**M. FASCHANG**[1]// mario.faschang@ait.ac.at // **C. SEITL**[1]// christian.seitl@ait.ac.at // **F. KUPZOG**[1]// friederich.kupzog@ait.ac.at //
**D. UMSONST**[2]// umsonst@kth.se // **B. KANG**[3]// b.kang@qub.ac.uk //
1 AIT Austrian Institute of Technology GmbH, Center for Energy, Electric Energy Systems, Tech Base Vienna, Austria.
2 KTH Royal Institute of Technology, Stockholm, Sweden
3 Queen's University Belfast, Northern Ireland, UK

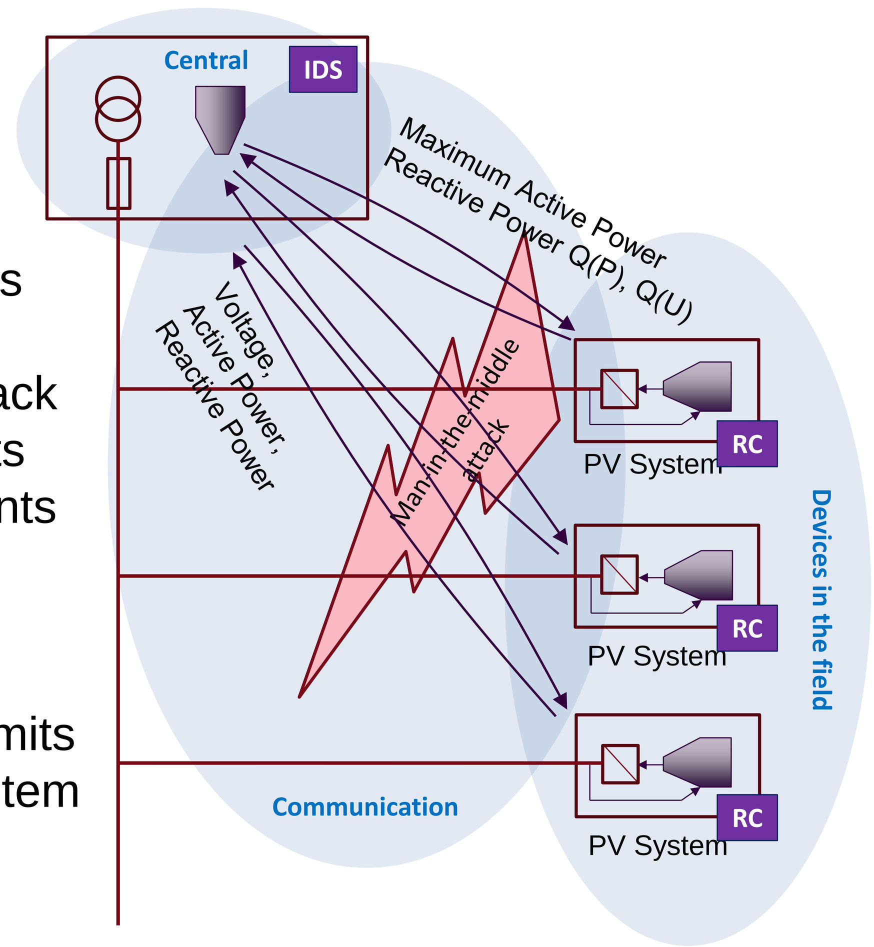
# SPARKS MULTI-STAGE CYBER-ATTACK AND COUNTERMEASURE DEMONSTRATION

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

**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

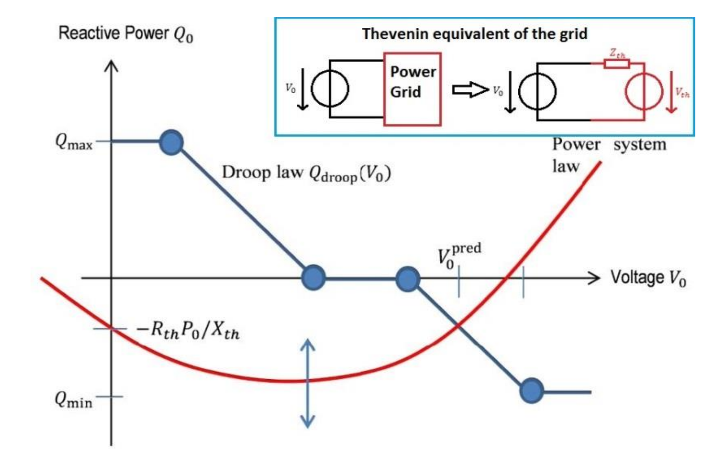
- Low voltage distribution grid
  - central controller
  - distributed PV systems
  - 61850 based Q(U) set-points
- Man-in-the-middle (MITM) attack
  - on plain 61850 MMS packets
  - sniffing voltage measurements
  - modifying Q(U) set-points
- Attacker's goals
  - violation of supply system limits
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




