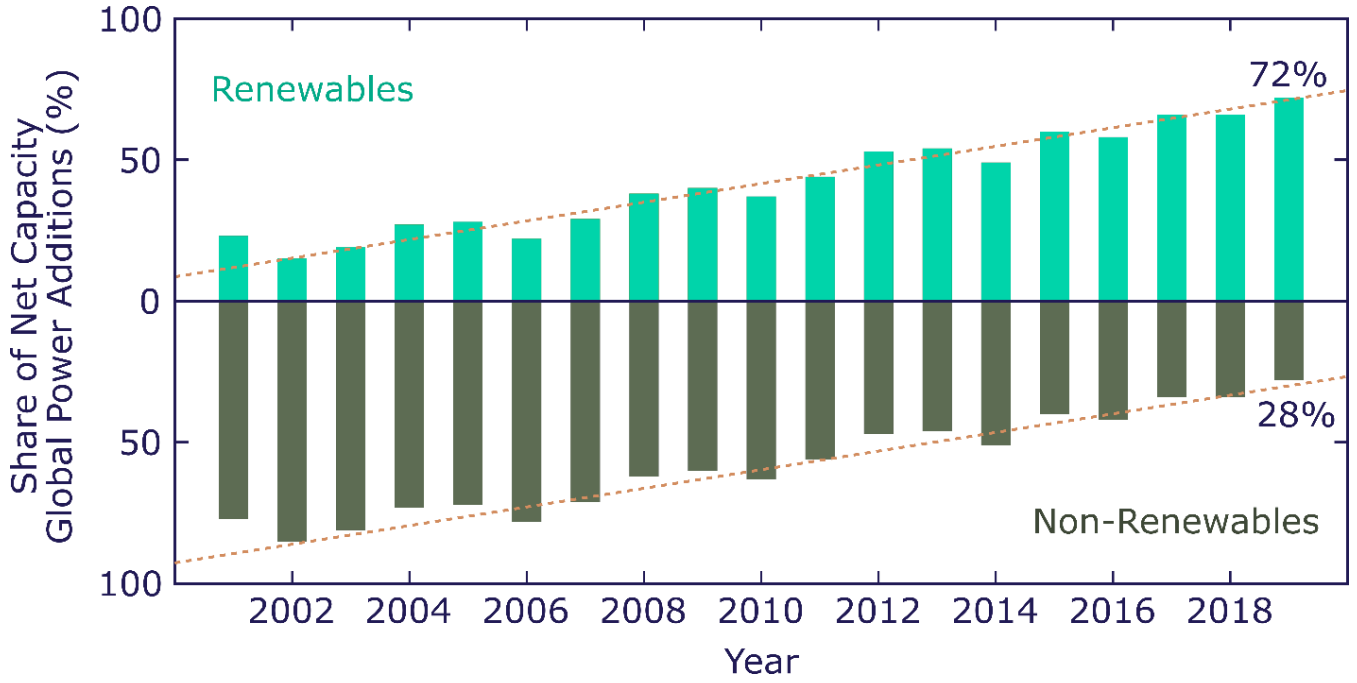
AALBORG UNIVERSITET

Self-Healing Cybersecure Microgrids

Subham Sahoo
Assistant Professor
Section for Applied Power Electronic Systems
Department of Energy
Website: www.energy.aau.dk

Monitoring of Power Systems



RES and non-RES as a share of the net total annual additions

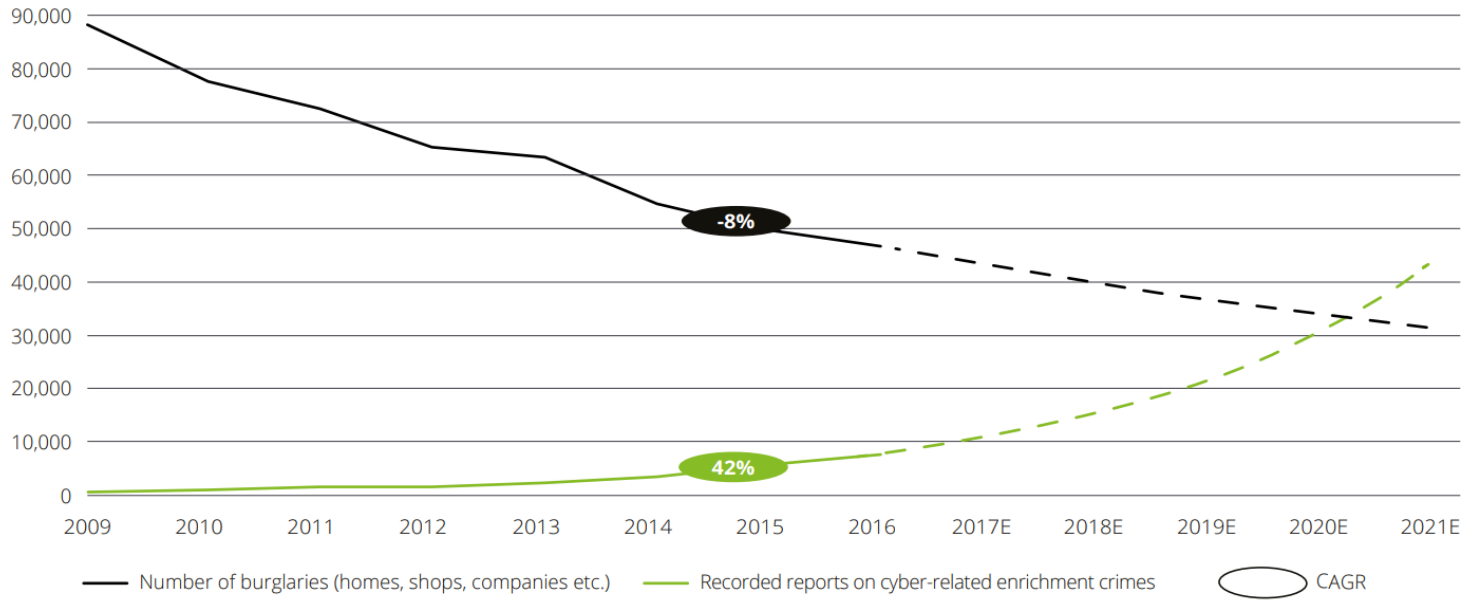
(Source: IRENA, "Renewable energy capacity statistics 2020", http://www.irena.org/publications, March 2020)

- Modern grids require health monitoring of equipments
- Growing facilities – sensors, data, processors, communication
- Power electronic converters dominating every energy sector

