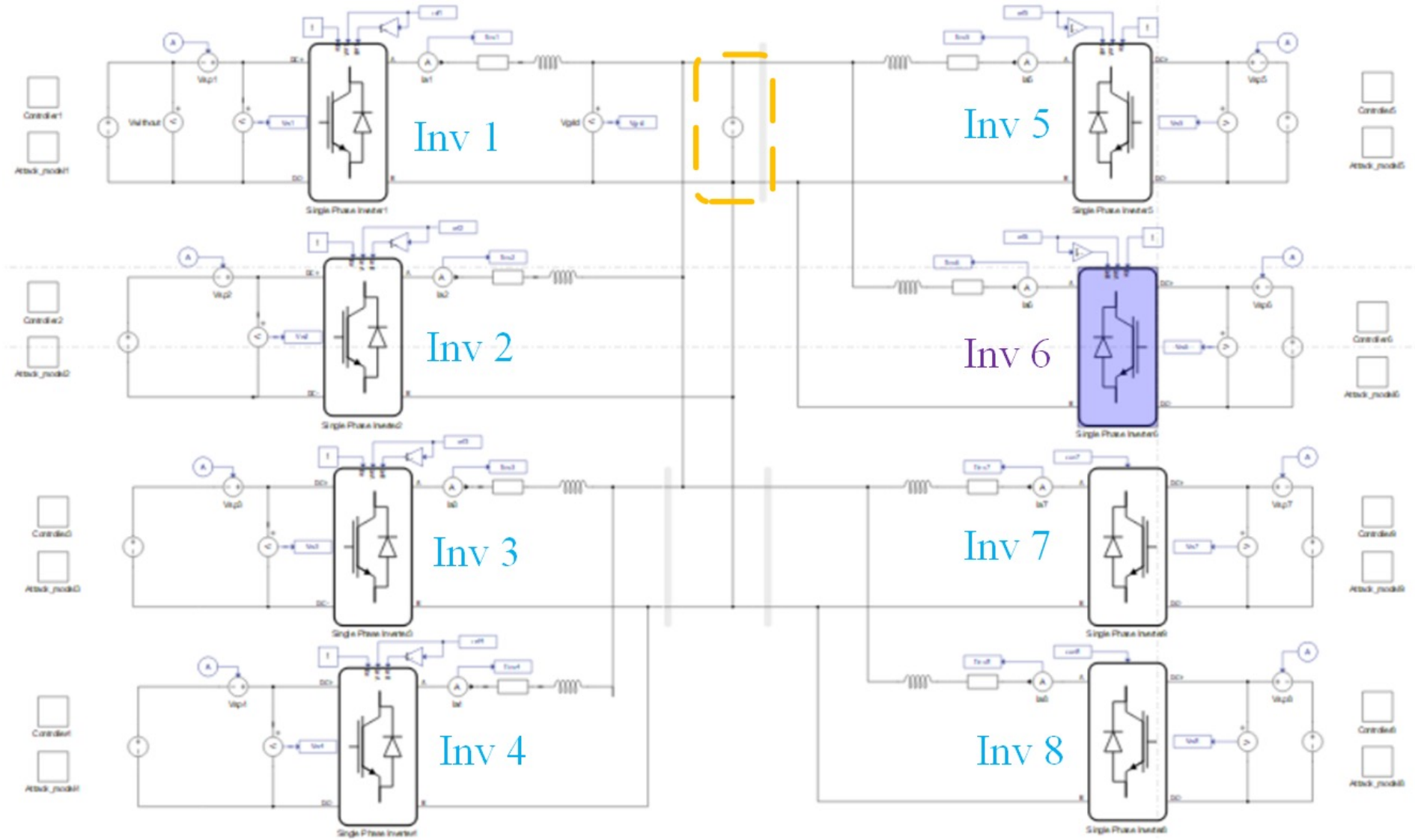
Real – time simulation in Typhoon HIL Software

Typhoon HIL

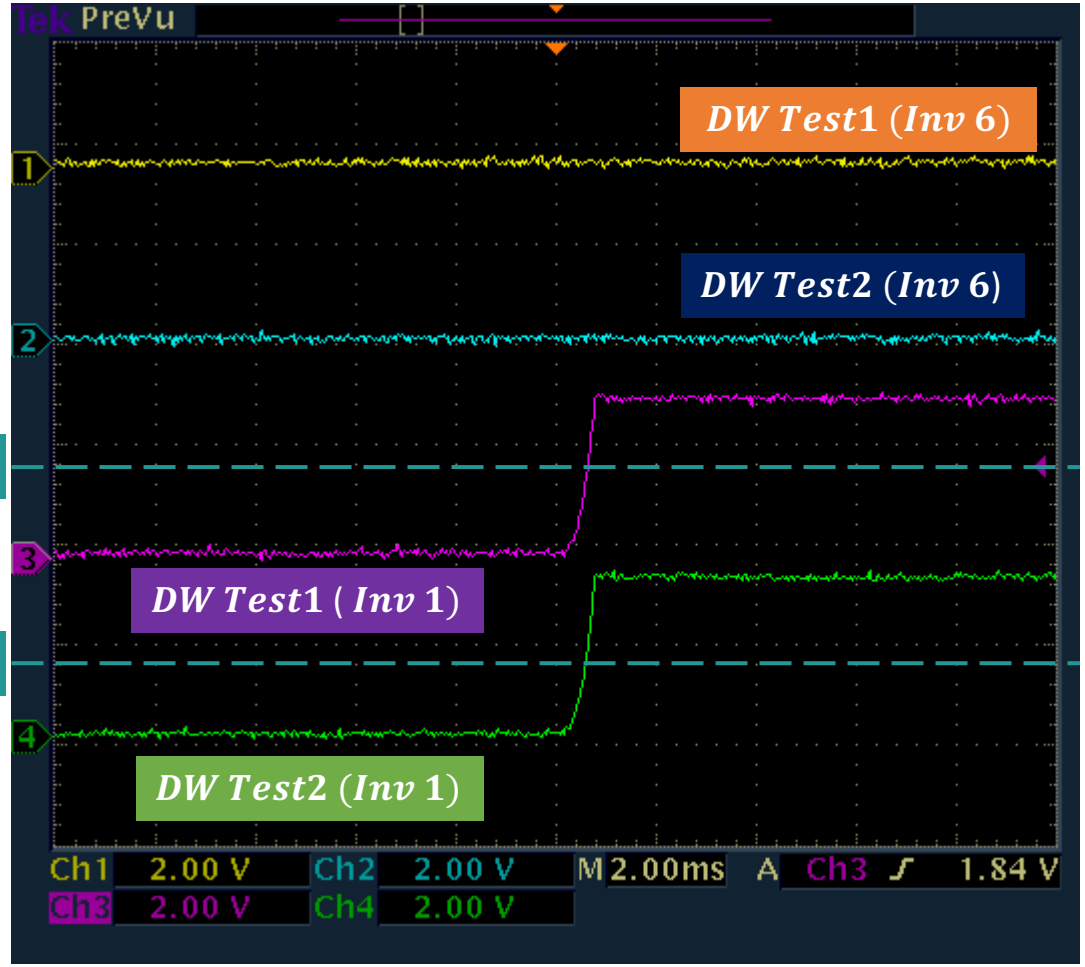
Typhoon HIL Multi-inverter Hardware emulator