## COUNTERMEASURES

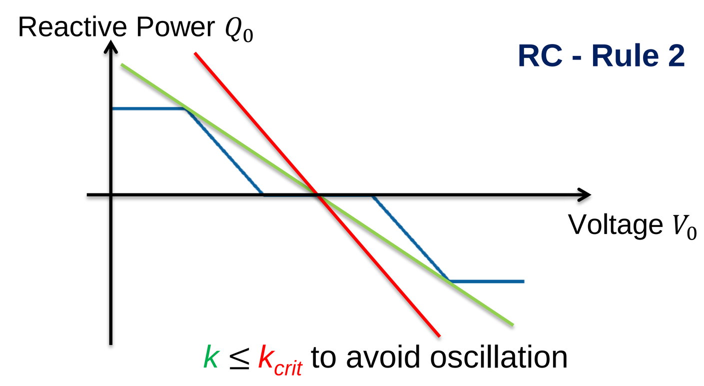
**Resilient Controller (RC)**

- rule-based local (at PV site) decision making
- **RC Rule 1** „Voltage Prediction"
  - estimation of set-points effects by
  - Thevenin equivalent & local droop law
- **RC Rule 2** „Critical Gain"
  - assessment of droop law's gain
  - limitation of effective gain $k$ to $k_{crit}$

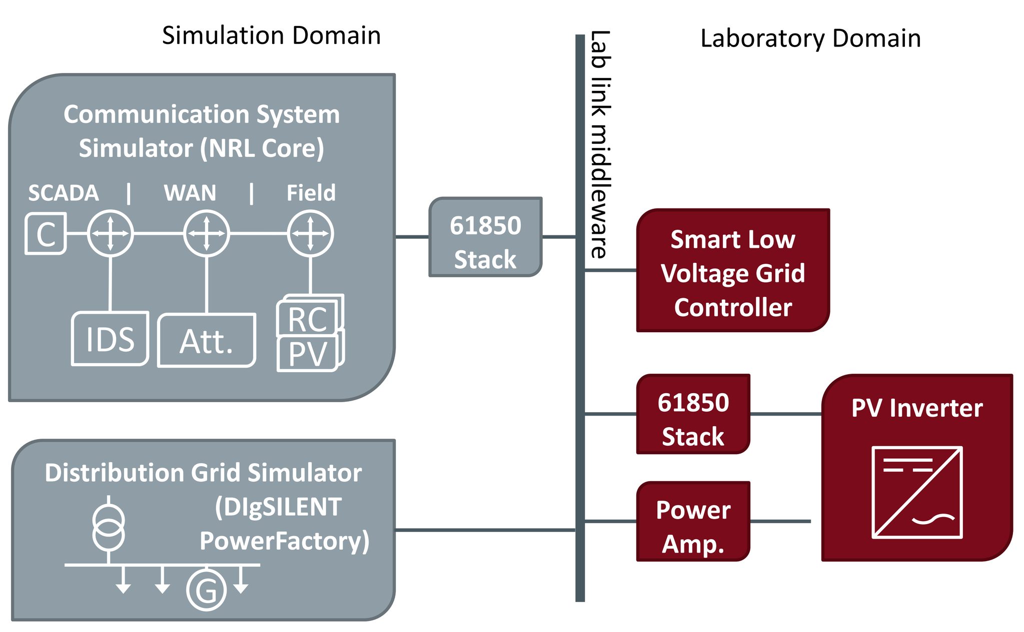



**Intrusion Detection System (IDS)**

- monitoring traffic in application layer
- **Mulìti-attribute Detection**
  - white/balcklist, known signatures
  - state-full analysis and anomaly detection
- **Alerts to Resilient Controller**
  - additional information for better RC reactions




## LABORATORY PHIL SET-UP




SCADA ... Supervisory Control & Data Akquisition
WAN ... Wide Area Network
PV ... Photovoltaic Inverter
IDS ... Intrusion Detection System
RC ... Resilient Controller

**Laboratory set-up**

- Power-hardware-in-the-loop (PHIL) integration of PV inverter in distribution grid simulation
- Man-in-the-middle attacker integration in TCP/IP communication system simulation
- IDS and RC implementation

**Real/physical entities**

- 2.5 kVA single phase PV inverter (SunSpec)
- IEC61850/SunSpec gateway IEC61499-impl.
- Smart Low Voltage Grid controller
- Spitzenberger & Spies power amplifier
- local load and line impedance

**Simulated entities**

- small rural distribution grid (20 households, 13 PV)
- TCP/IP communication grid (SCADA ↔ WAN ↔ Field)

