Imperial College
London

Cyber Resiliency of Digitalised Power Grids: can we keep the (most) lights on during major cyber intrusions?

Dr Fei Teng, f.teng@imperial.ac.uk
Imperial College London

A summary of research work from Dr Martin Higgins, Dr Wangkun Xu, Dr Pudong Ge, Dr Zhongda Chu and Dr Mengxiang Liu

Imperial College London

Cyberattack Incidents

2010

Stuxnet
Target: Iranian nuclear plant
Impact: Ruin of one-fifth nuclear centrifuges

Kimsuky
Target:Korea nuclear plant
Impact: Data leakage

BlackEnergy3
Target: Ukraine power grid
Impact: Power outage for 230000 consumers

2015

Industroyer
Target: Ukraine power grid
Impact: Cut one fifth of city's power consumption

2017

WannaCry
Target: Energy sectors
Impact: Data theft, Ransomware

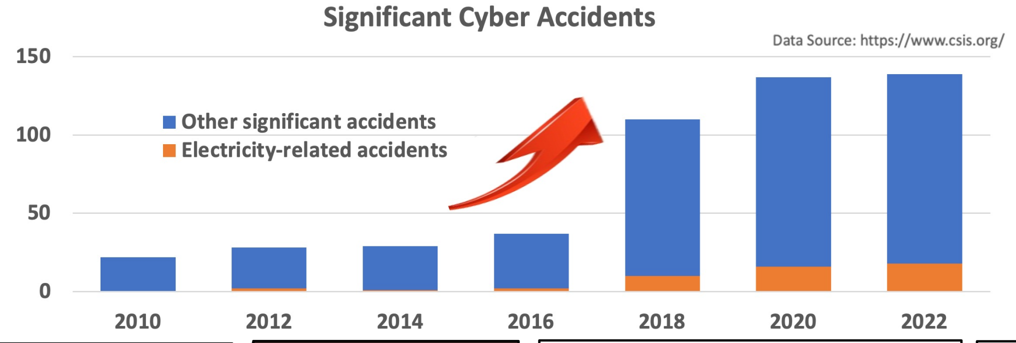
Shamoon3
Target: Italian gas contractor
Impact: Data wiping, file disruption

sPower
Target: Utah elecrical utilities
Impact: Operation interruption

Electromagnetic Attack
Target: Venezuelan power grid
Impact: Outage of the entire country

2020

Solarwinds
Target:US Dep. of Energy, FireEye, …
Impact: Data leakage, Unauthorized network access


Significant Cyber Accidents

Data Source: https://www.csis.org/

REvil
Target:US renewable energy company
Impact: Data leakage, *Ransomware*

2021

Vestas
Target: Wind turbine manufacture
Impact: *Ransomware*, Data leakage

BlackCat
Target: Italian energy sector GSE, European gas pipeline Creos
Impact: *Ransomware*, Websites and systems taken down

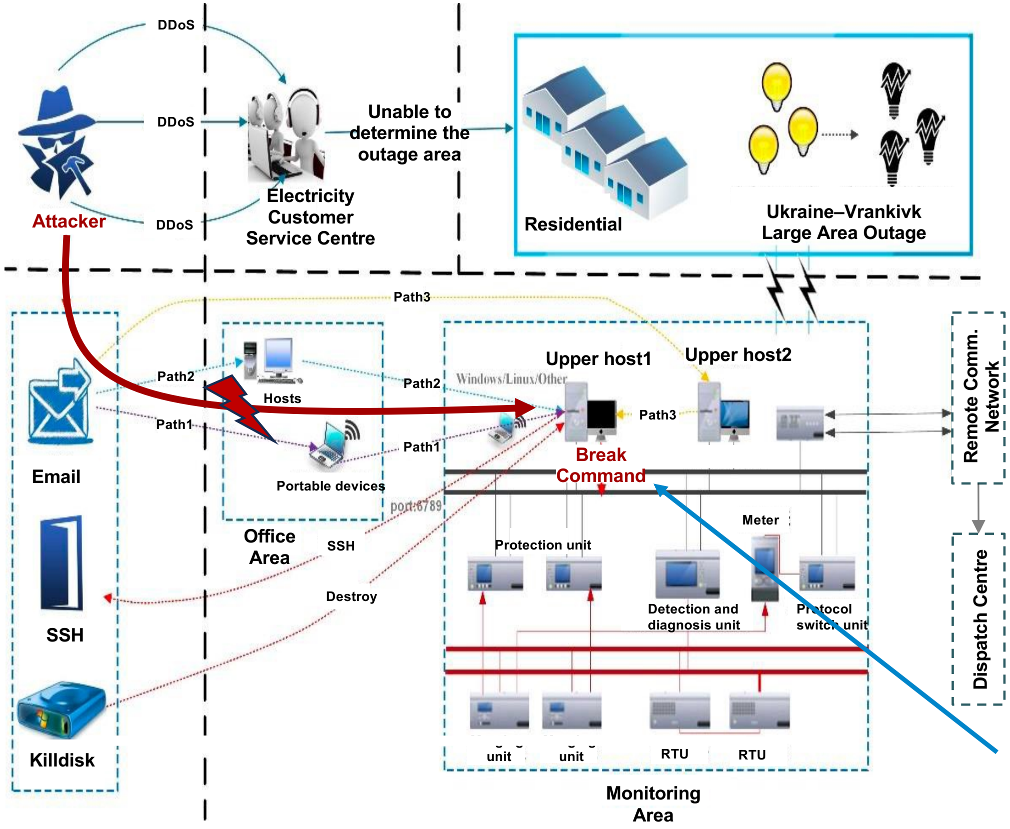
2022

EnerCon
Target: Wind turbine manufacture
Impact: *Disruption* of satellite comm.

