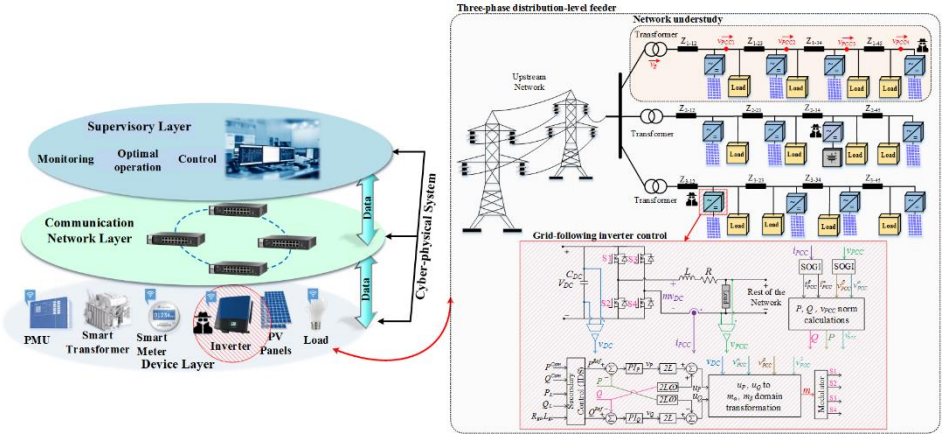
Project Title: Enabling Cybersecurity, Situational Awareness and Resilience in Distribution Grids through Smart Devices and Deep-learning

Lead PI: Haitham Abu-Rub
Lead Institution: Texas A&M University at Qatar
Co-Investigators: Ahmad Alkuwari, Tingwen Huang, Mohammad Shadmand, George Amariucai

Project/Technology Description

- **Objective:** Data-driven multi-level cyberattack detection approach for smart grid with bottom-up and top-down anomaly detection and classification.
- **Key Results:** deep-learning real-time anomaly detection and classification for smart inverters, post-attack cybersecurity mechanism, proactive control strategy.
- **Intellectual property position:** patentable disclosure submitted to QF on post cyberattack synchronization for smart grid.



Technical Approach and Solution:

- **Major Challenges addressed:** real-time detection of anomalies, classification of anomalies versus normal power system and power electronics failures, development of comprehensive deep learning tools responsive to grid reconfiguration
- **Approach/Solution:** development of models for grid clusters, identification problematic grid clusters via hybrid deterministic and probabilistic tools, identification of compromised smart inverters via sanity authentication of control commands and machine learning tools, proactive control approach for during attack and post attack resiliency of the active distribution network.

Key Outcomes

- Preventing stealthy attacks on power electronics dominated grid, a cybersecurity approach at the design stage of distributed generation.
- Real-time AI multi-class classifier that classifies, cyberattacks, power electronics failures and grid transients.
- Data-driven based corrective actions and detection for intrusive sensor behaviors in smart grid.
- Voltage stability assessment for deriving the stability margin of a grid cluster to be employed in intrusion detection systems.
- Post cyberattack synchronization for active distribution networks.
- Workshop and educational modules on cybersecurity and artificial intelligence for power grid.
- Training local engineers on state-of-the-art cybersecurity technologies.

Benefits/Potential Applications/Customers/Markets

- **Benefit:** Improving the cybersecurity and resiliency of smart grid.
- **Application:** The proposed technologies can be applied to smart grid, microgrids, and other cyber-physical energy systems.
- **Potential Customers/Market:** KAHRAMAA and other international utility companies, Siemens, ABB, ENPHASE, GE, etc.

Major Impacts: Improving cybersecurity of Qatar's current and future power grid and critical infrastructure