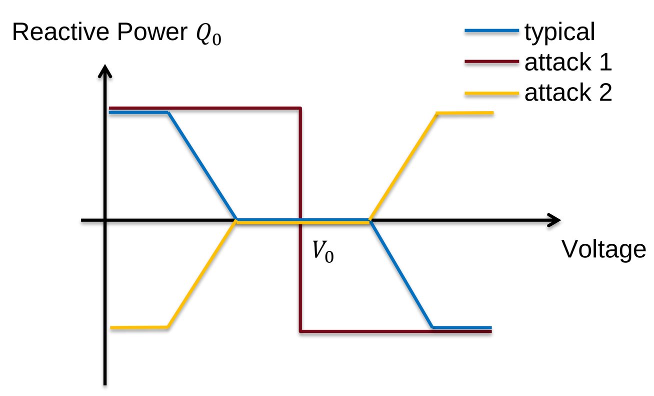
## DEMONSTRATION OF CYBER-ATTACKS AND COUNTERMEASURES

**Attacks**

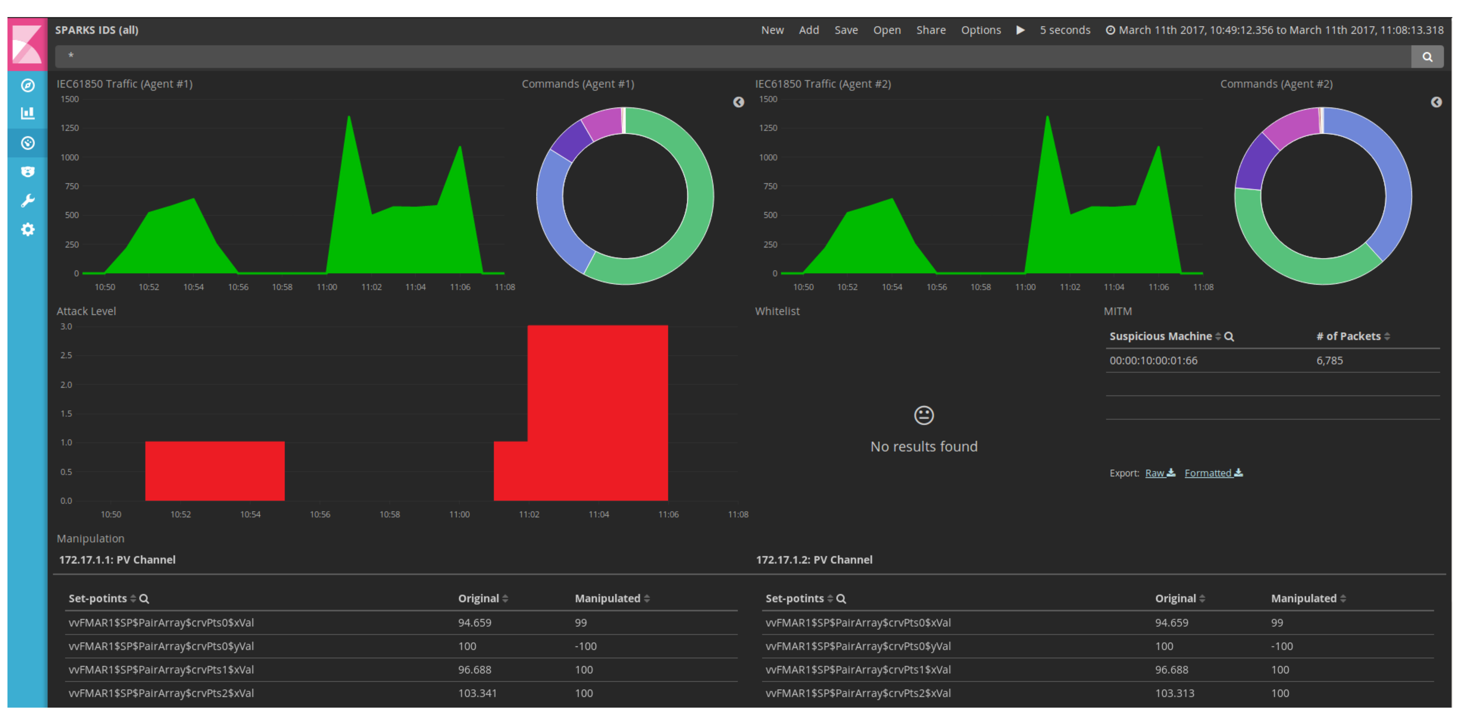
Attacker changes set-points to modify the inverters' characteristics