Nordex
Target: Wind turbine manufacture
Impact: Shut down IT systems

SaiFlow
Target:EV Charge Station
Impact: Disable EV charge point, Cause service disruption

BlackEnergy Attack in Ukraine Power Grid



Attack Path

- ✓ Phishing emails infecting office hosts
- ✓ Propagation to reach critical upper hosts
- ✓ Issue wrong break commands
- ✓ Overwrite sectors, clear logs and make hosts unable to recover
- ✓ DDoS attack targeting at customer service centre

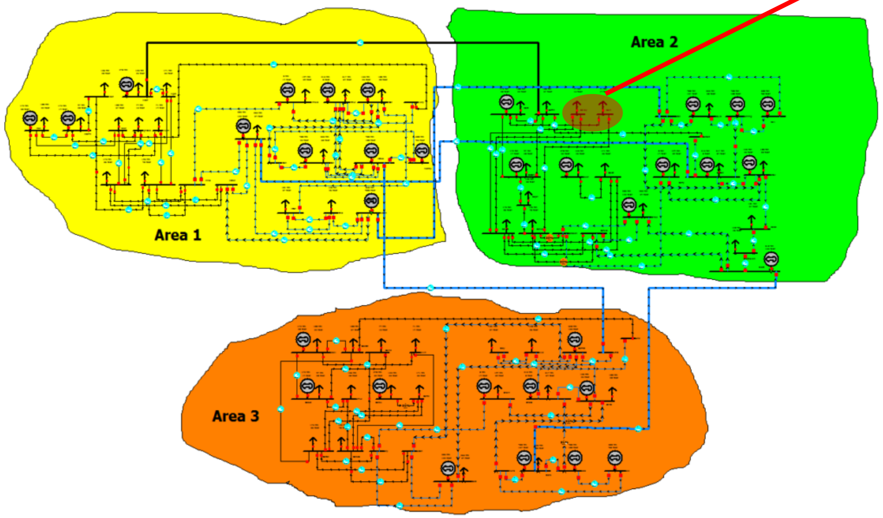
Consequence：

- ✓ 225,000 consumers disconnected for 1-6 hours
- ✓ Constrained operations for months

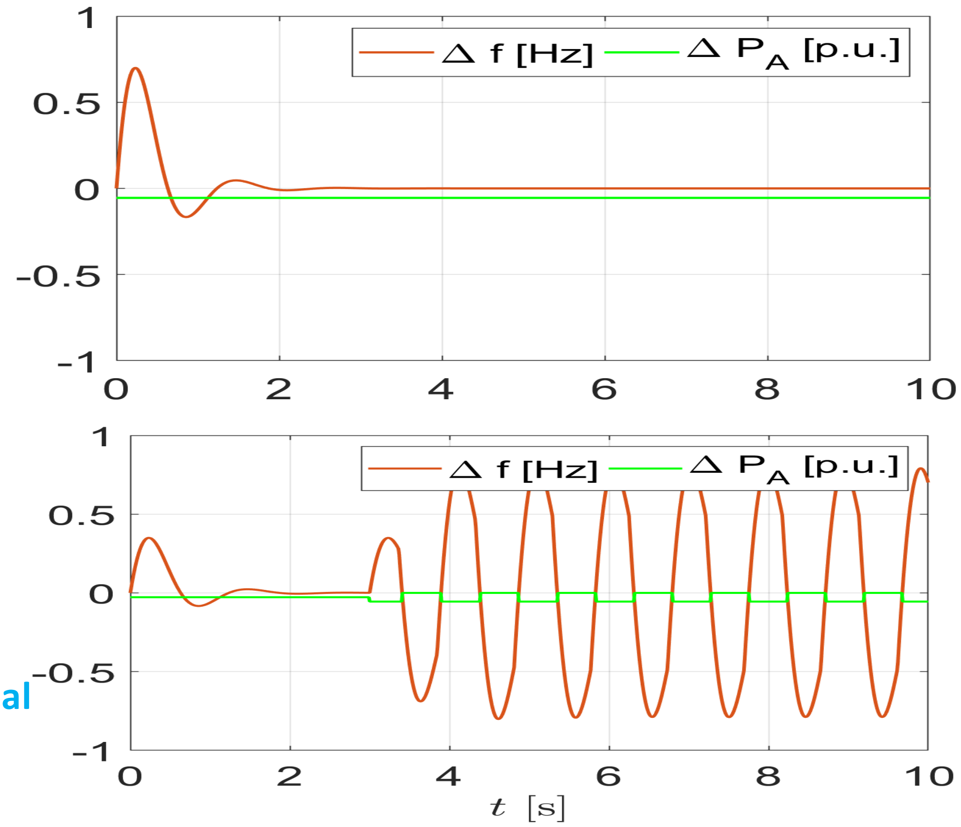
- **Is there anything the defenders can still do at this stage?**
- **Is this the worst damage if the attackers get to this stage (and one of them is a power engineer)?**

Is it possible, by controlling a small part of the system, to cause a system-wide blackout?