DW Tests on separate DSP1, 2 for inverter6 ,and the attacked inverter

Grid-connected multi-inverter system in Typhoon HIL

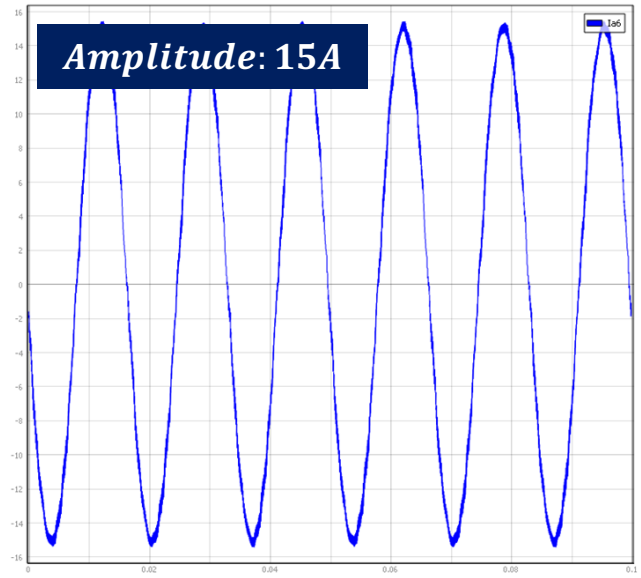


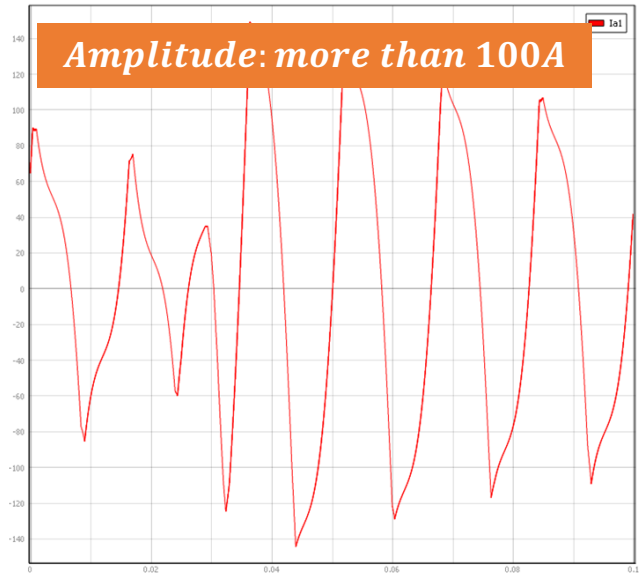
Time Delay attack on inverter 1



Threshold

Threshold



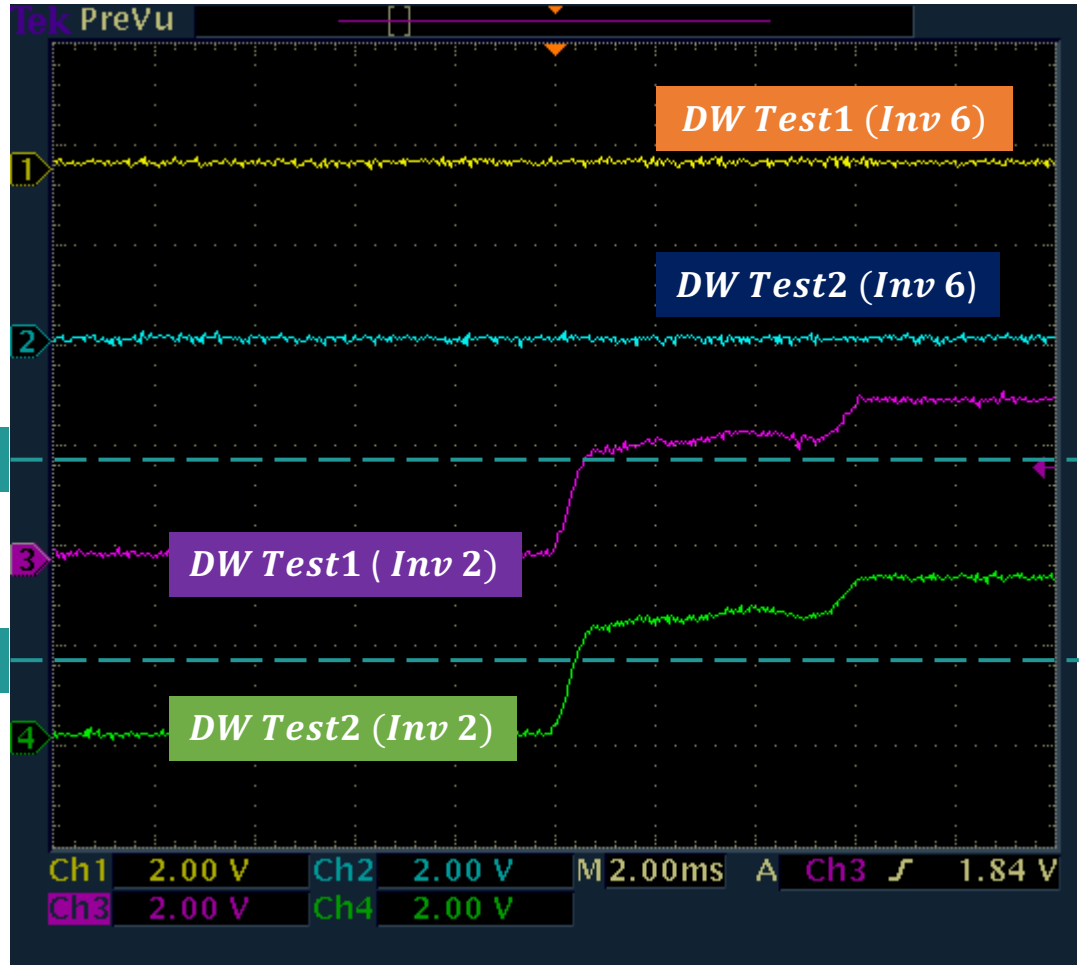


Normal operation (Inv 6)

Typhoon HIL

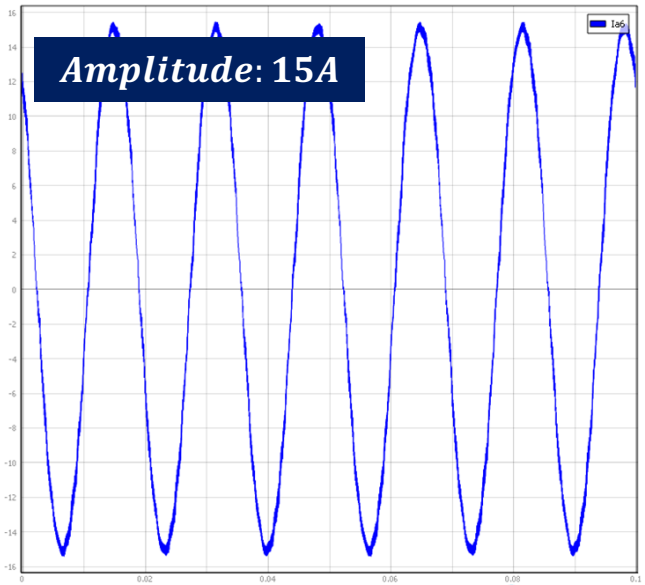
Time Delay (Inv 1)

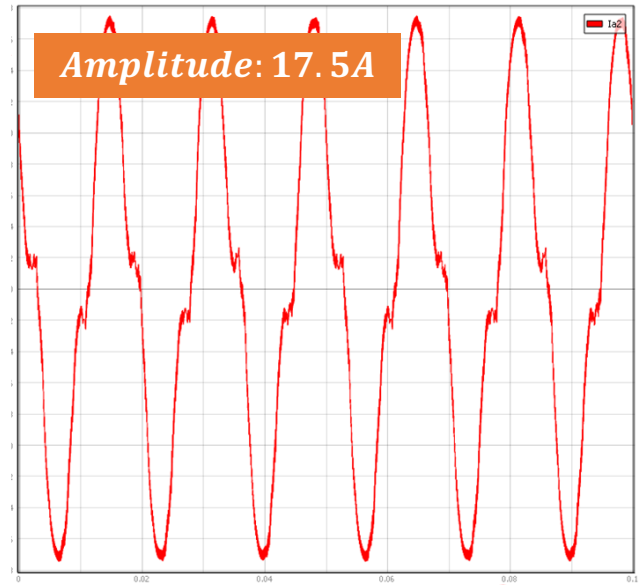
Harmonics Injection attack on inverter 2