- Attack 1: infinite gain Q(U)
- Attack 2: flipped Q(U) curve

**Q(U) characteristics**

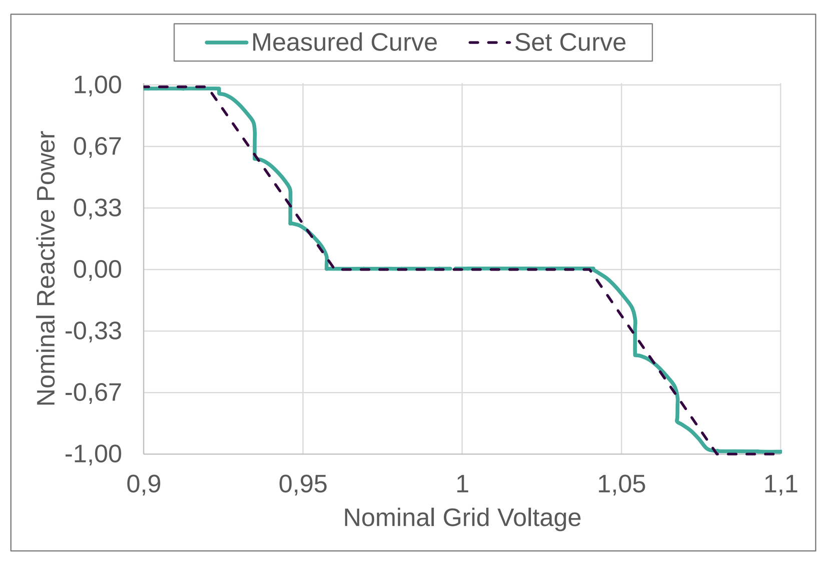



**Intrusion Detection System**

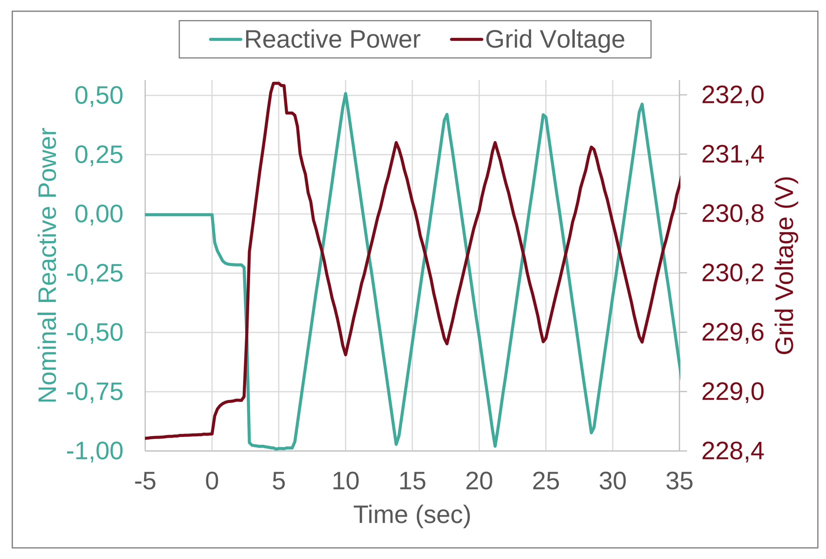


**Measured effects**

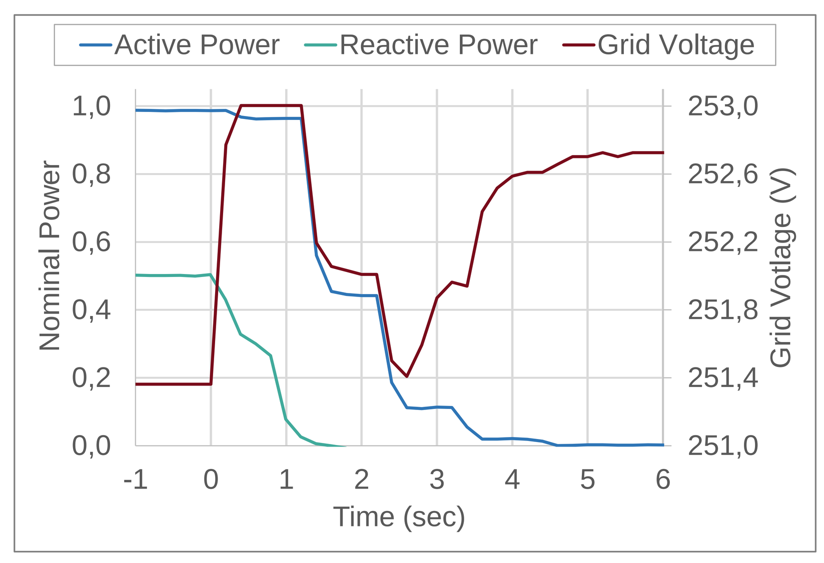
- Before first attack
  - regular Q(U) characteristic
  - deadband at $U_{nom}$ ± 4%
  - Voltage supporting Q(U)




- After first MITM-attack
  - inverters with malicous 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 malicous Q(U) characteristic: **flipped curve**
  - no more Q(U) voltage support
  - further increase of high voltage
  - voltage limit violation
  - autom. 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

EU FP7 Programme
Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS