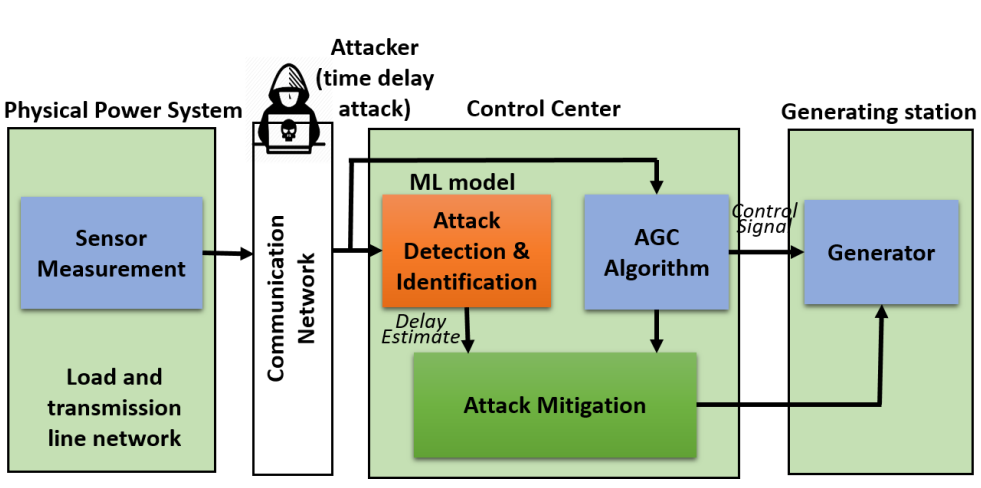
ACRES: AI-ENABLED CYBER RESILIENCE FOR POWER SYSTEMS

PROJECT SUMMARY

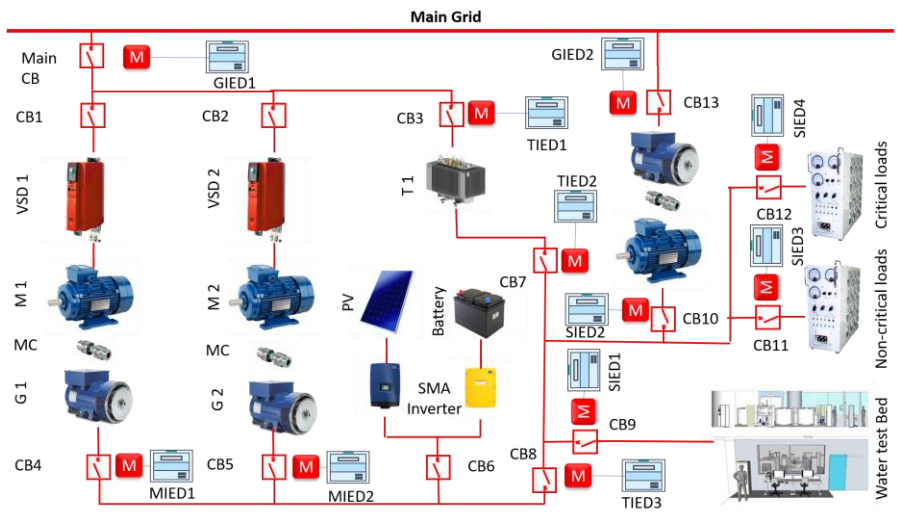
ACRES aims to secure the convergence between Operational Technology (OT) and Information Technology (IT) for next-generation power systems as mission-critical ICS. This convergence has important business benefits such as asset management but introduces a critical attack surface for cyber-space malwares/intrusions to compromise the physical system's trustworthiness.

To mitigate the constraints from the convergence, we aim to achieve:

- Robust and resilient machine learning for real-time attack detection and identification;
- Fast and accurate mitigation of an identified ongoing intrusion, to provide integrity and availability as two salient security properties; and
- In-depth defense based on system semantics to provide resilience beyond traditional perimeter or air-gapped protection.



The ML based attack detection and identification algorithm and mitigation module are embedded in power system to counter the impact of time delay attack launched in communication channels