Threshold

Threshold



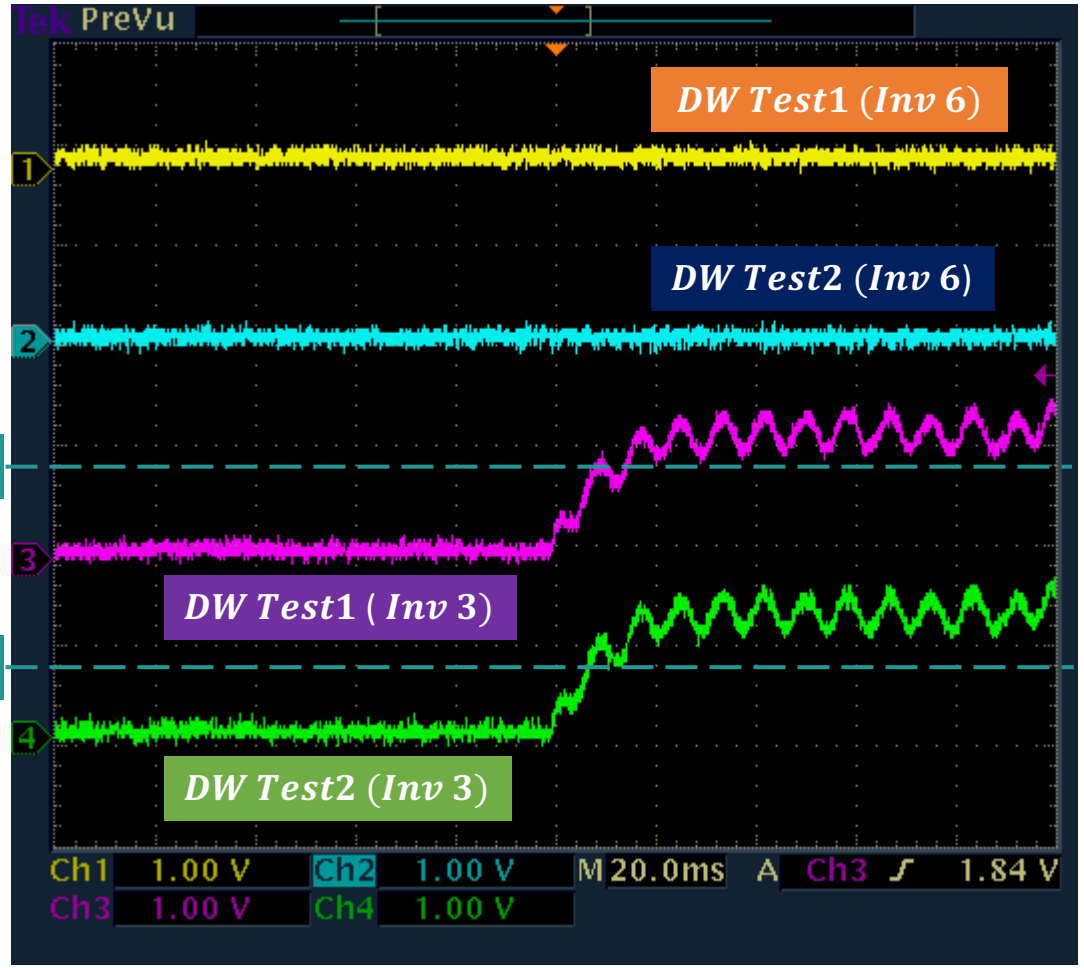


Normal operation (Inv 6)

Typhoon HIL

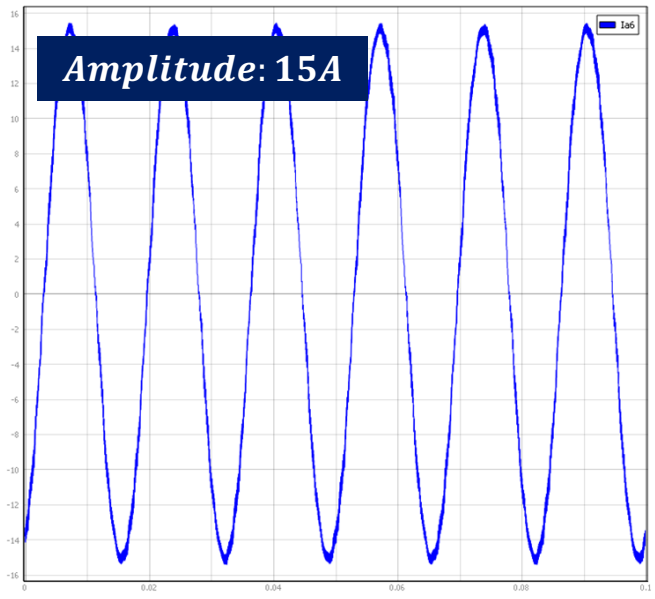
Harmonics Injection (Inv 2)

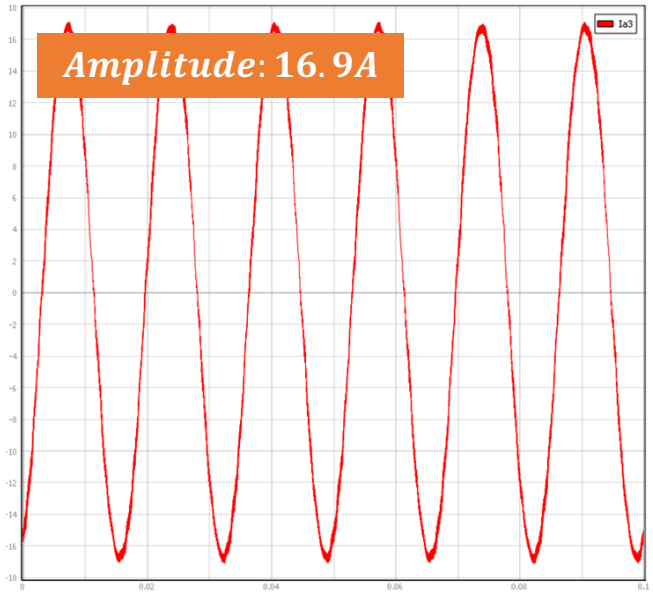
Amplitude Reduction attack on inverter 3



