SMART GRID PROTECTION AGAINST CYBER ATTACKS

Example of a Cyber-Physical Attacks Investigation on IEC 61850/61499 equipped PV Inverters using 4DIAC

BooJoong Kang, Peter Maynard, Kieran McLaughlin, Sakir Sezer
CSIT Centre for Secure Information Technologies, Queen's University Belfast

Filip Andrén, Christian Seitl, Friederich Kupzog, Thomas Strasser
AIT Austrian Institute of Technology, Energy Department, Electric Energy Systems

Presented by BooJoong Kang (CSIT)

6th 4DIAC User's Workshop (4DIAC)

20th IEEE International Conference on
Emerging Technologies and Factory Automation (ETFA'2015)
September 8-11, Luxembourg

IEEE 1951-2011 60th anniversary

EU FP7 Programme Contract No. 608224

Outline

- About FP7 SPARKS
- Recent cyber-attacks
- IEC 61850 smart grid environment
- IEC 61850/61499 PV remote control in 4DIAC
- Cyber-attack scenario
- Conclusions

EU FP7 Programme Contract No. 608224

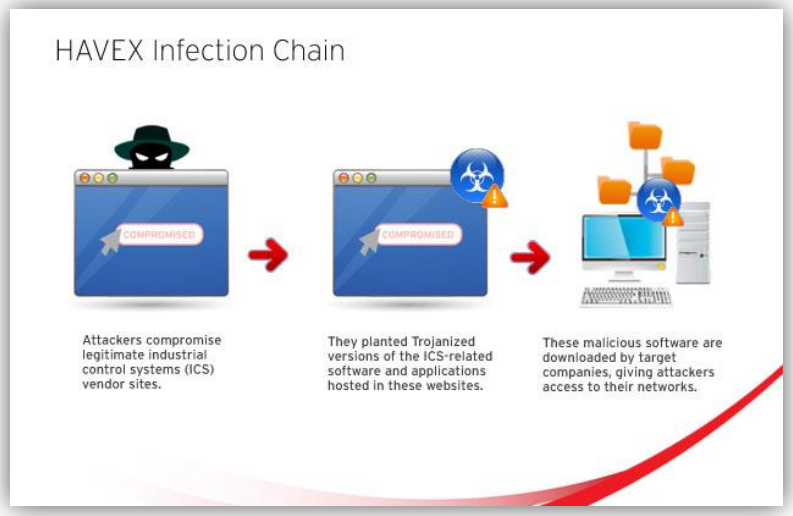
About FP7 SPARKS

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- FP7 project deals with smart grid cyber security
- Objectives
  - Engage stakeholders and perform demonstrations
  - Analyze smart grid security and risk
  - Propose smart grid security standards
  - Develop security measures and procedures
  - Investigate financial, legal and social issues
- Project details
  - Funded by European Union (EU) under FP7, SEC-2013.2.2-3 Protection of smart energy grids against cyber attacks
  - Contract No. 608224,
  - Start Date: 1st April, 2014, duration of 3 years

Recent Cyber-Attacks

- "Black Energy"
  - Malware discovered on internet-connected HMIs
  - Targets HMI products from three vendors: GE, Siemens, BroadWin
- "Havex" Remote Access Trojan (RAT)
  - Targets OPC communications
  - Client/server technology widely used in process control systems



Ref: Trend Micro

Recent Cyber-Attacks

- German steel plant
  - ‘Spear phishing’ emails and social engineering techniques
  - Login credentials obtained
  - Access gained to the plant office network ...

    and then to the production systems
  - Blast furnace could not shut down as normal
  - Caused “massive damage”

→ *Attackers showed technical expertise*

EU FP7 Programme Contract No. 608224

Recent Cyber-Attacks

- Take Away Message

Cyber attack

but ...