- Physics-aware Intelligent Cyberattacks



Manipulated load: 5% in Area 2

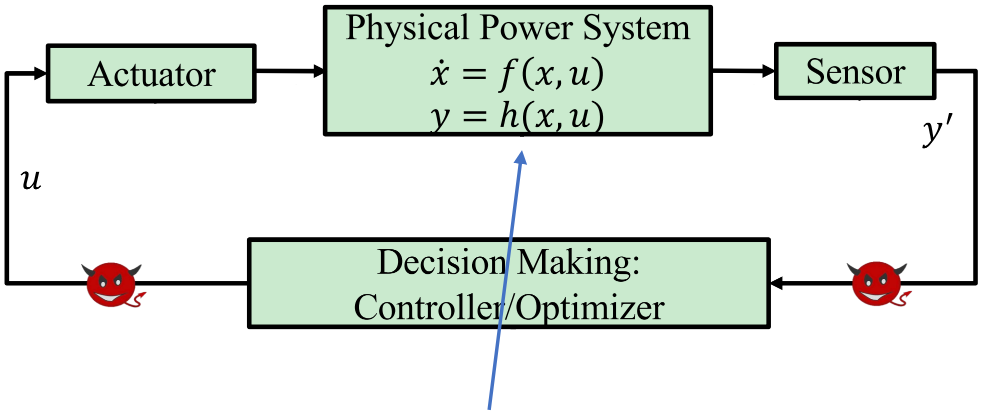


There is a risk of cyber attacks propagating through physical networks!

Chu,and,Teng. Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch, IEEE TSG, 2022

Cyber Resiliency of Digitalised Power Grid

- Control/operational perspective of intelligent cyber attack



Actuator

Physical Power System

$\dot{x} = f(x,u)$

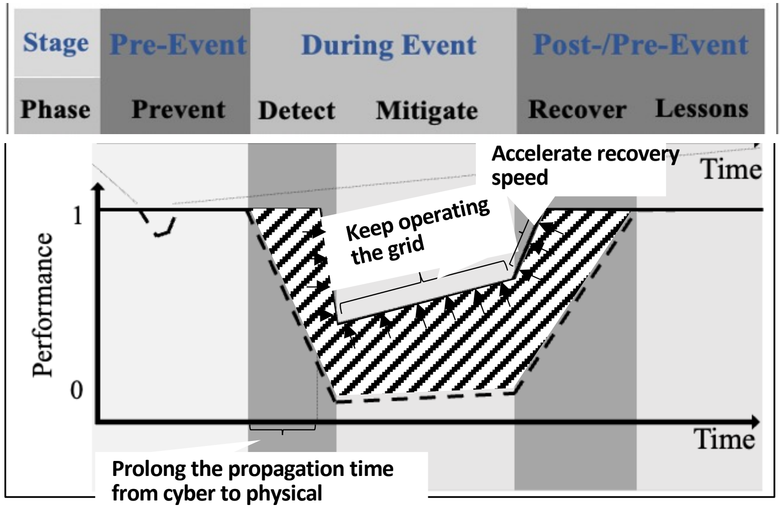
$y = h(x,u)$

Sensor

y'

u

Decision Making: Controller/Optimizer



Stage	Pre-Event	During Event		Post-/Pre-Event	
Phase	Prevent	Detect	Mitigate	Recover	Lessons

Accelerate recovery speed

Keep operating the grid

Prolong the propagation time from cyber to physical

Can we maintain the “minimum” physical functionality of the power grid against intelligent attacks by developing more intelligent decision-making?

Availability (delay and dropout)	Integrity (corruption, forging)	Confidentiality (observation)

Imperial College London

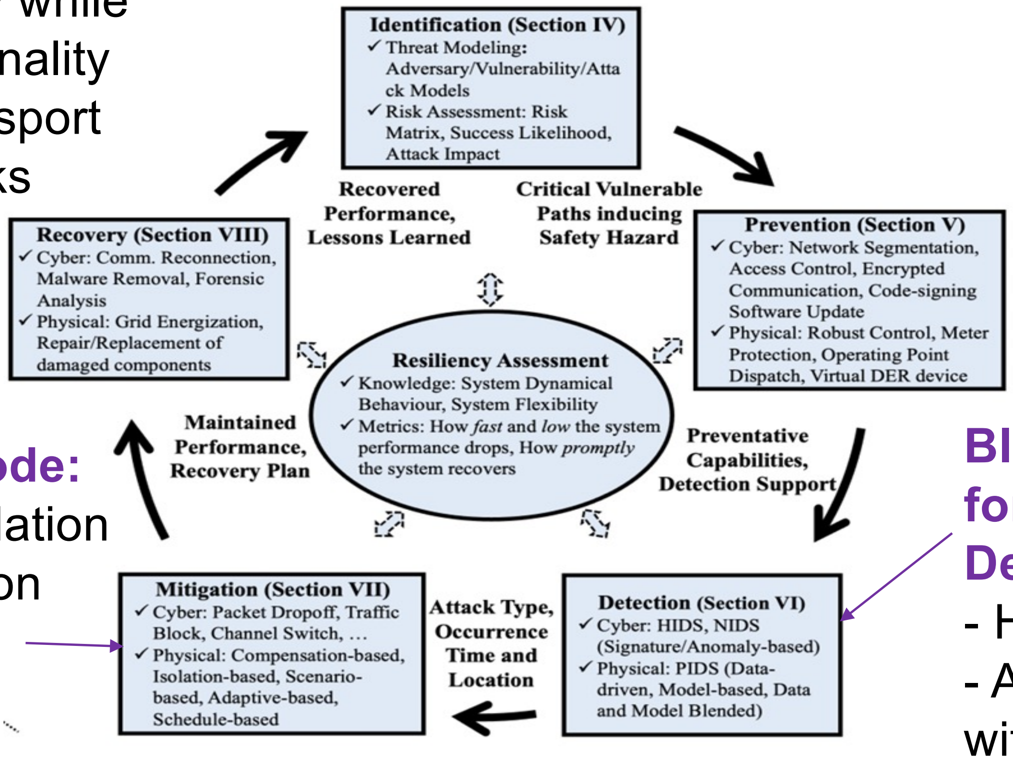
A Defence-in-Depth Strategy for Cyber Resiliency of Energy System

Fast cyber-physical recovery:

- Restore cyber functionality while maintaining physical functionality
- Coordinate electricity, transport and communication networks

"CyberSafe" operation mode:

- Ride through cyber degradation
- Coordinate control/operation flexibility for mode transition
- Adapt according to attack information availability



Identification (Section IV)
✓ Threat Modeling: Adversary/Vulnerability/Attack Models
✓ Risk Assessment: Risk Matrix, Success Likelihood, Attack Impact

Critical Vulnerable Paths inducing Safety Hazard

Prevention (Section V)
✓ Cyber: Network Segmentation, Access Control, Encrypted Communication, Code-signing Software Update
✓ Physical: Robust Control, Meter Protection, Operating Point Dispatch, Virtual DER device

Preventative Capabilities, Detection Support

Detection (Section VI)
✓ Cyber: HIDS, NIDS (Signature/Anomaly-based)
✓ Physical: PIDS (Data-driven, Model-based, Data and Model Blended)

Attack Type, Occurrence Time and Location

Mitigation (Section VII)
✓ Cyber: Packet Dropoff, Traffic Block, Channel Switch, …
✓ Physical: Compensation-based, Isolation-based, Scenario-based, Adaptive-based, Schedule-based

Maintained Performance, Recovery Plan

Recovery (Section VIII)
✓ Cyber: Comm. Reconnection, Malware Removal, Forensic Analysis
✓ Physical: Grid Energization, Repair/Replacement of damaged components

Recovered Performance, Lessons Learned

Resiliency Assessment
✓ Knowledge: System Dynamical Behaviour, System Flexibility
✓ Metrics: How *fast* and *low* the system performance drops, How *promptly* the system recovers

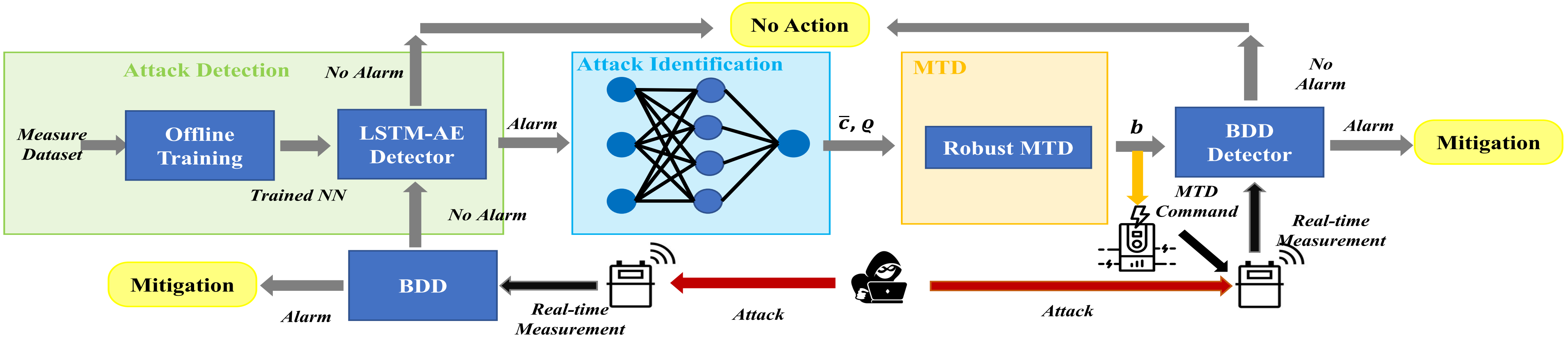
Blending Data and Physics for Proactive Cyber Attack Detection:

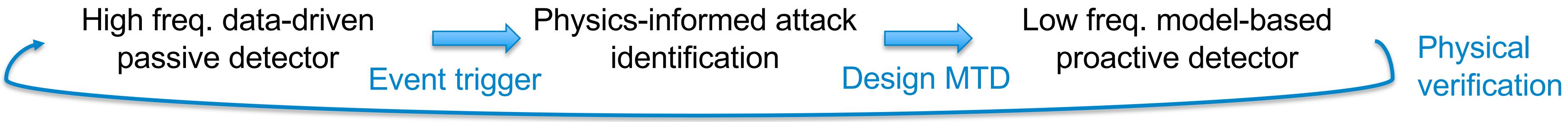
- Hunt the attackers
- Achieve high detection without false alarms
- Inform mitigation strategies

Liu, Teng, et la, Enhancing Cyber-Resiliency of DER-based Smart Grid: A Survey, TSG

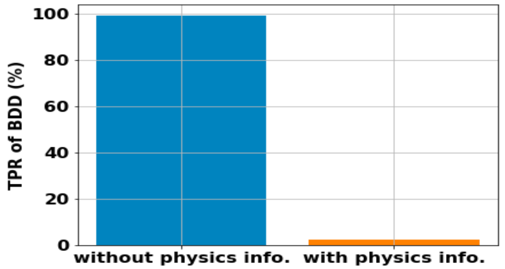
Imperial College London

Cyber Resiliency – Attack Detection: Blending Data and Physics

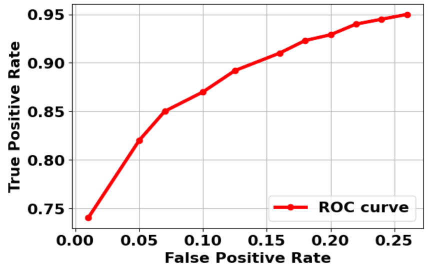



High freq. data-driven passive detector
Event trigger
Physics-informed attack identification
Design MTD
Low freq. model-based proactive detector
Physical verification

TPR of BDD



ROC of data-driven detector



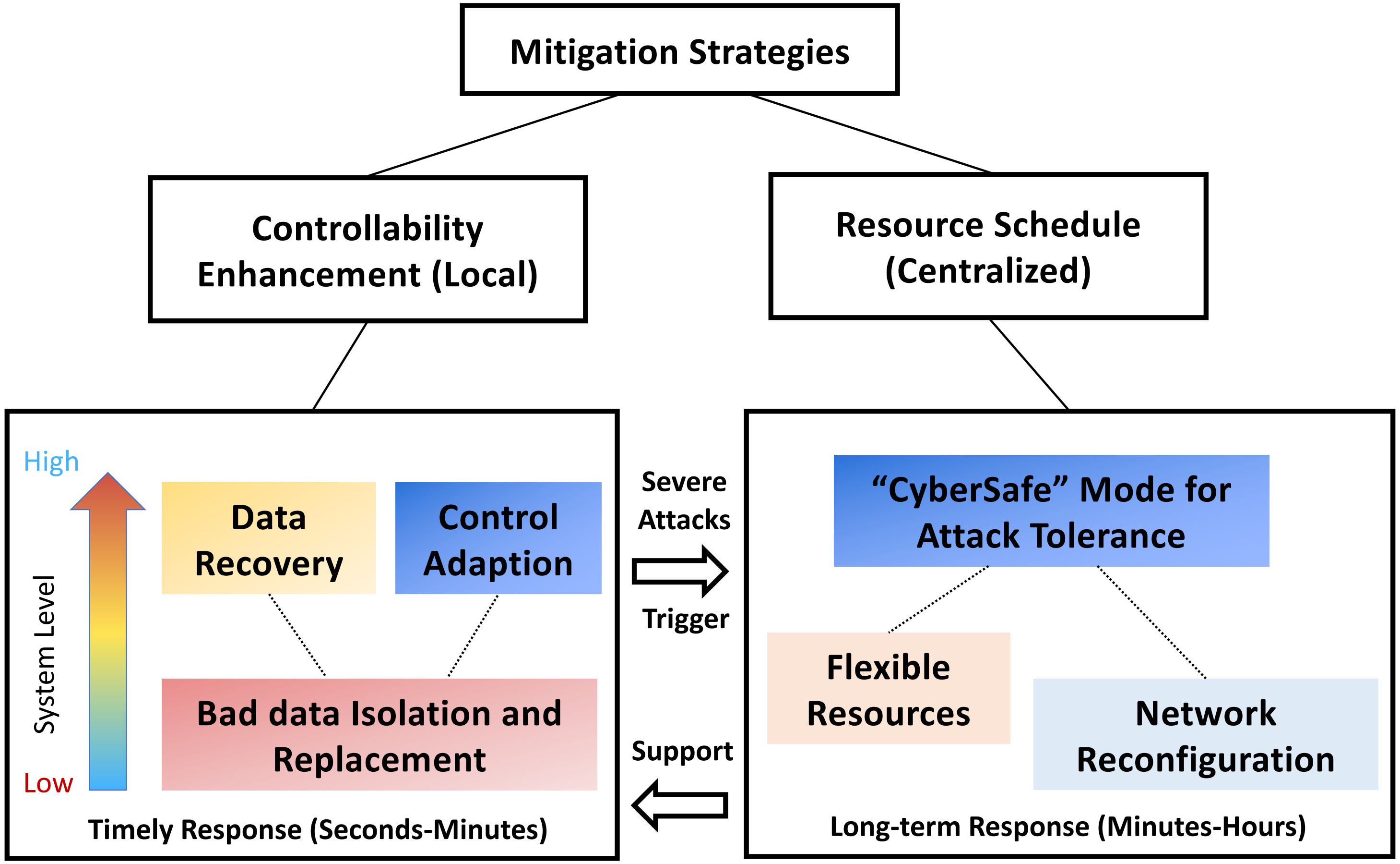
FPR of data-driven detector

No MTD	12.84%
With MTD	**1.83%**

Xu, Higgins,Teng Blending Data and Physics Against False Data Injection Attack: An Event-Triggered Moving Target Defence Approach, IEEE TSG, 2023

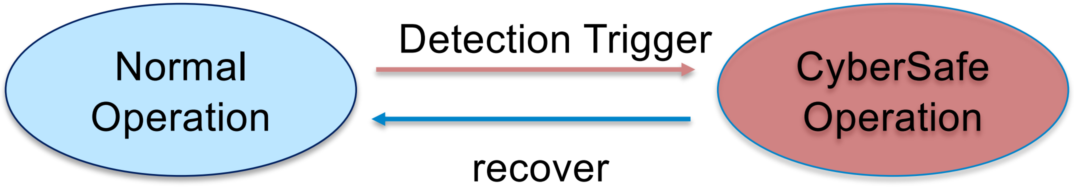
Imperial College London

Cyber Resiliency – Attack Mitigation: How to keep the light on under a major cyber intrusion?

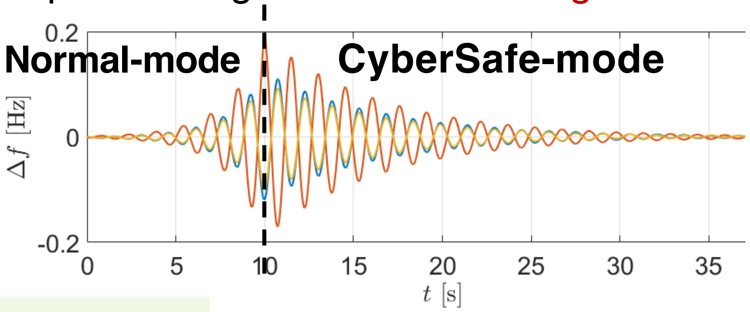

Mitigation Strategies
Controllability Enhancement (Local)
Resource Schedule (Centralized)
High
System Level
Low
Data Recovery
Control Adaption
Bad data Isolation and Replacement
Timely Response (Seconds-Minutes)
Severe Attacks
Trigger
Support
"CyberSafe" Mode for Attack Tolerance
Flexible Resources
Network Reconfiguration
Long-term Response (Minutes-Hours)