Threshold

Threshold



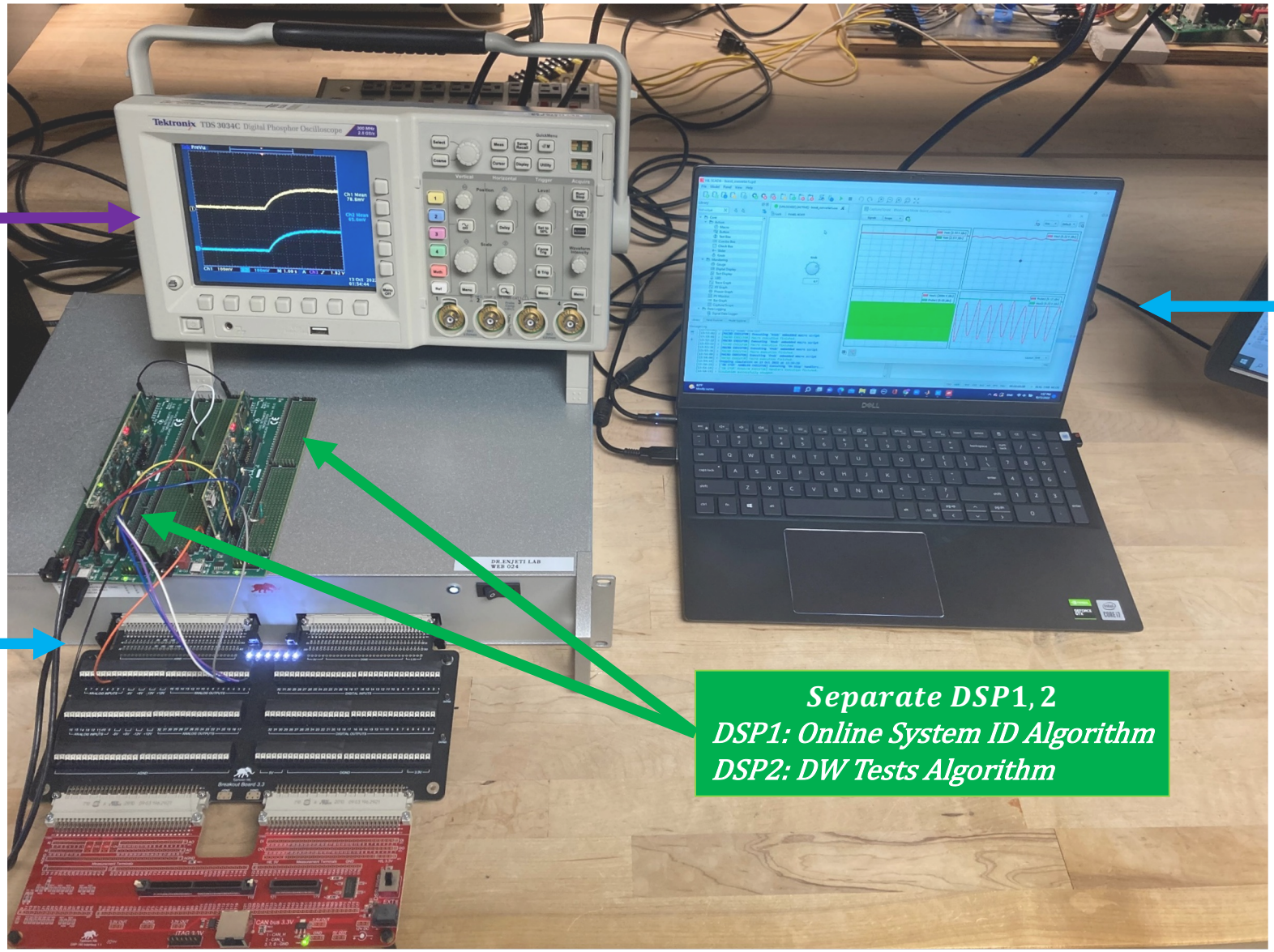


Normal operation (Inv 6)

Typhoon HIL

Amplitude Reduction (Inv 3)

Implementing on-line system identification on DSP



Oscioscilloscope DW Tests

Real – time simulation in Typhoon HIL Software

Typhoon HIL

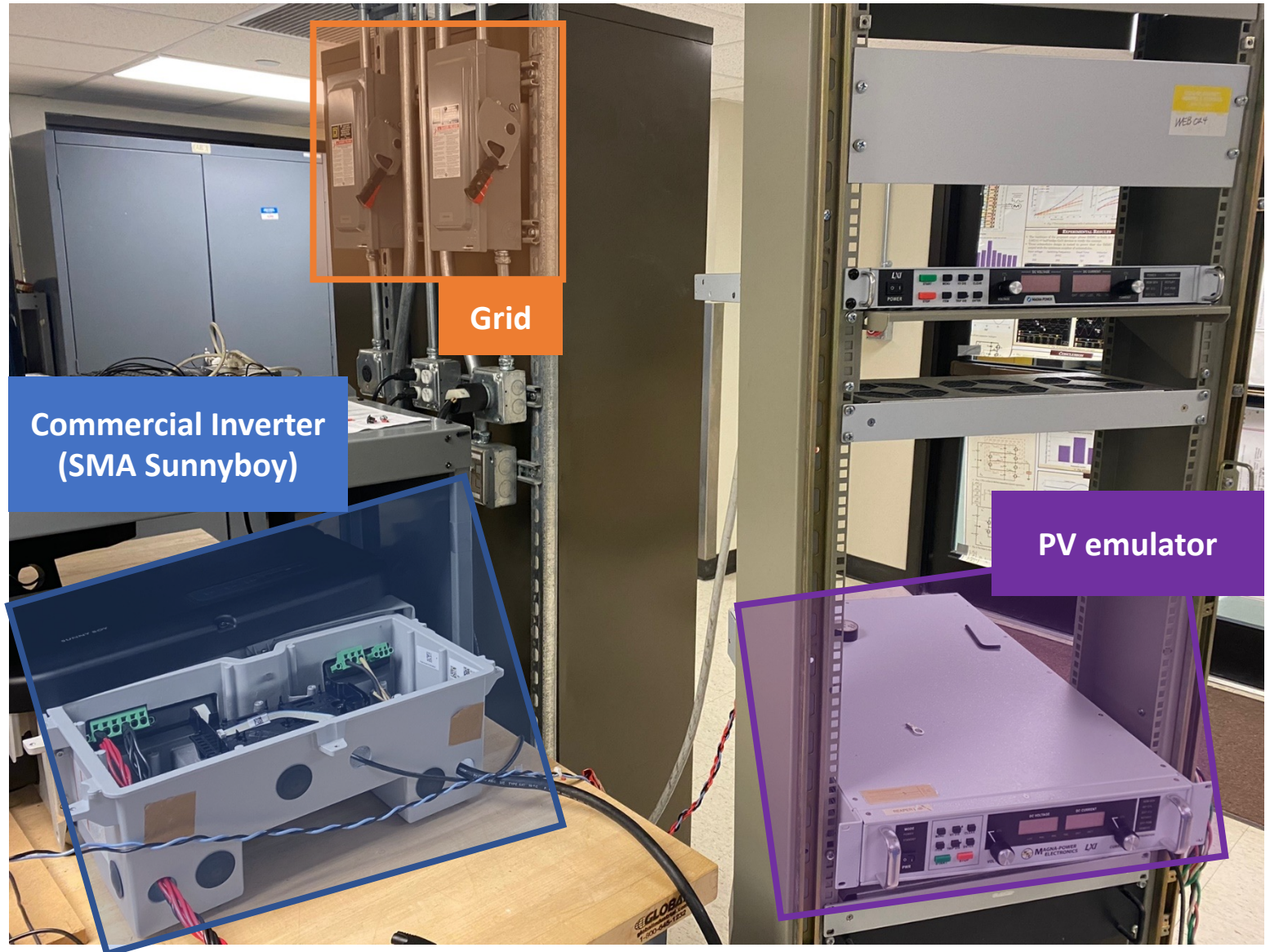
Typhoon HIL Hardware emulator

Separate DSP1, 2
DSP1: Online System ID Algorithm
DSP2: DW Tests Algorithm

Commercial grid connected Inverter (SMA Sunny Boy 3.8-US)

Technical data	Sunny Boy 3.0-US		Sunny Boy 3.8-US		Sunny Boy 5.0-US	
	208 V	240 V	208 V	240 V	208 V	240 V
Input (DC)						
Max. PV power	4800 Wp		6144 Wp		8000 Wp	
Max. DC voltage			600 V			
Rated MPP voltage range	155 - 480 V		195 - 480 V		220 – 480 V	
MPPT operating voltage range			100 – 550 V			
Min. DC voltage / start voltage			100 V / 125 V			
Max. operating input current per MPPT			10 A			
Max. short circuit current per MPPT			18 A			
Number of MPPT tracker / string per MPPT tracker	2/1				3 / 1	
Output (AC)						
AC nominal power	3000 W	3000 W	3330 W	3840 W	5000 W	5000 W
Max. AC apparent power	3000 VA	3000 VA	3330 VA	3840 VA	5000 VA	5000 VA
Nominal voltage / adjustable	208 V / ●	240 V / ●	208 V / ●	240 V / ●	208 V / ●	240 V / ●
AC voltage range	183 – 229 V	211 – 264 V	183 – 229 V	211 – 264 V	183 – 229 V	211 – 264 V
AC grid frequency			60 Hz / 50 Hz			
Max. output current	14.5 A	12.5 A	16.0 A	16.0 A	24.0 A	21.0 A
Power factor (cos ϕ)			1			
Output phases / line connections			1 / 2			
Harmonics			< 4 %			

