

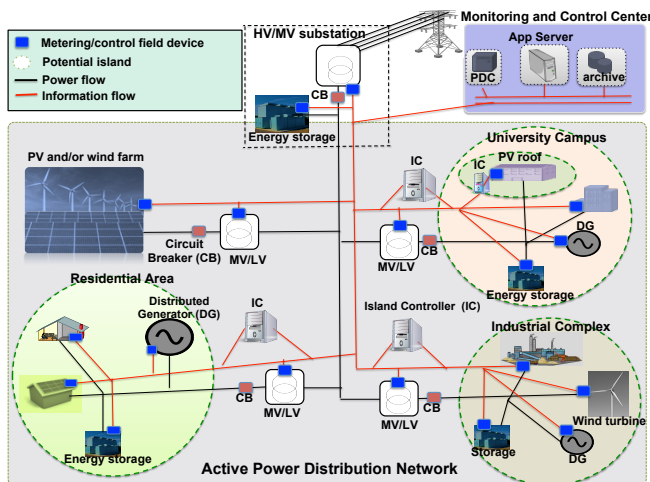
Cyber-Secure Communication Architecture for Active Power Distribution Networks (ADN)

Teklemariam T. Tesfay, Jean-Pierre Hubaux, Jean-Yves Le Boudec, and Philippe Oechslin

Email: {tech.tesfay, jean-pierre.hubaux, jean-yves.leboudec, philippe.oechslin}@epfl.ch



Cyber-physical Infrastructure of an ADN



From Passive to Active Distribution Networks

Conventional power distribution network

- Passive, requires minimal centralized control strategy

Active power distribution network

- Highly distributed and more sophisticated monitoring and control strategy
- A large number of sensing and actuating field devices dispersed over a large geographic area in remote locations
- Pervasive communication infrastructure

Security implications of ADN

- A wide range of options to compromise the network
- Attacks from insiders or outsiders

Attacker's goals

- Compromise the availability, authenticity or freshness of sensor data or control signals

Security Goals of an Active Distribution Network

An attacker should not have more power than a classical sabotage by physical destruction

- Being **smart** should not translate to a **more fragile** system

No unchecked trust on individuals and devices

- Treat all individuals and devices as potentially malicious
 - Authenticate and authorize individuals to access devices and services
 - Authenticate all devices for network access
 - Constantly monitor network and look for suspicious activities

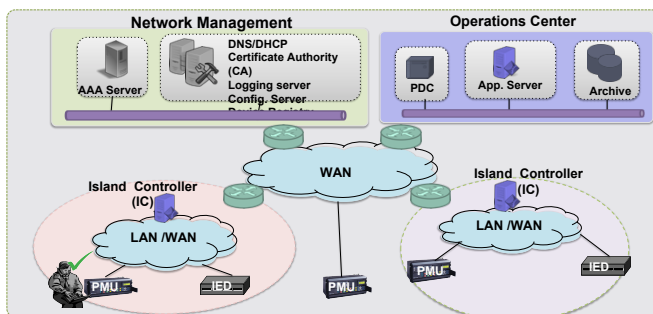
Role Based Access Control and Activity Monitoring

Each user has an individual account managed by a central authentication server

- No per-device account
- Role based access control (RBAC) policy specifies privileges for each account
- Prevents unauthorized access by outsiders

Activity and event monitoring for accountability

- User activity and event logs centrally managed in a logging server
- Postmortem analysis of log data to hold insiders accountable for their activity
- Revoke privileges of suspected insiders



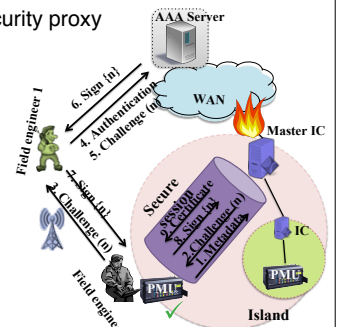
Network Access Control - Keep the bad devices at bay

Two steps to successfully connect a device to the network

- Field technician authenticated by central server
 - Verify device attributes satisfy a set of requirements
- Device issued digital certificate and other parameters after the two steps are accomplished
 - Digital certificate for device authentication and for secure session setup (e.g., (D)TLS)

Secure device installation and configuration during Islanding

- Disturbance in the main grid can cause an ADN to operate in islanded mode
- Island controller (IC) provides local control and protection functions
- Islanding can render the AAA server unreachable
- Malicious insiders or outsiders can exploit such emergency situation
- Authenticate users using challenge-response mechanism
- Use Island controller (IC) as a security proxy



- IC issues temporary certificate to newly installed devices
- Assumes existence of out-of-band communication (e.g. 3G) between AAA server and the island.