ABSTRACT – Remotely operated Smart Grid components such as photovoltaic (PV) and battery inverters, electric vehicle (EV) supply equipment, or wind generators introduce new vulnerabilities that could be exploited by attackers. One such attack scenario has recently been presented in the AIT SmartEST laboratory as described below. Through a man-in-the-middle attack to the 61850 communication, a set of simulated and one real PV inverter are forced into unstable situation and start oscillating. By a follow-up attack, the inverters disconnect due to a maliciously created overvoltage situation. A centralized SCADA intrusion detection system (IDS) and decentralized implemented resilient controllers (RC) – developed in the SPARKS project (https://project-sparks.eu) – are able to successfully counteract the demonstrated attacks.

ATTACK SCENARIO
- Low voltage distribution grid
- Central controller
- Distributed PV systems
- 61850 based Q(U) set-points
- Man-in-the-middle (MITM) attack
- on plain 61850 MMS packets
- sniffing voltage measurements
- modifying Q(U) set-points
- Attacker’s goals
- violation of supply system limits
- destabilisation of supply system

LABORATORY PHIL SET-UP

COUNTERMEASURES
Resilient Controller (RC)
- rule-based local (at PV site) decision making
- estimation of set-points effects by
- Thevenin equivalent & local droop law
- RC Rule 1 „Voltage Prediction“
- assessment of droop law’s gain
- limitation of effective gain k to K

Intrusion Detection System (IDS)
- monitoring traffic in application layer
- Multi-attribute Detection
- white/blacklist, known signatures
- state-full analysis and anomaly detection
- Alerts to Resilient Controller
- additional information for better RC reactions

DEMONSTRATION OF CYBER-ATTACKS AND COUNTERMEASURES

Attacks
- Attacker changes set-points to modify the inverters’ characteristics
- Attack 1: infinite gain Q(U)
- Attack 2: flipped Q(U) curve

Intrusion Detection System

Q(U) characteristics

Measured effects
- Before first attack
  - regular Q(U) characteristic
  - deadband at U_{nom} ±4%
  - Voltage supporting Q(U)
- After first MITM-attack
  - inverters with malicious Q(U) characteristic: infinite gain
  - unstable, oscillating behaviour
  - ΔQ oscillation 0.75 p.u.
  - ΔU oscillation ~2.0 Vpp

- After second MITM-attack
  - inverter with malicious Q(U) characteristic: flipped curve
  - no more Q(U) voltage support
  - further increase of high voltage
  - voltage limit violation
  - autm. inverter disconnection

CONCLUSION
- Centralized (IDS) and decentralized (RC) countermeasures able to protect the attacked system
- Best protection through combined RC+IDS approach and resilient fall-back
- Encryption of remote commands crucial as basic cyber-attack prevention
- Trade-off between configuration freedom and protection of field devices