Commercial grid connected Inverter (SMA Sunny Boy 3.8-US) Hardware set-up in the Lab



- Texas A&M team working on
  - Implementing real-time/on-line system identification on DSP
  - Testing the DW method on a commercial SMA Sunny Boy 3.8-US PV grid connected inverter in the lab

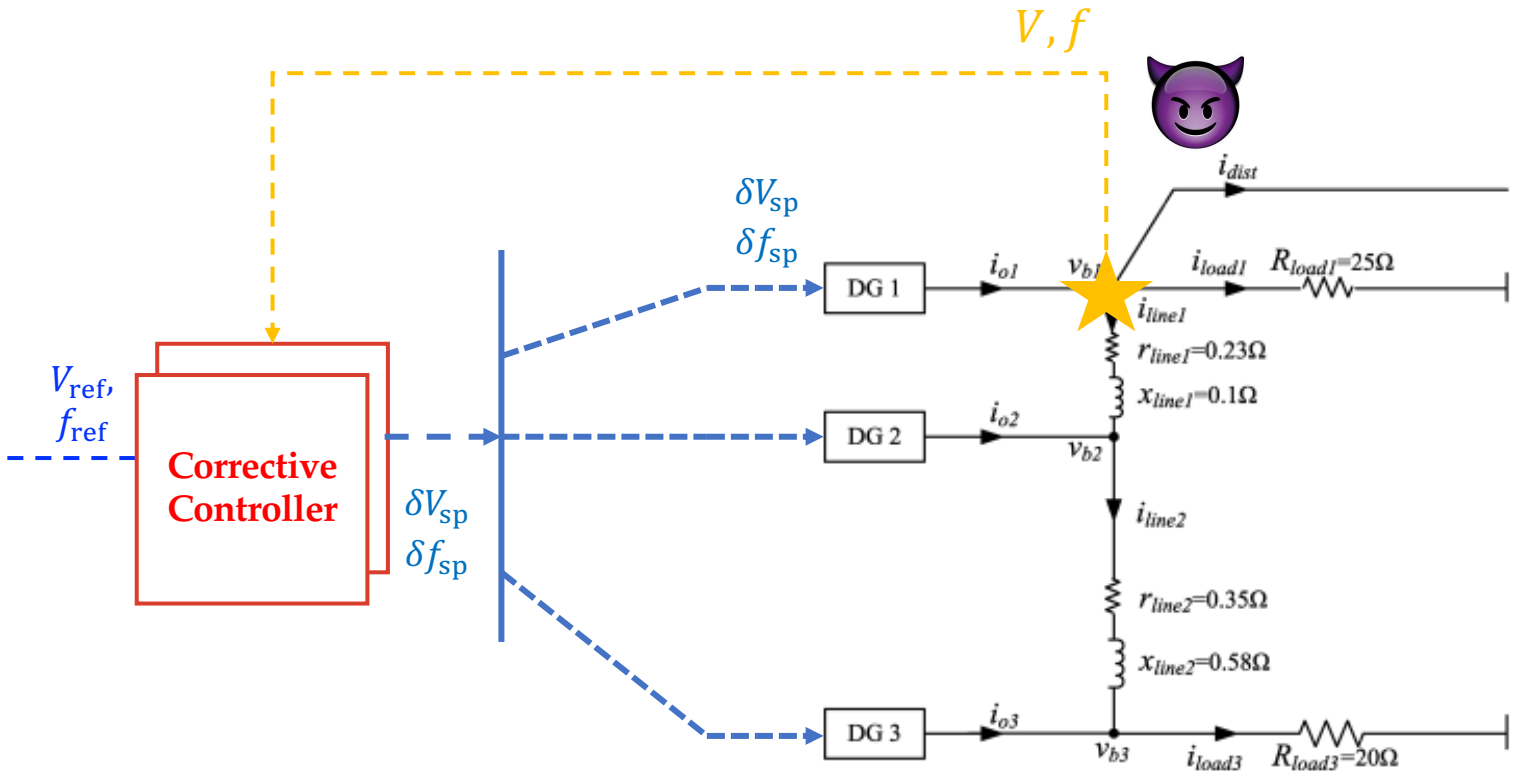
Cyber-resilient control

- The distribution system to be studied can be stabilized in the presence of PV fluctuations.
- The protection and control scheme is shown to stabilize the system within a few minutes under unknown cyberattacks.

T. Huang, D. Wu, and M. Ilic, "Cyber-resilient Automatic Generation Control for Systems of Microgrids," MIT working paper, to submit to IEEE Transactions on Smart Grid.

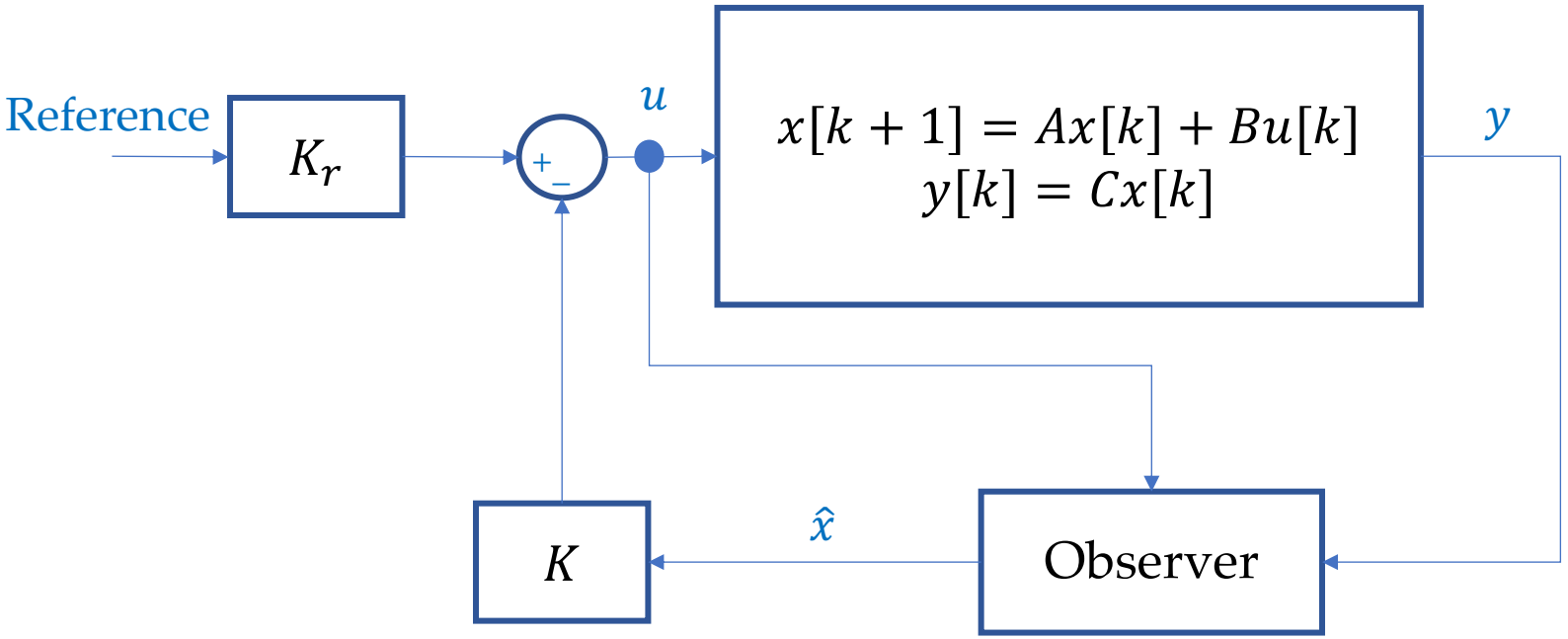
D. Wu, P. Bharadwaj, P. Rowles, and M. Ilic, "Cyber-Physical Secure Observer-Based Corrective Control under Compromised Sensor Measurements," *2022 American Control Conference*.