EPIC testbed at SUTD to implement and test the developed algorithms

PROJECT OUTCOMES

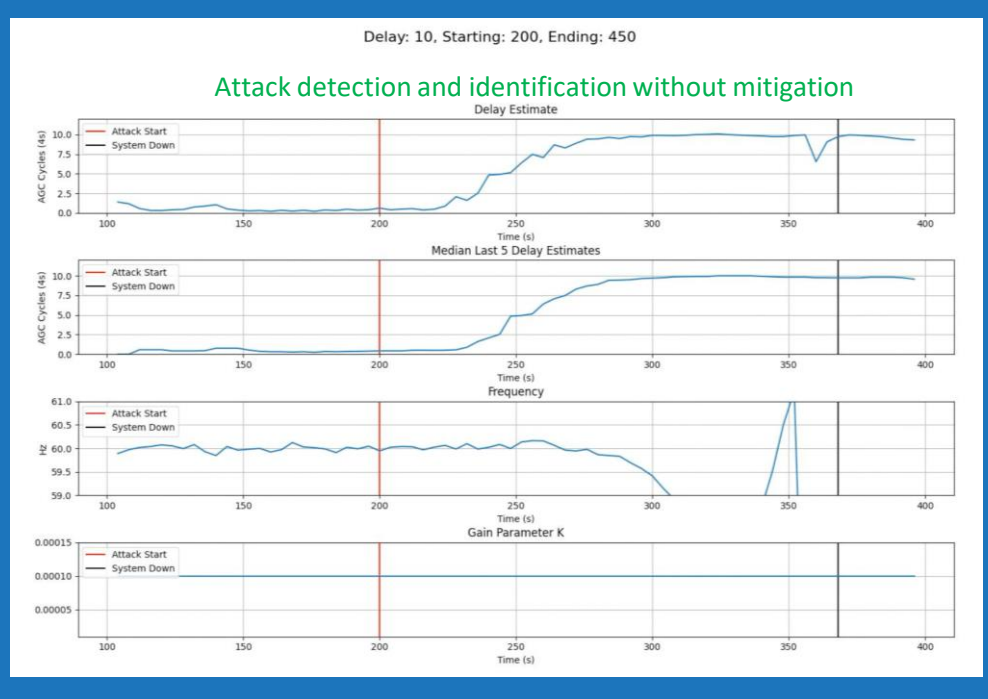
Key Developments include:

1. Actionable model of power system performance under ICT attacks.

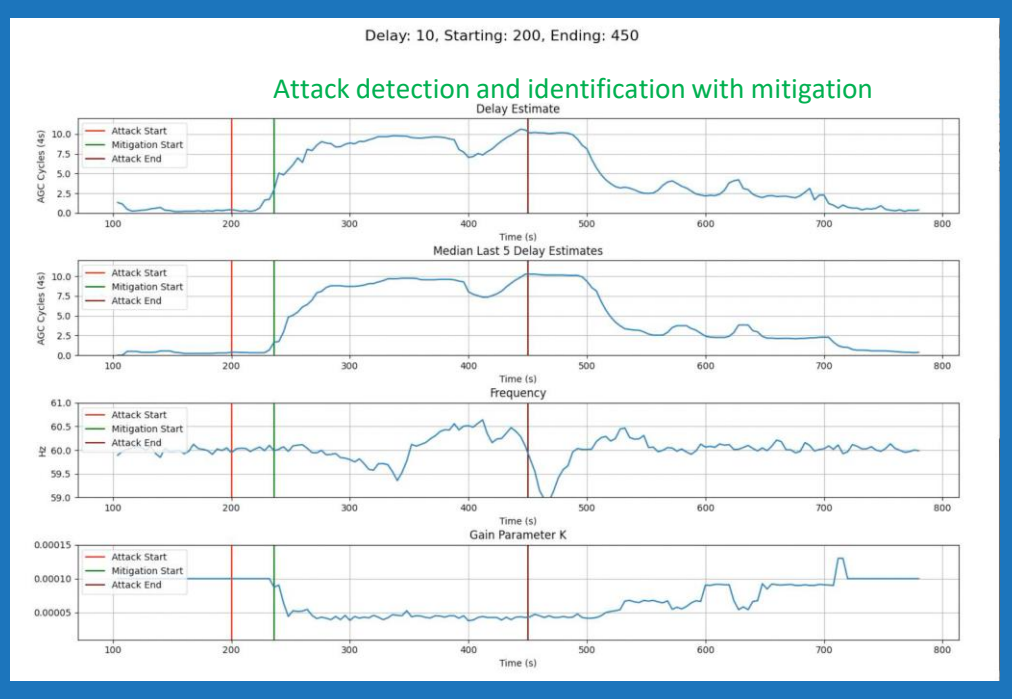
2. Machine Learning (ML) methods developed for practical attack detection/identification:
   - Recurrent ML that can deal with significant temporal correlations in time-series data. In comparison to Gated Recurrent Units (GRUs), the attack identification using developed the recurrent ML model can be improved by 1.4%.
   - Generative and unsupervised ML to overcome insufficient volume and diversity of data, particularly lack of comprehensive attack data labels.
   - Statistical analysis to improve detection of borderline attack samples resulting in (i) less reliance on hard-to-optimise detection thresholds; and (ii) reduction of false positives as a common weakness of unsupervised ML. In comparison to the standard Autoencoder (AE) method, attack detection using developed unsupervised ML can be improved by 2.6%.

3. ML-guided robust mitigation for timing attacks against power system automatic generation control:
   - Agile and informed adaptation of gain parameter in the control loop.
   - Keep stability of frequency profile within critical safety limits, despite an ongoing attack.

4. Team demonstrated an integrated attack detection-identification-mitigation for a 37-bus system using PowerWorld, an industry-strength power system simulator (see images below). The developed mitigation strategy has an efficiency of 84.18 % for saving the system from failure due to time delay attack.



Without any mitigation, a time delay attack can destabilize system frequency.



With mitigation, we use our median delay estimate to determine an optimal gain parameter, K, used in AGC control. Modifying the gain allows the system to survive a time delay attack and return to normal shortly after the attack ends.

PRINCIPAL INVESTIGATOR
David Yau
Professor, SUTD

PARTNERS
ST Electronics (InfoSec) Pte Ltd
University of Illinois at Urbana–Champaign