Physical impact

EU FP7 Programme Contract No. 608224

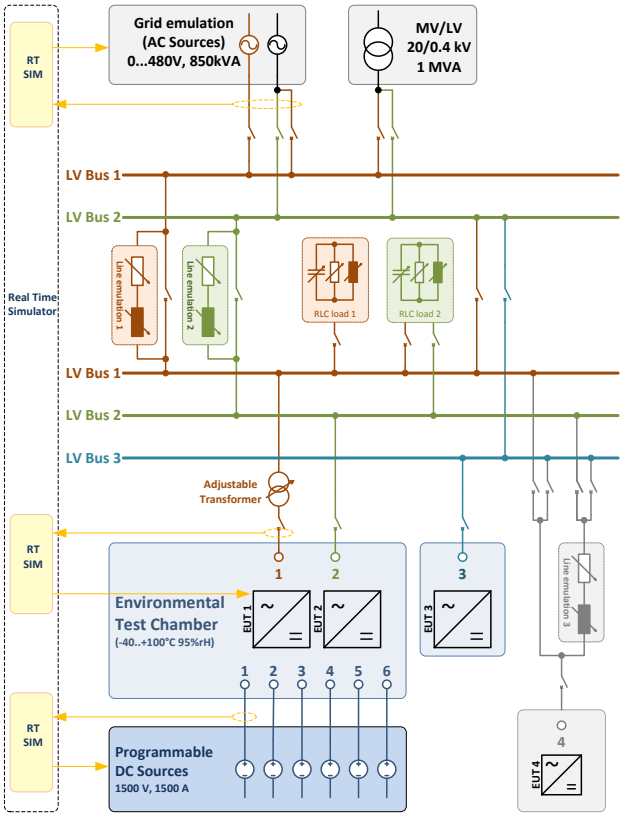
IEC 61850 Smart Grid Environment

- AIT SmartEST laboratory
  - Test laboratory for distributed energy resources (DER) in SPARKS
  - Specialized in inverter tests and system tests with multiple components and environmental testing capabilities