Ge, Teng. Cyber-Resilient Self-Triggered Distributed Control of Networked Microgrids Against Multi-Layer DoS Attacks. IEEE TSG, 2022.
Chu, Teng Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch, IEEE TSG, 2023

Cyber Resiliency - Attack Mitigation: A "CyberSafe" Operational Mode

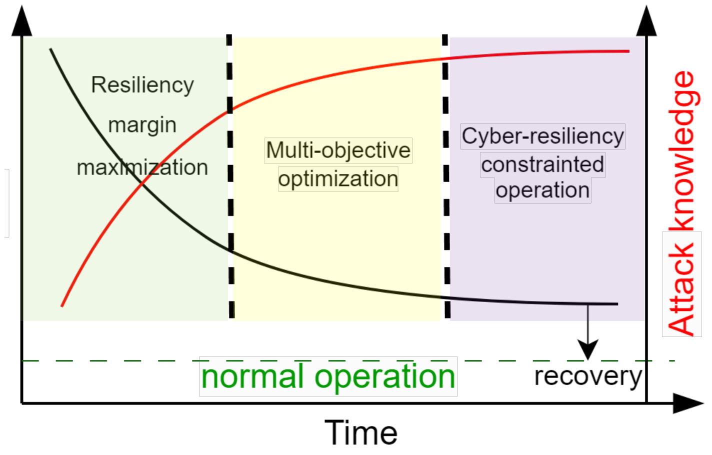


CyberSafe operation against Load Altering Attacks



$\min\limits_{x}$ Operation cost, $C(x)$

s.t. Power balance constraints;
Physical Security constraints ("N-1");
…


Resiliency margin maximization
Multi-objective optimization
Cyber-resiliency constrainted operation
Attack knowledge
normal operation
recovery
Time

$\max\limits_{x}$ Cyber-Resiliency Margin, $M(x)$

s.t. Critical power balance constraints;
~~Physical Security constraints ("N-1");~~
…

$\max\limits_{x}$ $\alpha \cdot M(x) - \beta \cdot C(x)$

s.t. Critical power balance constraints;
~~Physical Security constraints ("N-1");~~
…

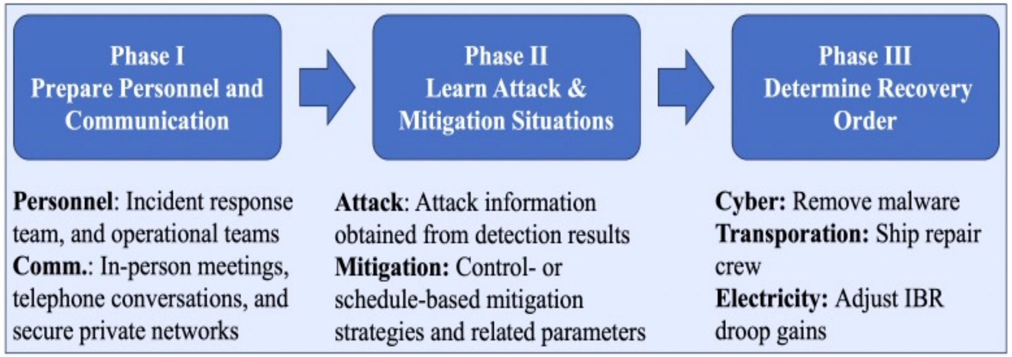
$\min\limits_{x}$ Operation cost, $C(x)$

s.t. Critical power balance constraints;
Resiliency constraint, $M(x) \geq M_0$
~~Physical Security constraints ("N-1");~~
…

Chu and Teng. "Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch." IEEE Trans. Smart Grid, 2022

Cyber Resiliency – Cyber Recovery: Linking Electricity, Transportation, and Communication

➢ General process of cyber recovery

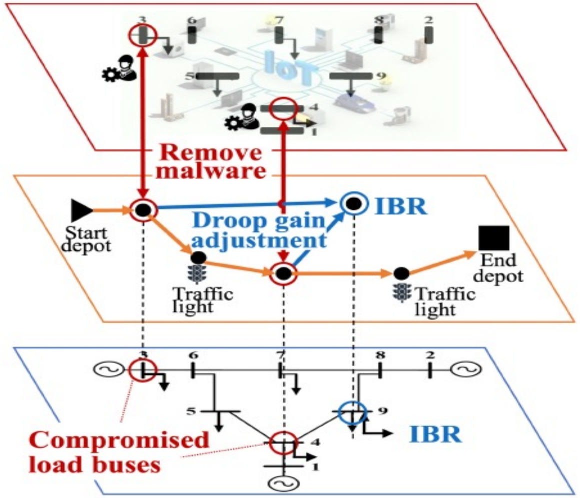


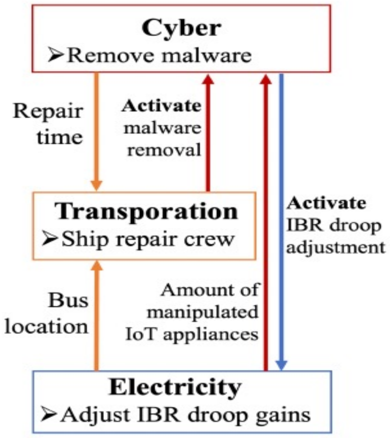
Phase I Prepare Personnel and Communication → Phase II Learn Attack & Mitigation Situations → Phase III Determine Recovery Order

Personnel: Incident response team, and operational teams
Comm.: In-person meetings, telephone conversations, and secure private networks

Attack: Attack information obtained from detection results
Mitigation: Control- or schedule-based mitigation strategies and related parameters