Hence, cybersecurity risks have gone up

Denmark Acknowledges the Threat

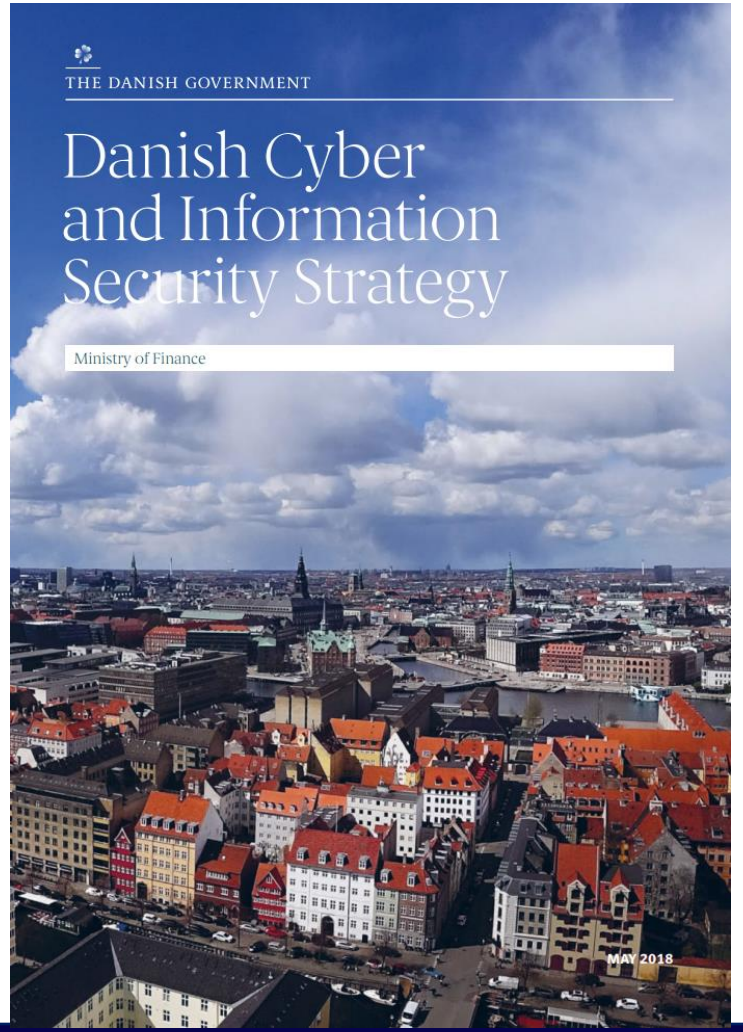
Source: Danish Police, Danmarks Statistik



Cyber related crimes are increasing everyday in Denmark

- Denmark is one of the digital front runners in the world
- Denmark primarily focuses on three key trends in digitalization:
  - Cybersecurity competences
  - Secure networks
  - Security by design

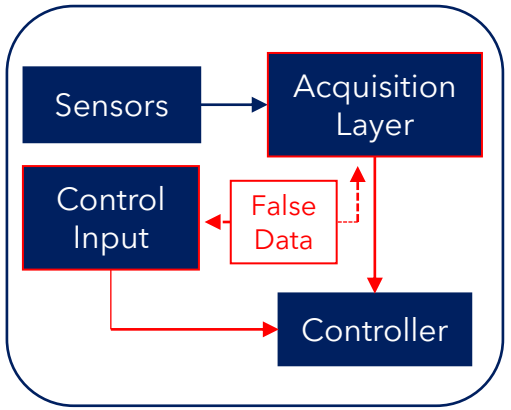
Source: Danish Cyber and Information Security Strategy, The Danish Government



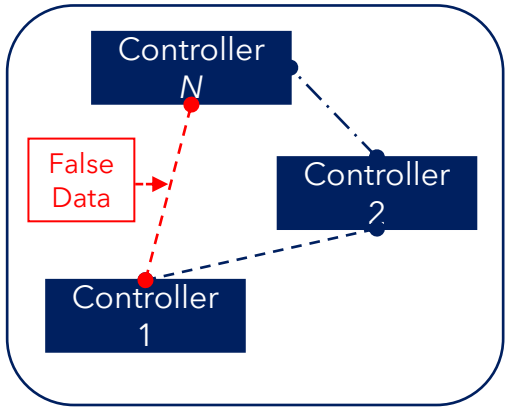
Cyber Attacks[1]

A cyber attack is a

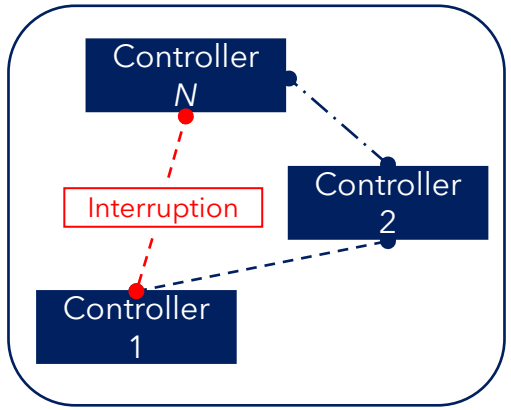
- third-party excitation
- conducted in an illegitimate manner
- by injecting
  - false data on single/multiple sensors, communication links, actuators
- by denying
  - Information from single/multiple sensors, communication links, actuators
- with the capacity to disorient system objectives/goals



False Data Injection Attack (FDIA)



Man-in-the-Middle Attack (MITM)



Denial of Service (DoS)

[1]Recognized by the US Government Accountability Office (GAO), North American Electric Reliability Corporation (NERC)

Cyber Attacks – Last Decade

2010
Iran
Cause: Stuxnet

2012
Saudi Arabia
Cause: Shamoon

2014
South Korea
Data theft

2015
Ukraine
Highest Impact
Many electric substations disconnected from the grid; affecting 225,000 customers

2016
Ukraine
No electricity for an hour

Secure PELS Era?

Vestas (Source: Vestas)

Vestas impacted by cyber security incident

Vestas Wind Systems A/S, Aarhus, 20 November 2021

Company announcement no. 22/2021

Vestas has on 19 November 2021 been impacted by a cyber security incident. To contain the issue, IT systems are shut down across multiple business units and locations.

As part of our crisis management setup for cyber security, we are working together with our internal and external partners to contain the issue fully and recover our systems.

Customers, employees and other stakeholders may be affected by the shutdown of several of our IT-systems.

We will provide further updates when we have more information.

Hackers Remotely Kill a Jeep on the Highway—With Me in It

(Source: Wired)