Corrective Secondary Control

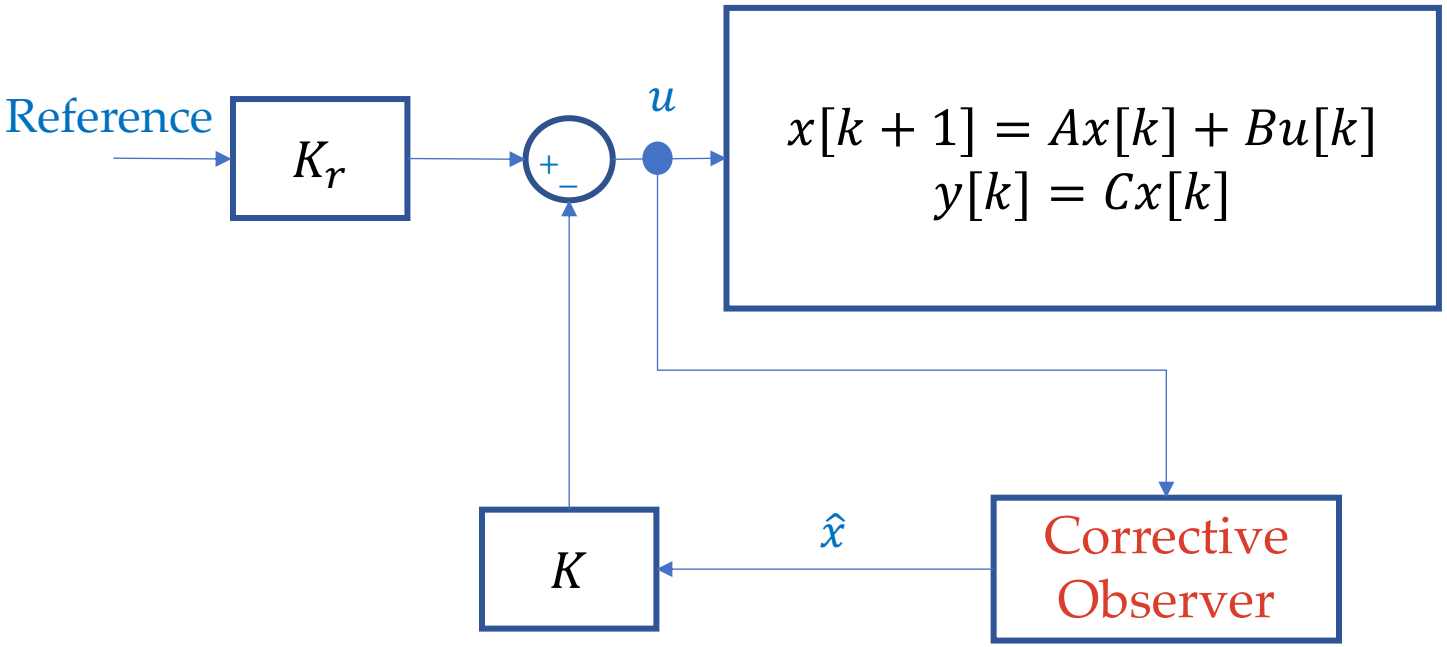


- Secondary control architecture
- Cyber vulnerability
- If cyber attack occurs, we switch to a corrective controller to achieve the control objectives

Secondary Control Design (No Attack)

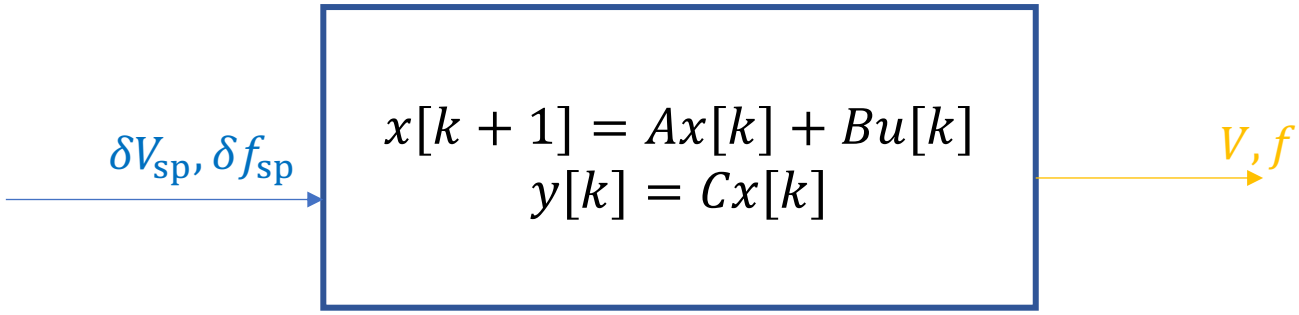


Corrective Secondary Control Design



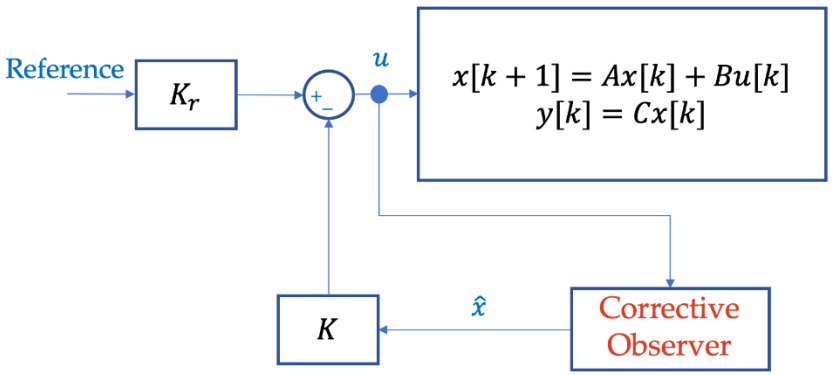
D. Wu, P. Bharadwaj, P. Rowles, and M. Ilic, "Cyber-Physical Secure Observer-Based Corrective Control under Compromised Sensor Measurements," *2022 American Control Conference*.

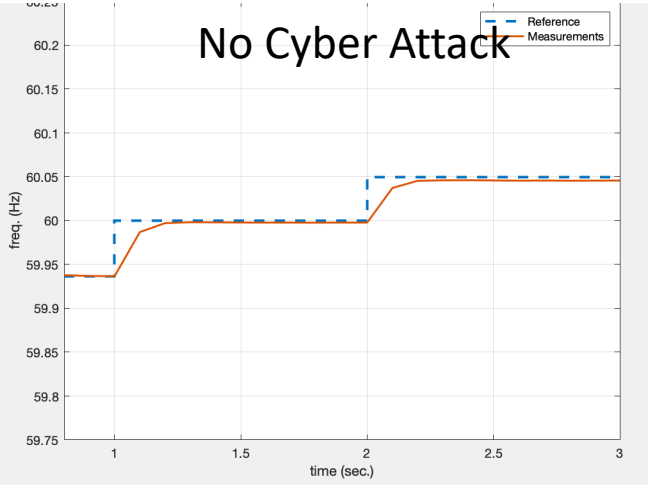
Obtain System Matrix

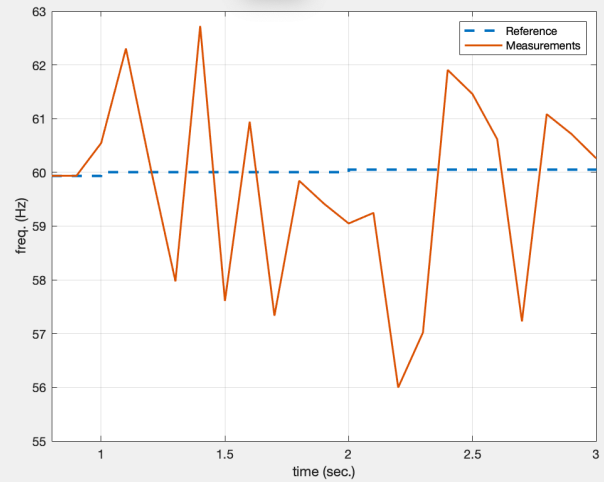


- Corrective control design requires the system model
- We can identify A, B and C from input and output data
- Inject white noise to the Simulink model ($\mathrm{Var}(\delta V_{sp}) = \mathrm{Var}(\delta f_{sp}) = 5$)