Cyber: Remove malware
Transporation: Ship repair crew
Electricity: Adjust IBR droop gains





Cyber
➢Remove malware

Repair time

Activate malware removal

Transporation
➢Ship repair crew

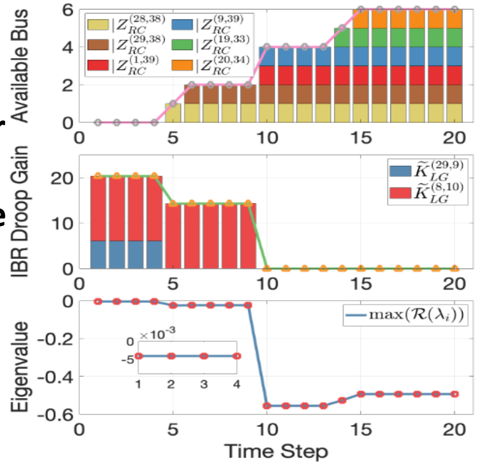
Activate IBR droop adjustment

Bus location

Amount of manipulated IoT appliances

Electricity
➢Adjust IBR droop gains

Not consider couplings among three networks



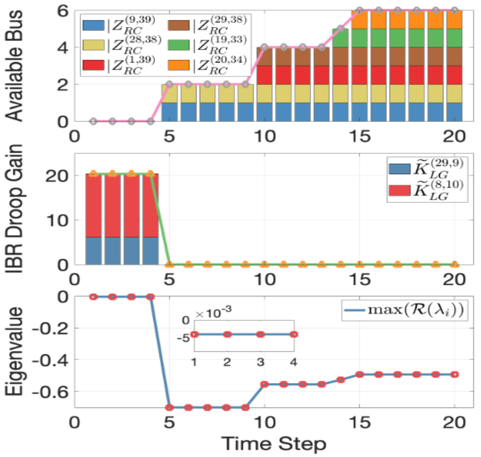
⇨ Attacked buses are repaired at time step 15

⇨ Mitigation-related parameters are reset at time step 10

⇨ Stability can be guaranteed within the recovery process

Consider couplings among three networks

Faster recovery!



⇨ Attacked buses are repaired at time step 15

⇨ Mitigation-related parameters are reset at time step 5

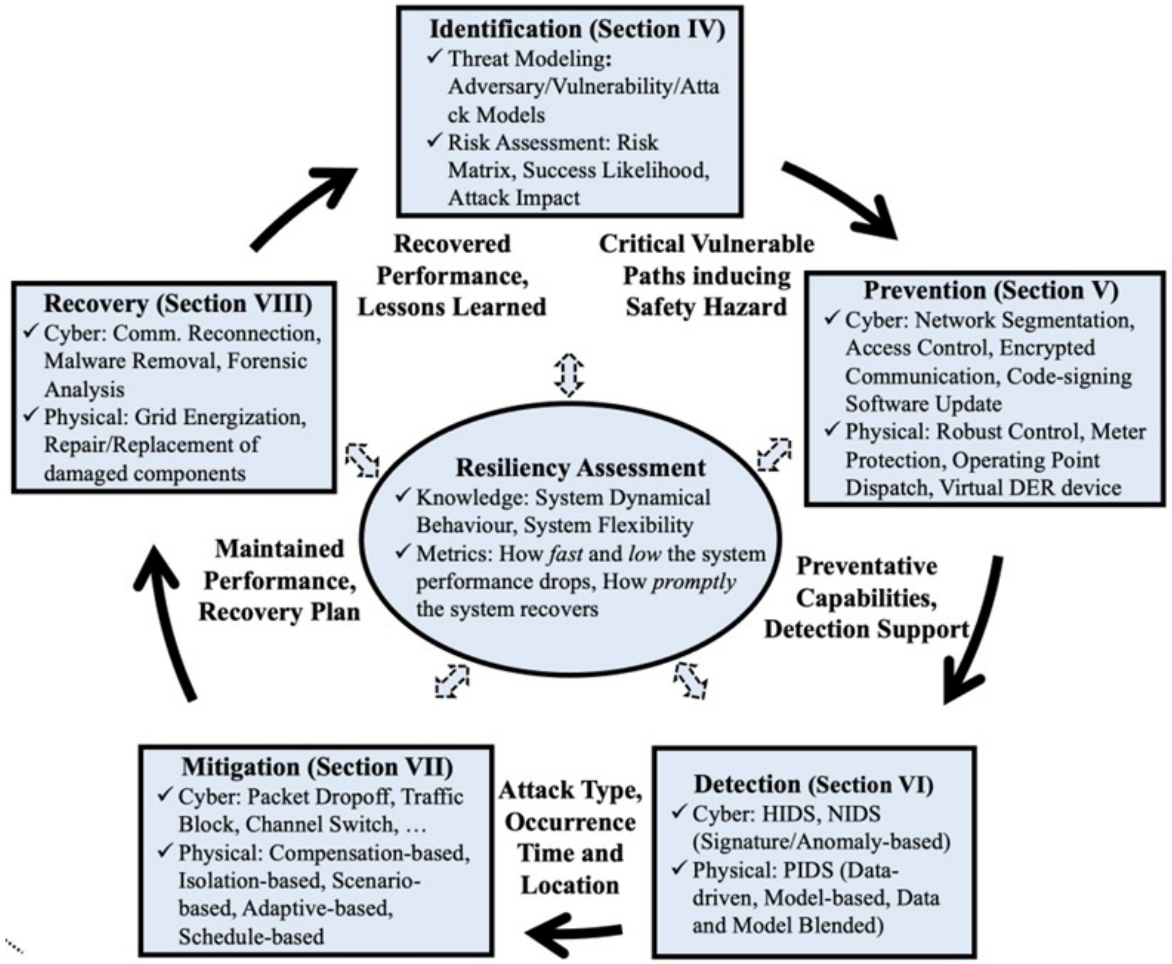
⇨ Stability can be guaranteed within the recovery process

Liu, Chu, Teng, Cyber Recovery from Dynamic Load Altering Attacks: Linking Electricity, Transportation, and Cyber Networks, TIFS, under review

Imperial College London

Conclusion

We need to go beyond the cyber security mindset to develop a holistic and end-to-end cyber resiliency framework for the future power grid!