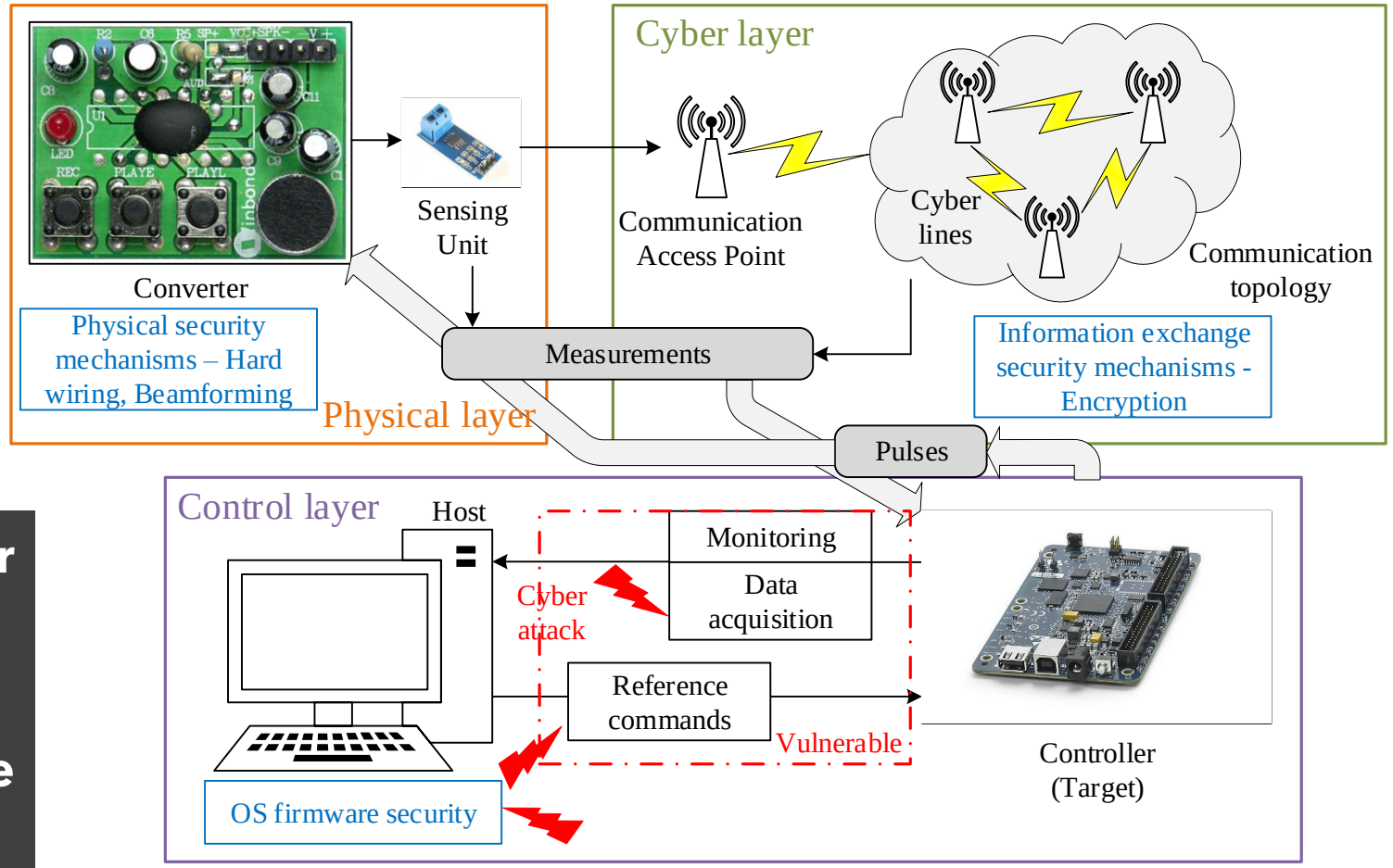
(Source: Forbes)

This Man Hacked His Own Solar Panels... And Claims 1,000 More Homes Vulnerable

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

Vulnerabilities

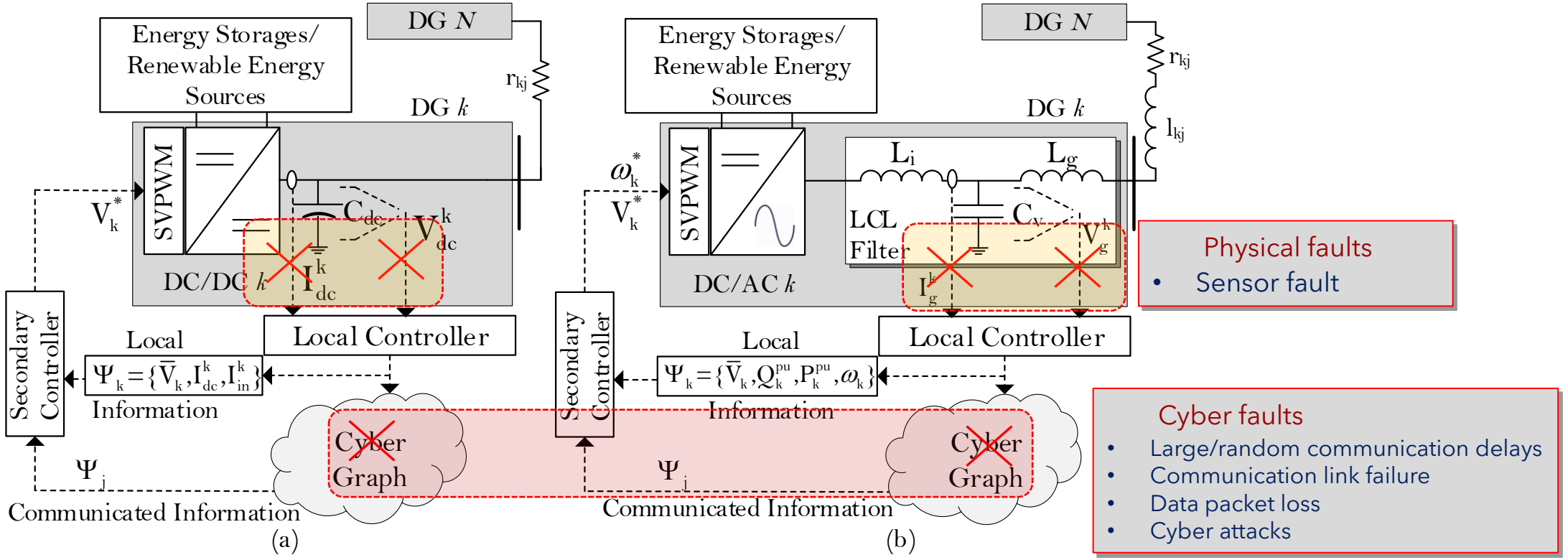


The point of access by the attacker is NOT important

The final target point is more important

Source: S. Sahoo, JCH Peng, S Mishra, T Dragicevic, "Distributed Screening of Hijacking Attacks in DC Microgrids," IEEE Trans. Power Electron., vol. 35, no. 7, pp. 7574-7582, 2019.