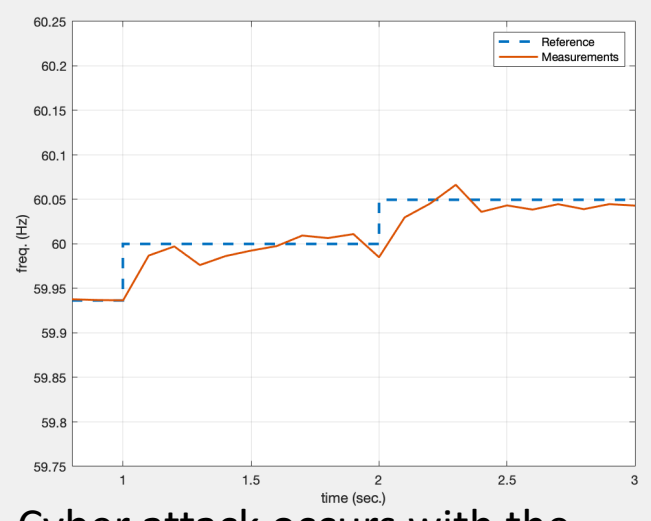
Secondary Corrective Control







Cyber attack occurs without the corrective control

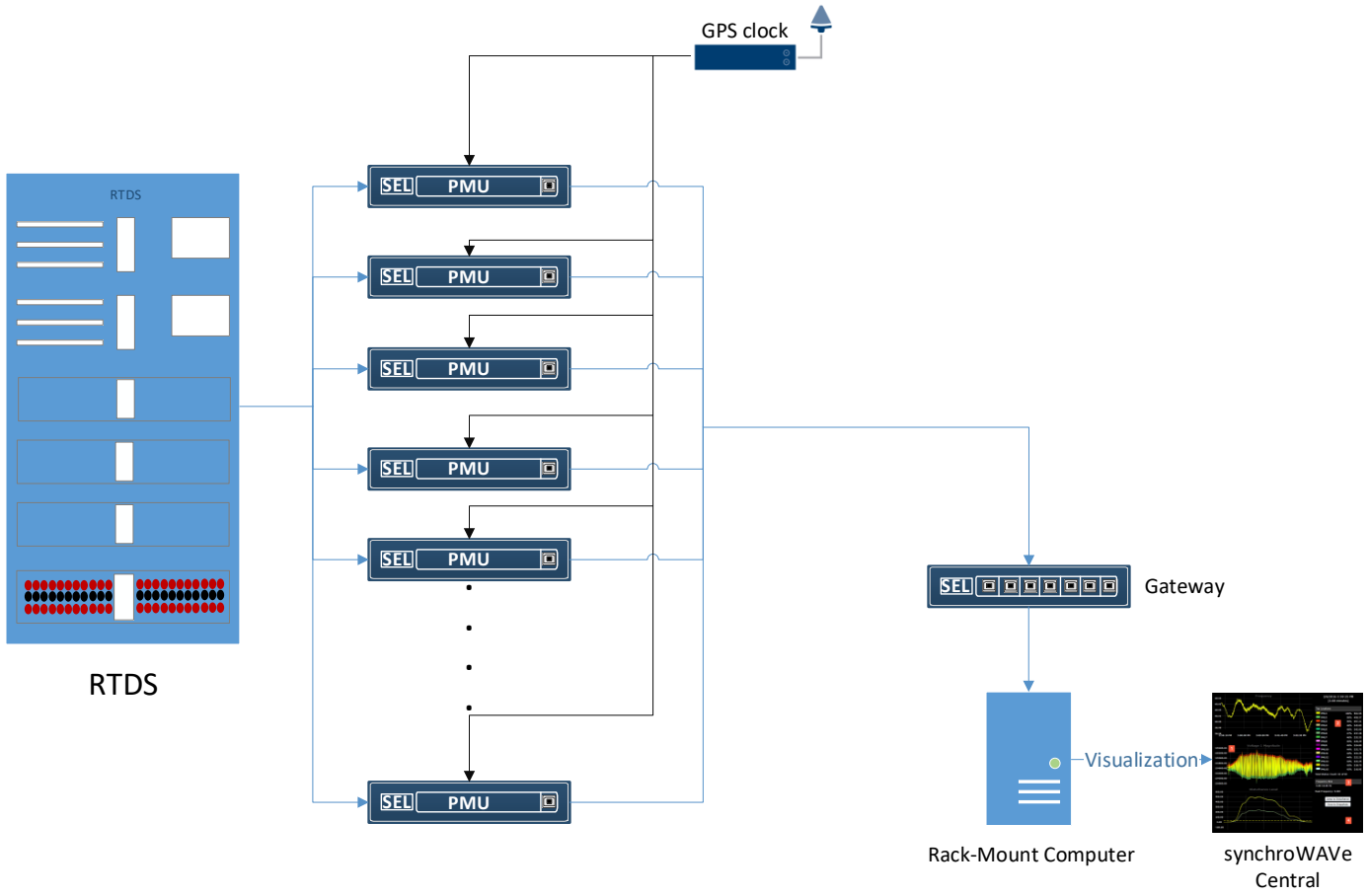


Cyber attack occurs with the corrective control

IIT RTDS Lab

- Setup and Configuration:
  - Two NovaCor racks (processing unit), each with 4 licensed cores
  - GTNETx2 card (communication unit) with SKT and DNP3 protocols
  - Four 16-channel output cards (GTAO)
  - Digital panel I/O
  - NovaCor Cubicle
  - RSCAD software educational license
  - Connected to the IIT network
  - PMUs
    - 4 SEL-351S relays
    - 2 SEL-451 relays
    - 4 SEL-751 relays
    - Time Synchronization: SEL-2488 Satellite-Synchronized Network Clock
    - Ethernet Switch: SEL-2730U Unmanaged 24-Port Ethernet Switch
    - Rack Mount Computer: SEL-3355 Automation Controller
    - Display and Analysis: SEL-5078-2 synchroWAVe Central