Identification (Section IV)
- ✓ Threat Modeling: Adversary/Vulnerability/Attack Models
- ✓ Risk Assessment: Risk Matrix, Success Likelihood, Attack Impact

Critical Vulnerable Paths inducing Safety Hazard

Prevention (Section V)
- ✓ Cyber: Network Segmentation, Access Control, Encrypted Communication, Code-signing Software Update
- ✓ Physical: Robust Control, Meter Protection, Operating Point Dispatch, Virtual DER device

Preventative Capabilities, Detection Support

Detection (Section VI)
- ✓ Cyber: HIDS, NIDS (Signature/Anomaly-based)
- ✓ Physical: PIDS (Data-driven, Model-based, Data and Model Blended)

Attack Type, Occurrence Time and Location

Mitigation (Section VII)
- ✓ Cyber: Packet Dropoff, Traffic Block, Channel Switch, …
- ✓ Physical: Compensation-based, Isolation-based, Scenario-based, Adaptive-based, Schedule-based

Maintained Performance, Recovery Plan

Recovery (Section VIII)
- ✓ Cyber: Comm. Reconnection, Malware Removal, Forensic Analysis
- ✓ Physical: Grid Energization, Repair/Replacement of damaged components

Recovered Performance, Lessons Learned

Resiliency Assessment
- ✓ Knowledge: System Dynamical Behaviour, System Flexibility
- ✓ Metrics: How *fast* and *low* the system performance drops, How *promptly* the system recovers

Liu, Teng, et la, Enhancing Cyber-Resiliency of DER-based Smart Grid: A Survey, TSG,

Imperial College London

Acknowledgement

- "Cyber-Resilience Enhancing Detection and mITigation for Networked MicroGrids (CREDIT-NMG)", 2024-2026, EPSRC
- "Blockchain-enabled Cloud-Edge Coordination for Demand Side Management", 2022-2023, EPSRC
- "The Royal-Imperial Black Box: A low cost and novel approach for enhanced power system cyber-security featuring moving target defence", 2021-2022, Innovate UK
- "ICT-enabled Platform for Development and Verification on Distributed Resilient Control of Cyber-Physical Power Systems", 2021-2022, The Royal Society
- "Cyber-physical System Modelling for Cyber-security Analysis in Electricity Systems", 2017-2022, NERC

UKRI Engineering and Physical Sciences Research Council

UKRI Innovate UK

THE ROYAL SOCIETY

UKRI Natural Environment Research Council

List of Reference

- **MX. Liu**[S], **F. Teng***, ZY. Zhang, **PD Ge**[S], RL. Deng, MY. Sun, P. Cheng and JM. Chen “Enhancing Cyber-Resiliency of DER-based Smart Grid: A Survey” *IEEE Trans. Smart Grid,* 2024
- **JZ Hou** [v], **F. Teng**, WQ Yin, Y Song, and YH Hou “Preventive-Corrective Cyber-Defense: Attack-Induced Region Minimization and Cybersecurity Margin Maximization”, *IEEE Trans. Power System*, 2023
- **WK. XU** [S]**, M. Higgins** [S], JH Wang, I. Jaimoukha and **F. Teng***, “Blending Data and Physics Against False Data Injection Attack: An Event-Triggered Moving Target Defence Approach”, *IEEE Trans. Smart Grid*, 2022
- **PD. Ge** [S], BL. Chen and **F. Teng*** “Resilient Distributed Self-Triggered Control of Networked Microgrids Against Hybrid DoS Attacks”, *IEEE Trans. Smart Grid*, 2022
- **ZD Chu** [S], S. Lakshminarayana, B. Chaudhuri, and **F. Teng***. "Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch." *IEEE Trans. Smart Grid,* 2022
- **M. Higgins** [S]**, WK. Xu** [S], **F. Teng*** and T. Parisini “Cyber-Physical Risk Assessment for False Data Injection Attacks Considering Moving Target Defences”, *International Journal of Information Security,* 2022
- **WK. Xu** [S], I. Jaimoukha and **F. Teng***, “Robust Moving Target Defence Against False Data Injection Attacks in Power Grids”, *IEEE Trans. on Inf Foren & Secy,* 2022
- **PD. Ge S, F. Teng***, C Konstantinou and S. Hu “A Resilience-Oriented Centralised-to-Decentralised Framework for Networked Microgrids Management”, *Applied Energy*, 2021
- **M. Higgins** [S], Keith Mayes and **F. Teng*** “Enhanced Cyber-Physical Security Using Attack-resistant Cyber Nodes and Event-triggered Moving Target Defence”, *IET Cyber-Physical Systems: Theory & Applications*,
- **M. Higgins** [S], **F. Teng*** and T. Parisini “Stealthy MTD Against Unsupervised Learning-based Blind FDI Attacks in Power Systems”, *IEEE Trans. on Inf Foren & Secy*, 2020

Imperial College London

Cyber Resiliency of Digitalised Power Grids: can we keep the (most) lights on during major cyber intrusions?

Dr Fei Teng, f.teng@imperial.ac.uk

Imperial College London

A summary of research work from Dr Martin Higgins, Dr Wangkun Xu, Dr Pudong Ge, Dr Zhongda Chu and Dr Mengxiang Liu