Cy-Phy Power Electronics Platform



(a) DC Islanded Network, (b) AC Islanded Network

Attack Detection Surface for Power Electronics

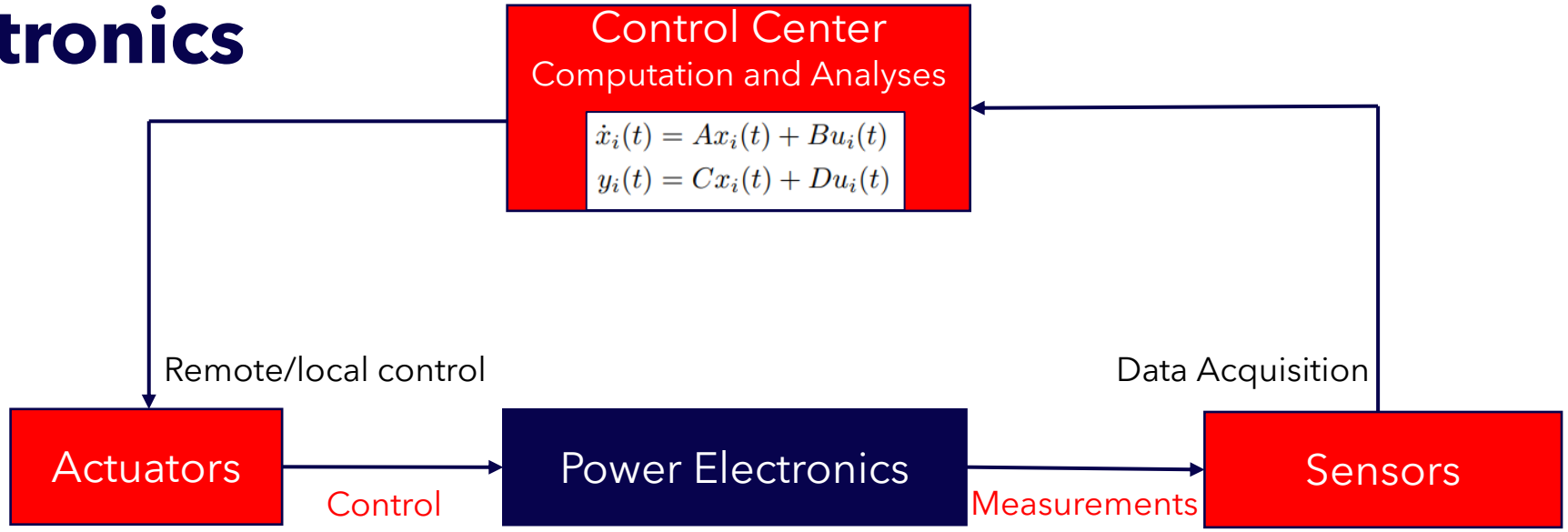


Fig. **Attacked** power electronics control structure

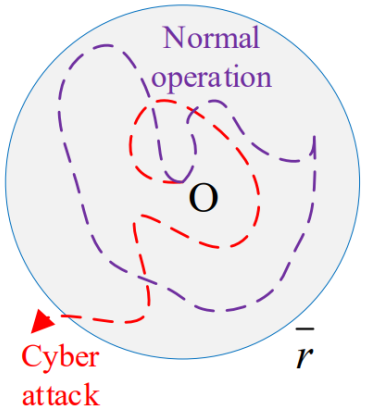


Fig. Attack detection surface

$$\dot{\hat{x}}_i(t) = (A + GC)\hat{x}_i(t) - Gy_i(t)$$
$$r_i(t) = C\hat{x}_i(t) - y_i(t)$$

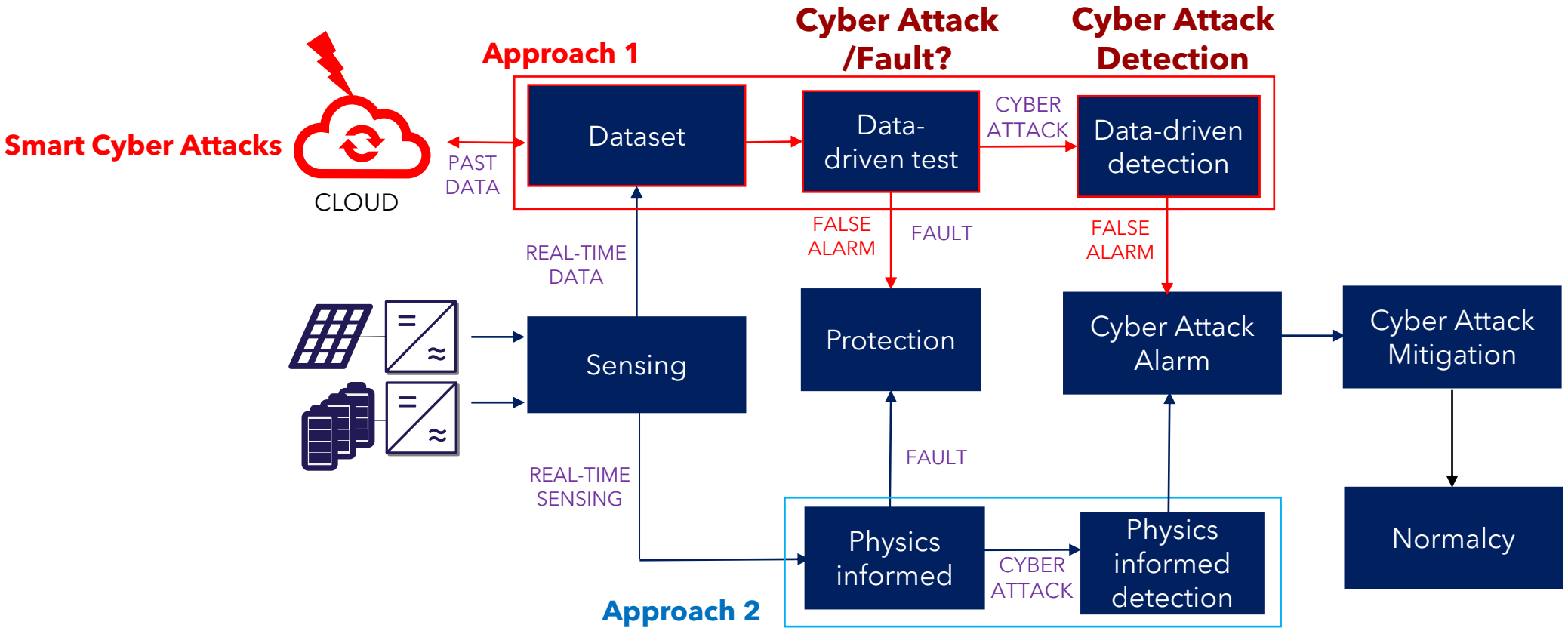
such that (A+GC) is Hurwitz.