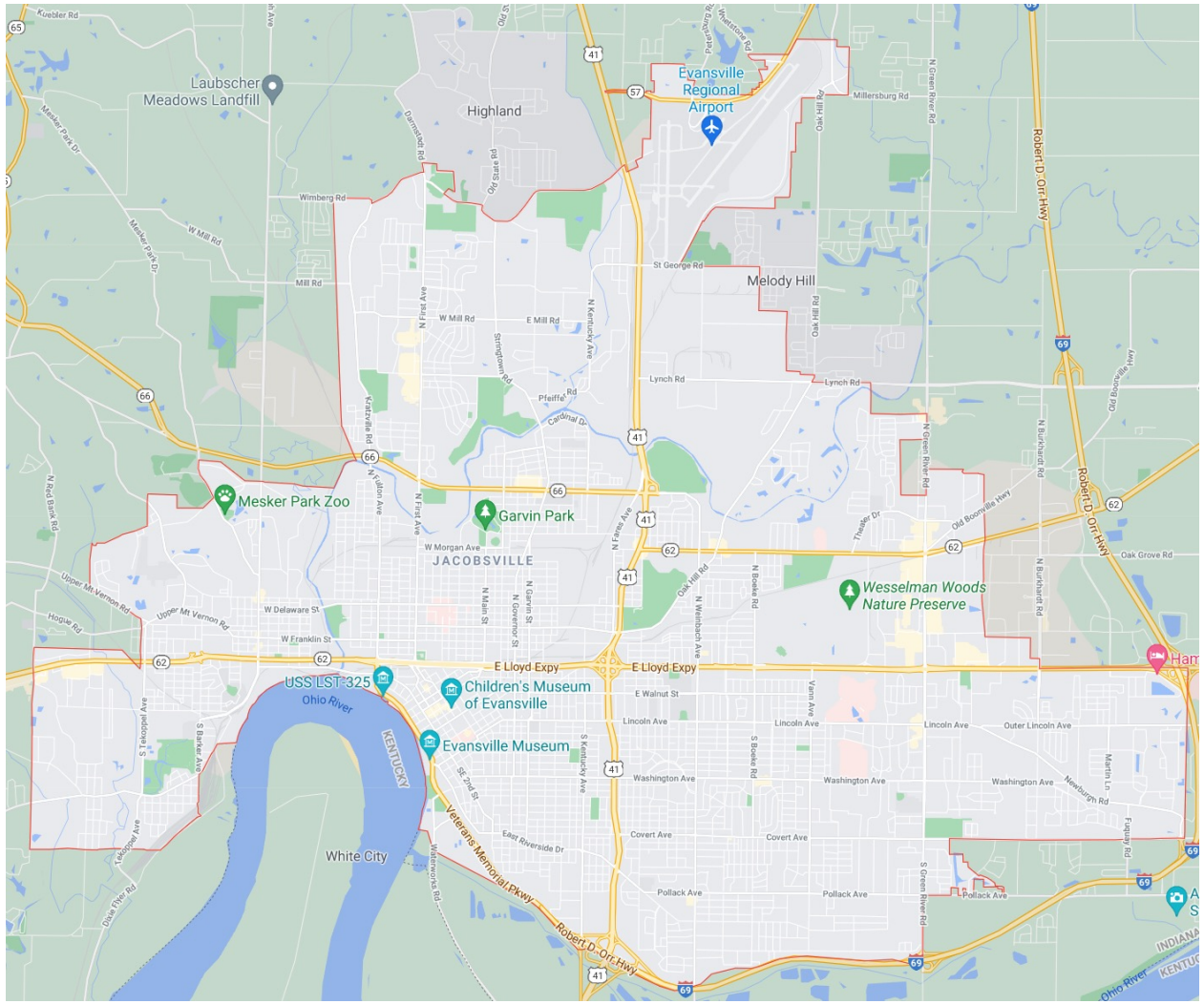
IIT RTDS Lab


GPS clock
RTDS
SEL PMU
SEL PMU
SEL PMU
SEL PMU
SEL PMU
SEL PMU
SEL
Gateway
Visualization
Rack-Mount Computer
synchroWAVe Central


SEL
SCHWEITZER ENGINEERING LABORATORIES

CenterPoint Energy Solar Farm in Evansville, IN

- Two subsystems
  - Oak Hill Solar Farm
  - Volkman Solar Farm
- Oak Hill Solar Farm
  - 2 MW solar field
- Volkman Solar Farm
  - 2 MW solar field
  - 1 MW battery storage
- Provides enough power to about 600 customers annually



Evansville, IN

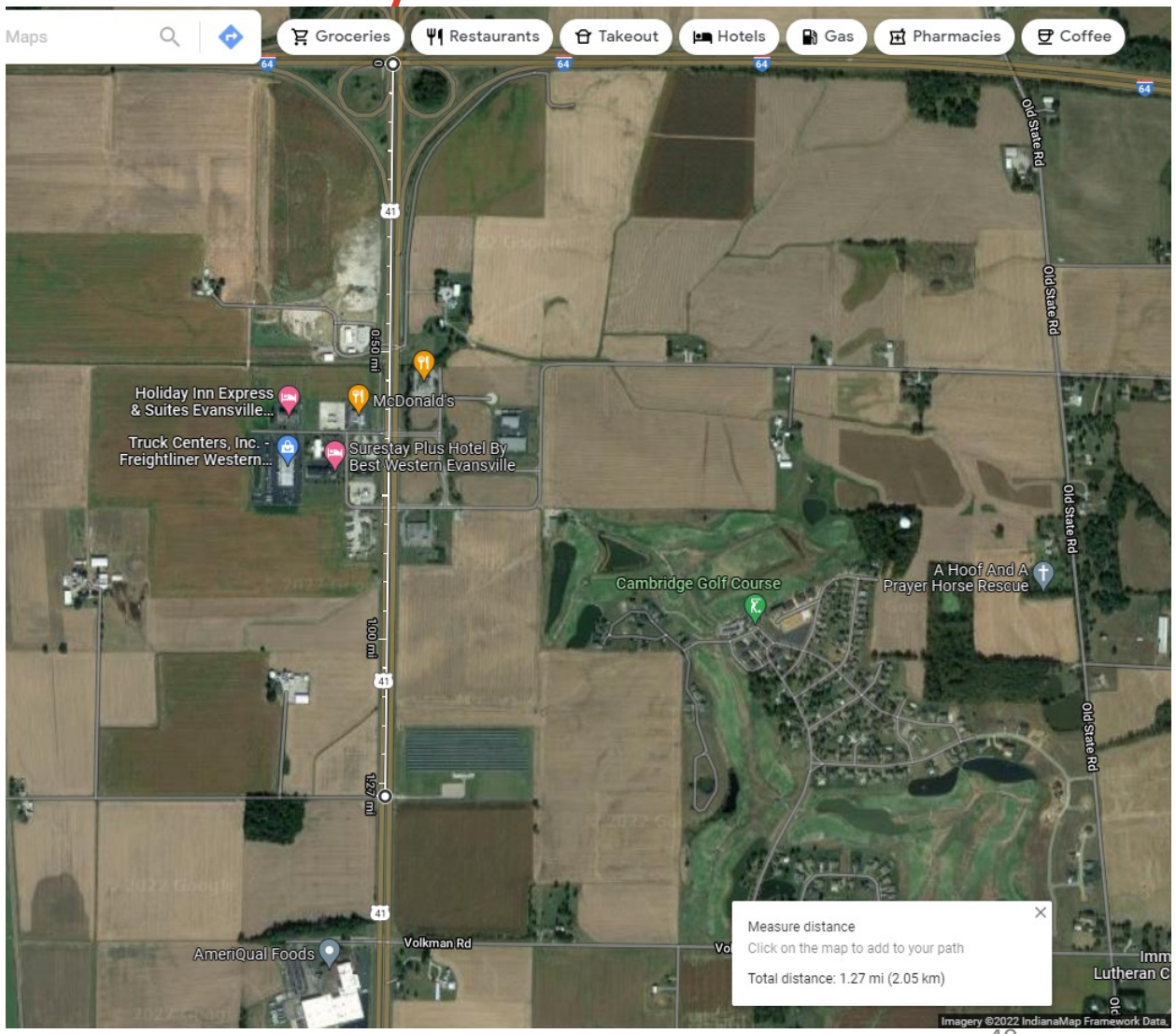
Oak Hill Solar Farm: A Summary

- 7,784 solar panels: 2 MW
  - 350W
  - 38.9V
  - 9.00A
- Single 2.5 MW inverter

Oak Hill Solar Farm

Volkman Solar Farm: A Summary

- 7,784 solar panels: 2 MW
  - 350W
  - 38.9V
  - 9.00A
  - Single 2.5 MW inverter
- 1 MW Battery
  - 18 racks of 17 battery modules: 306 modules
  - 290AH
  - Single 1.169 MW inverter



Volkman Solar Farm

Summary

- Provide an end-to-end ***monitoring framework*** of cyber-physical systems for ***solar-rich power distribution grids***
- Provide *a general-purpose cyber-attack defense methodology through Dynamic Watermarking*
- A*n online system identification for overcoming the requirement to know the system model*
- Scaled-up experimentation on actual microgrid

Future / On-going works:

- *Actual demonstration on CenterPoint Energy's solar farm*
- *Experiment on commercial grid connected Inverter systems*
- *Technology transfer*
- *Application to other cyber-physical systems*