Luenberger observer

Not our approach

Source: S Sahoo, T Dragicevic, F Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters - Challenges and Vulnerabilities", IEEE Journal of Emerging and Selected Topics in Power Electronics, Early Access, 2019.

Cyber Security Framework – A Perspective?



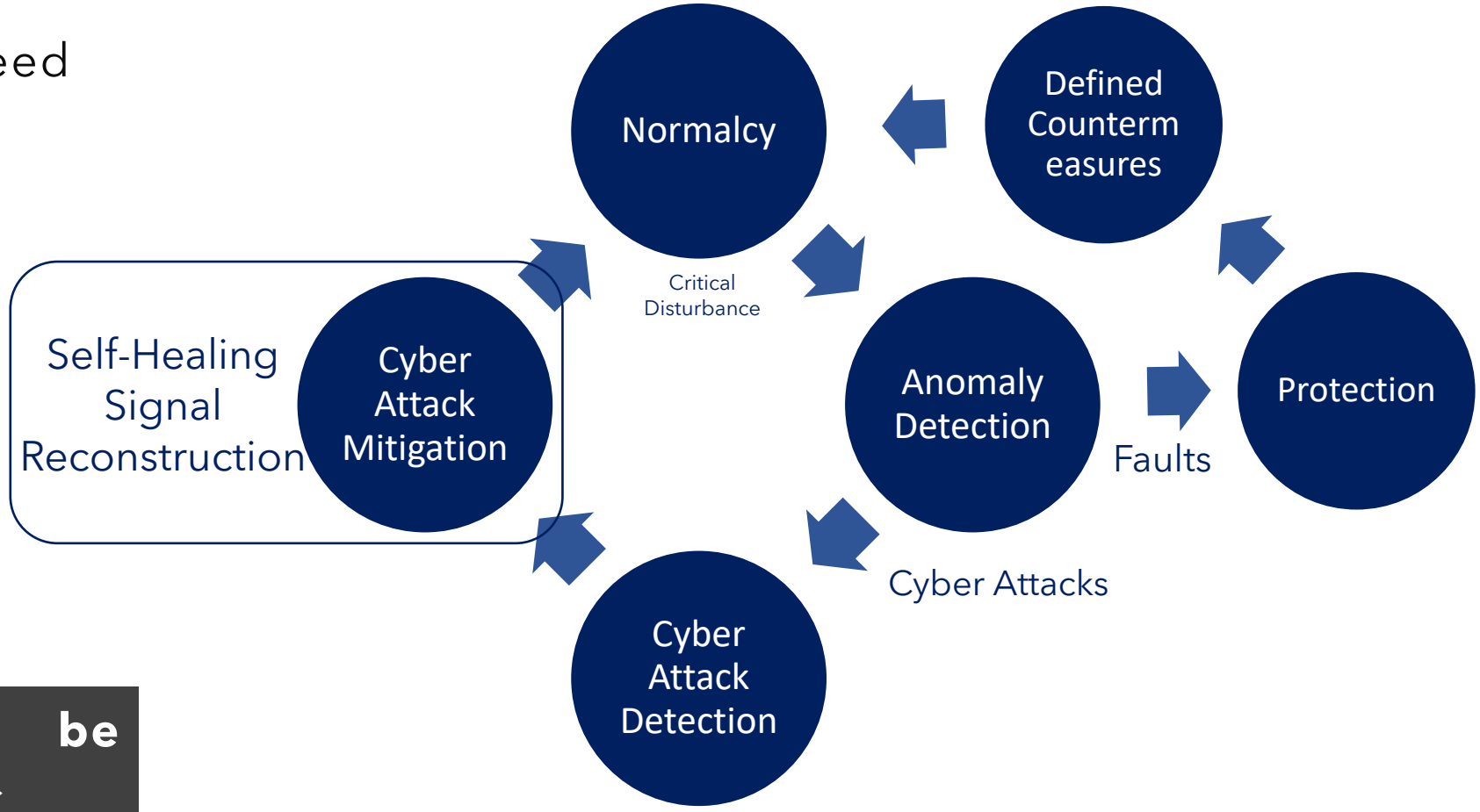
- Approach 1 – unreliable because of data (could always be manipulated)
- Approach 2 – Physics informed tools more reliable for security of PE

AALBORG UNIVERSITET

Cybersecurity Framework

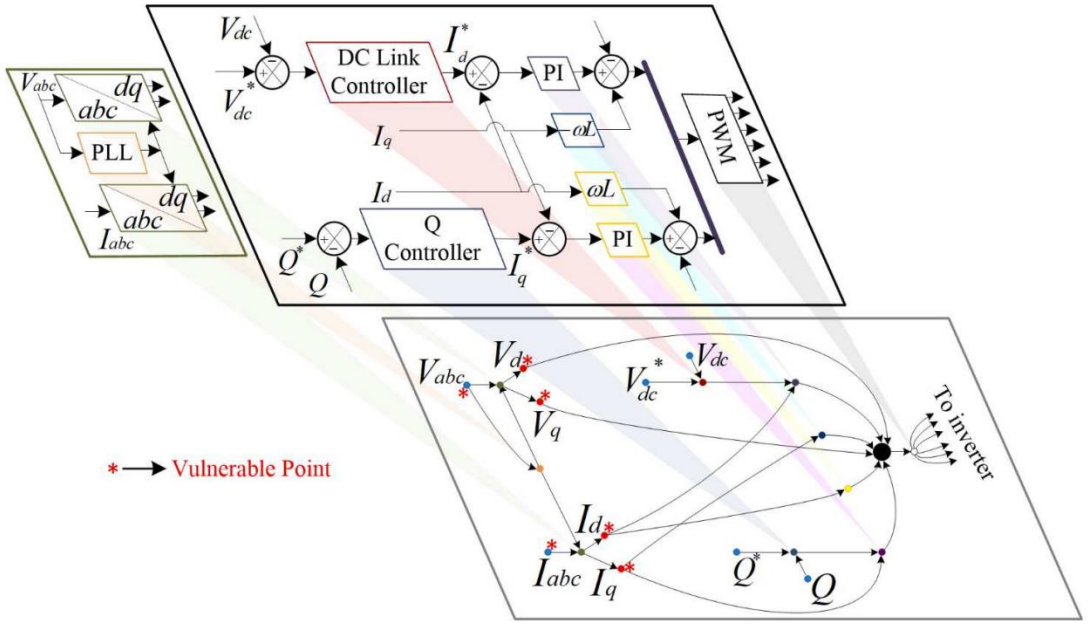
Cyber Security Framework

- Cybersecurity solutions need to be:
  - Fast
  - Accurate
  - Precise

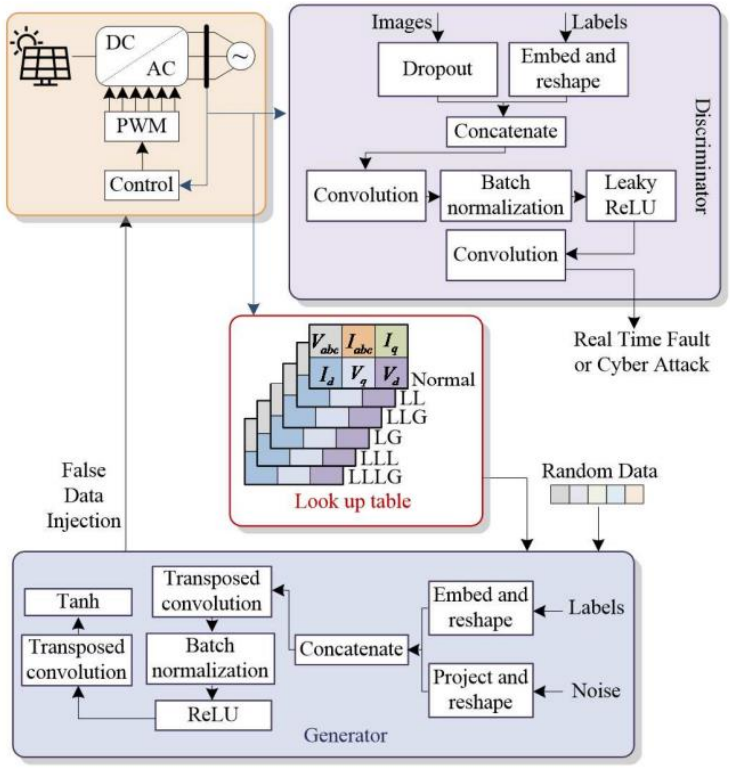


This framework needs to be completed in *few milliseconds*

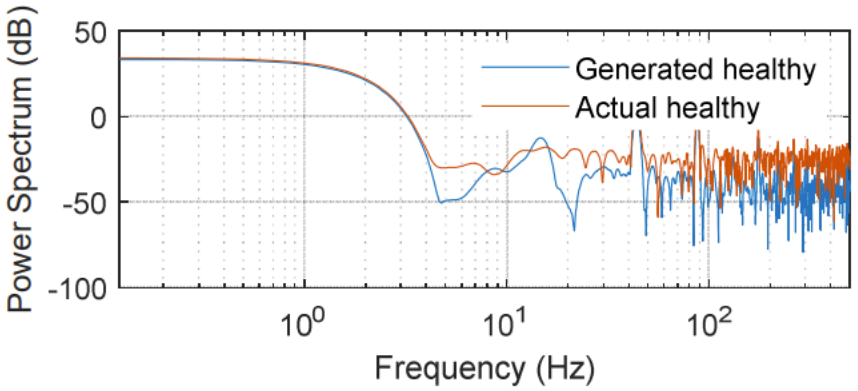
Cyber Attack Modeling

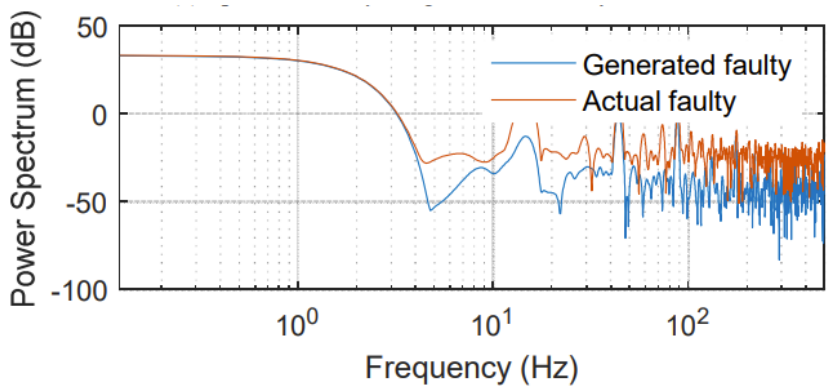


Graph theory model for prospective vulnerable points



Modeling using Generative Adversarial Networks



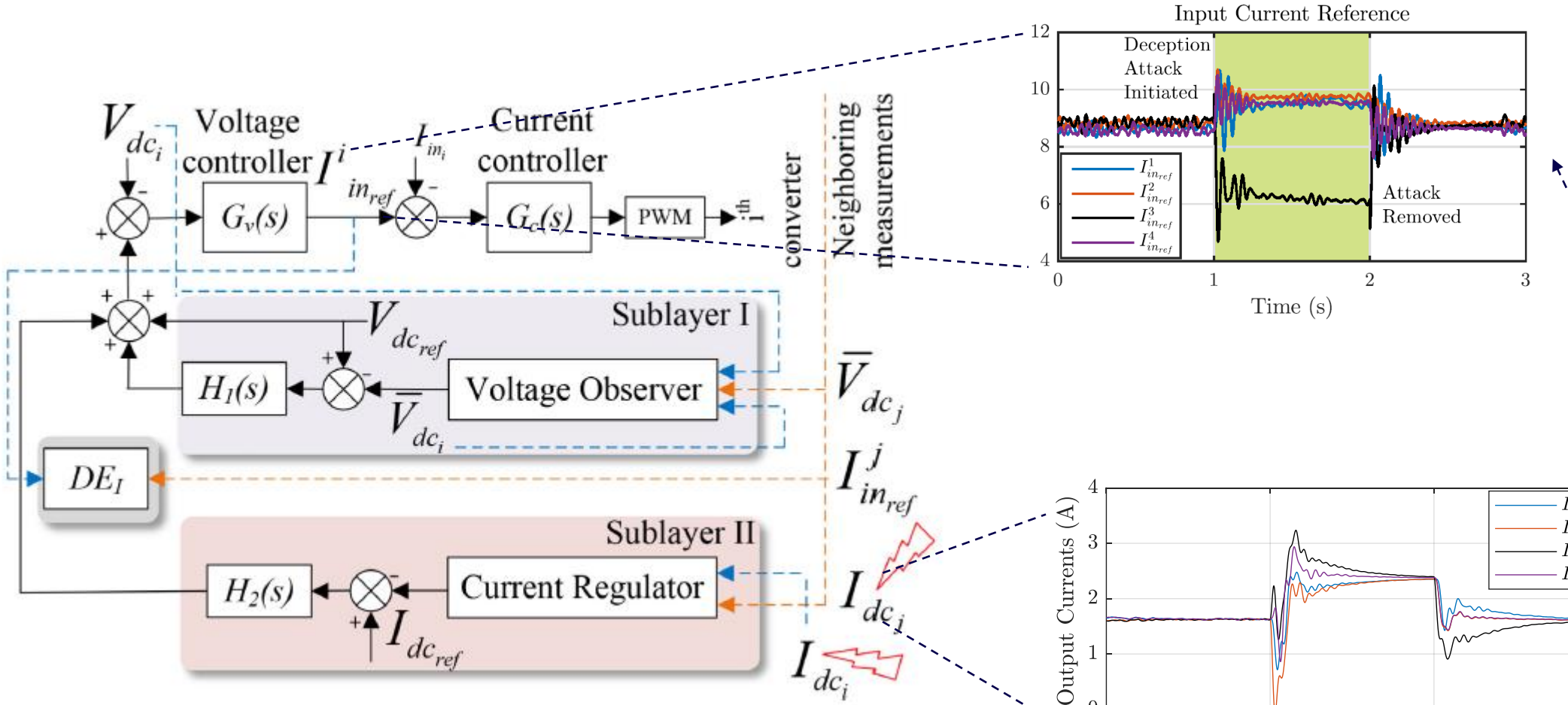


Anomaly Detection

- A non-invasive approach to determine between cyber attacks and faults
- The anomaly is diagnosed within **5 ms***
- We emphasize its design based on the protection systems configuration

*Measurements sampled at 1 kHz

Attack on Currents in DC Systems



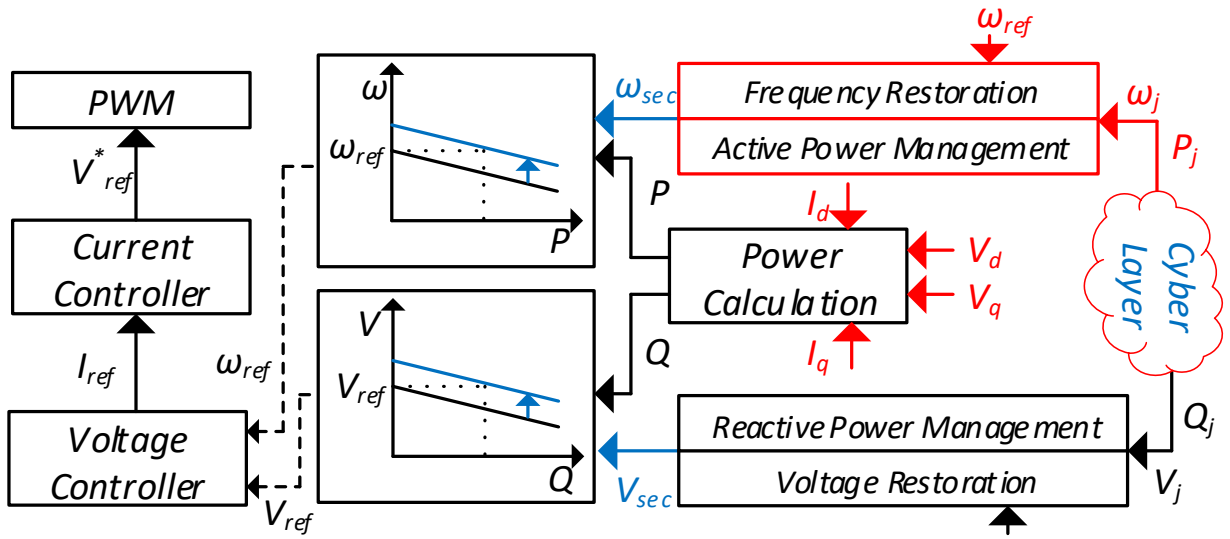
Disagreement

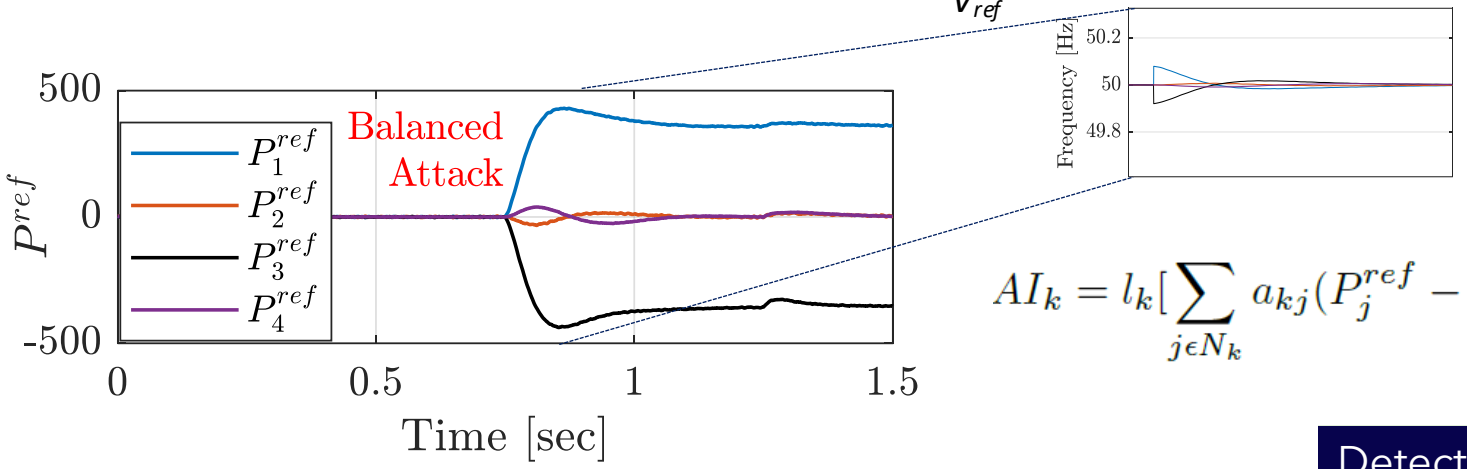
Detection Philosophy:
The consensusability law is broken under cyber attacks

Source: S Sahoo, JCH Peng, D Annavaram, S Mishra, T Dragicevic, "On Detection of False Data in Cooperative Microgrids – A Discordant Element Approach", IEEE Trans. Ind. Electron., vol. 67, no. 8, pp. 6562-6571, 2019.

Attack on Frequency in AC Systems

Cyber Attack Detection





$$AI_k = l_k[\sum_{j \epsilon N_k} a_{kj}(P_j^{ref} - P_k^{ref})][\sum_{j \epsilon N_k} a_{kj}(P_j^{ref} + P_k^{ref})]$$

Detection Philosophy:
The consensusability law is broken under cyber attacks

Source: S Sahoo, Y Yang and F Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks", IEEE Trans. Power Electron., vol. 36, no. 1, pp. 73-77, 2020.

Cyber Attack Detection - Summary

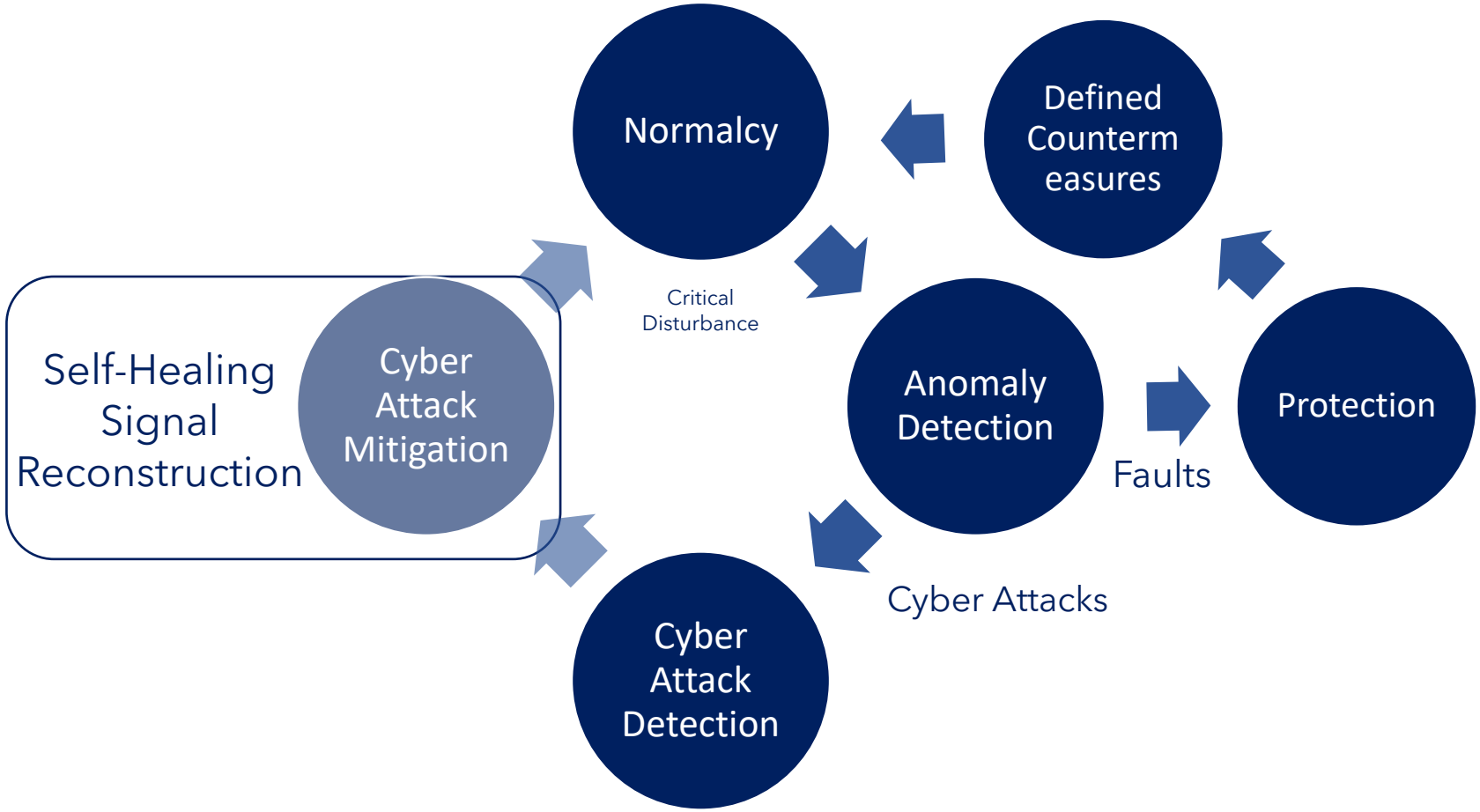
Cyber Attack Detection

$$|DI| = \begin{cases} \geq \beta, if\, \kappa = 1 \\ < \beta, else \end{cases}$$ **(Under Attack)**

Features of proposed attack detection metrics:

1. It does NOT require design of an observer
2. It does NOT need system information
3. It does NOT need historic data from system
4. It does NOT require additional resources

Cyber Security Framework



Towards Mitigation

Cyber Attack Mitigation

Detection

- Attacked measurement detected
- Stop communicating attacked measurement to other units

Authentication

- Assign authentication labels to each measurement upon detection of cyber attacks
- Authentication label of False (F) is assigned to attack measurements, and vice-versa

Mitigation

- Transmit corresponding measurements with authentication labels marked with True (T) to the attacked unit
- Reconstruct another signal using the trustworthy measurement and replace it with the attacked signal

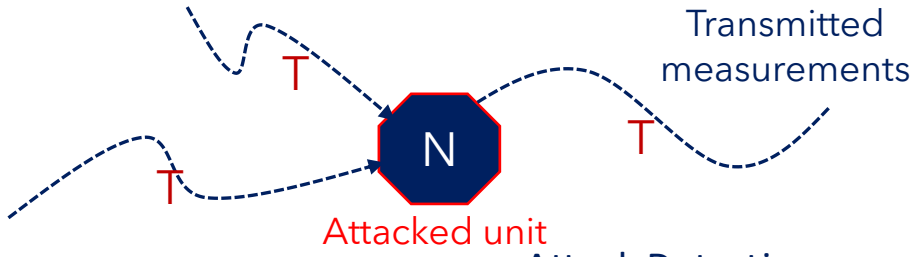
Self-Healing Signal Reconstruction

Cyber Attack Mitigation

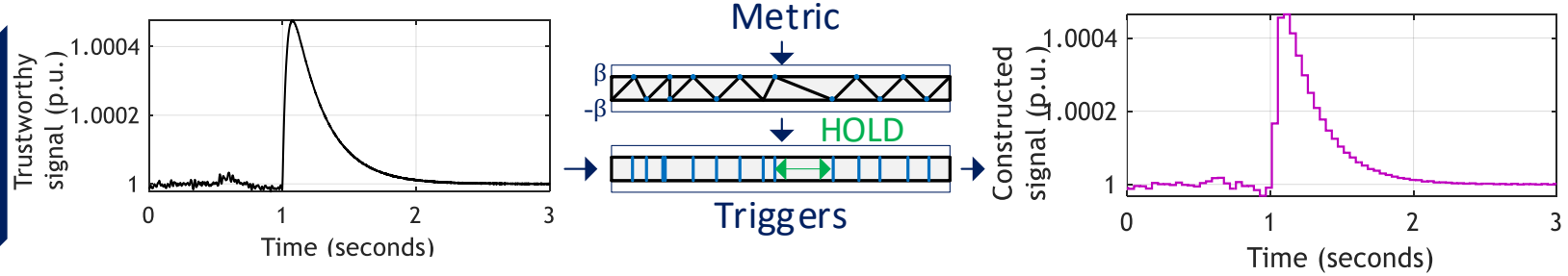
Detection

- Attacked measurement detected
- Stop communicating attacked measurement to other units

Authentication



Mitigation



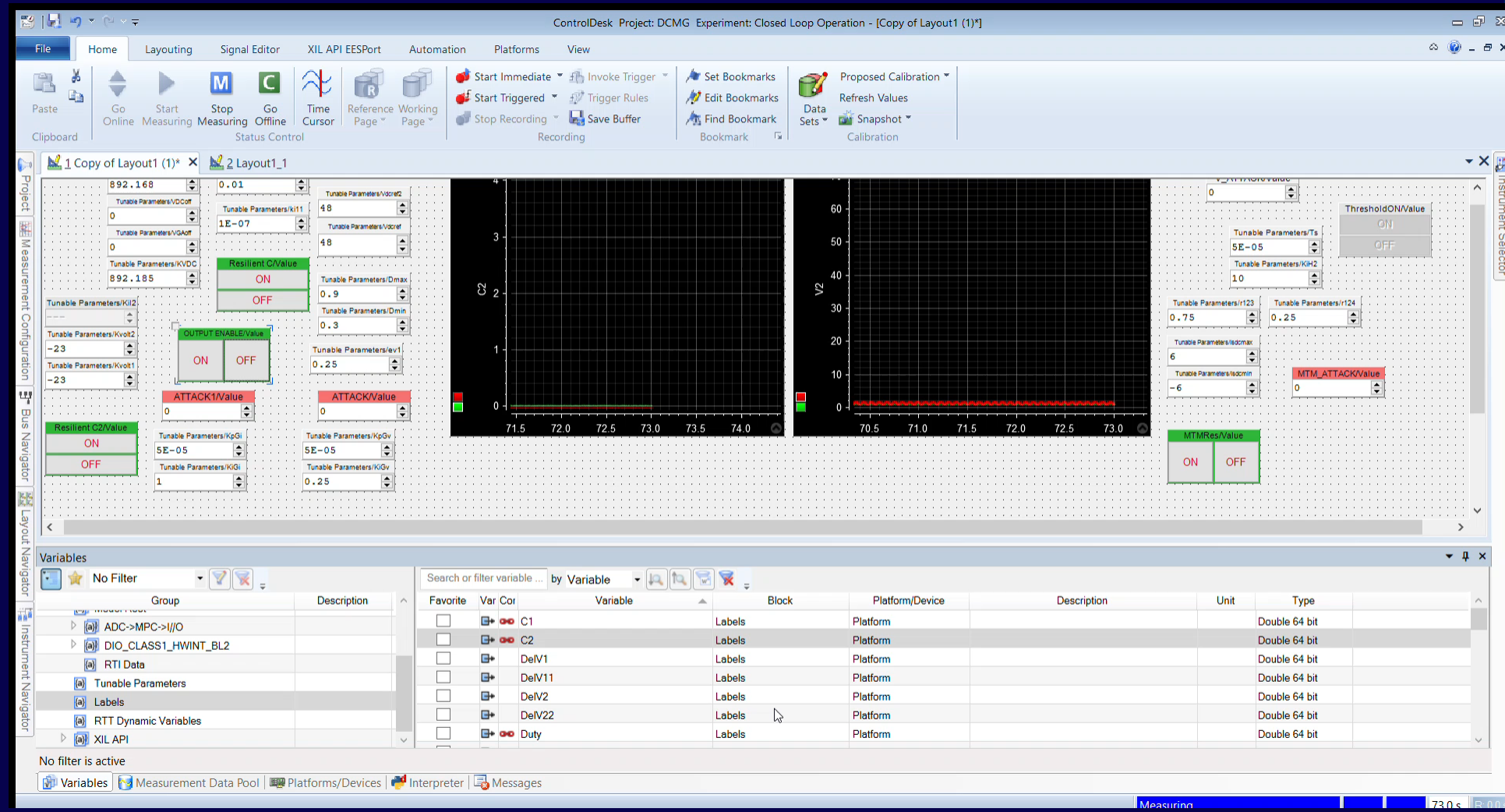
Attacked PE converter is used without any interruption, thereby healing the system from cyber attacks by itself

The presence of attack (identified using the defined cyber attack detection metrics) is termed as an "*event*"

Source: S Sahoo, T Dragicevic and F Blaabjerg, "An Event-Driven Resilient Control Strategy for DC Microgrids", IEEE Trans. Power Electron., vol. 35, no. 12, pp. 13714-13725, 2020.

AALBORG UNIVERSITET

Video



Source: S Sahoo, T Dragicevic and F Blaabjerg, "An Event-Driven Resilient Control Strategy for DC Microgrids", IEEE Trans. Power Electron., vol. 35, no. 12, pp. 13714-13725, 2020.

Features

- Different cyber attack models have been investigated
- Anomaly detection between cyber attacks and other malfunctioning events
- Physics-informed cyber attack detection metrics have been identified:
  - It does NOT require design of an observer
  - It does NOT need system information
  - It does NOT need historic data from system
  - It does NOT require additional resources
  - Analyzed for all prominent energy management schemes
- Event-driven signal reconstruction to mitigate cyber attacks:
  - Objective-oriented approach
  - Reports a resiliency scale of *N-1*
  - Resilient to noise
  - Feasible for worse case attack scenarios
- Computationally simple and easy to deploy

AALBORG UNIVERSITET

Questions?

Subham Sahoo
e-mail: sssa@energy.aau.dk