EU FP7 Programme Contract No. 608224

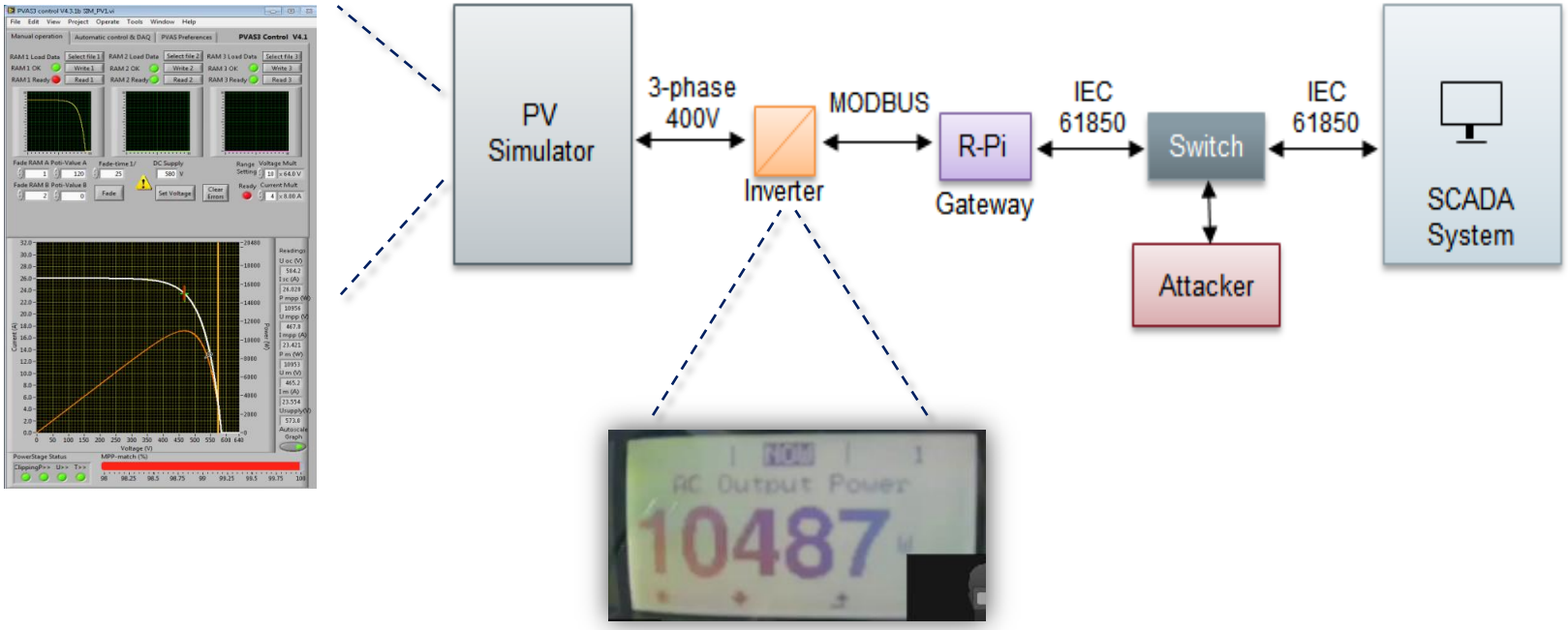
IEC 61850 Smart Grid Environment

- Electrical layout
  - Low voltage (LV) (400 V) laboratory
  - Supplied by local 20 kV medium voltage grid
  - Testing single DER components (e.g. PV inverters up to the 800 kW)
- DC sources (PV array simulation)
  - Independent dynamic PV-Array simulators (5x 1500 V, 1500 A, 960 kW)
- SCADA and automation system
  - Highly customizable laboratory automation system based using IEC 61499/4DIAC
  - Remote control possibilities of laboratory components



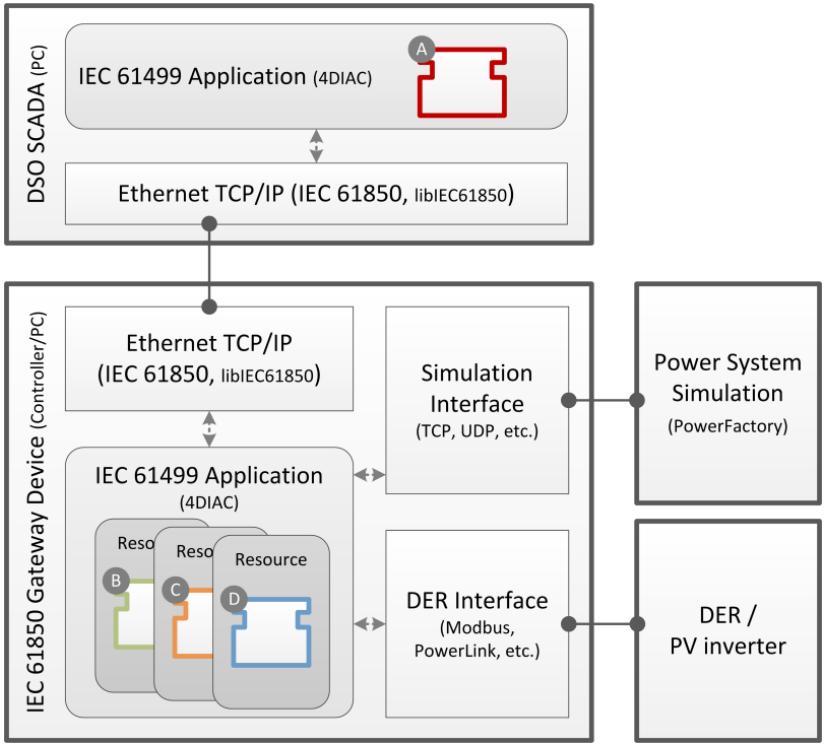
IEC 61850 Smart Grid Environment

- Simple overview of attack scenario



IEC 61850/61499 PV Remote Control

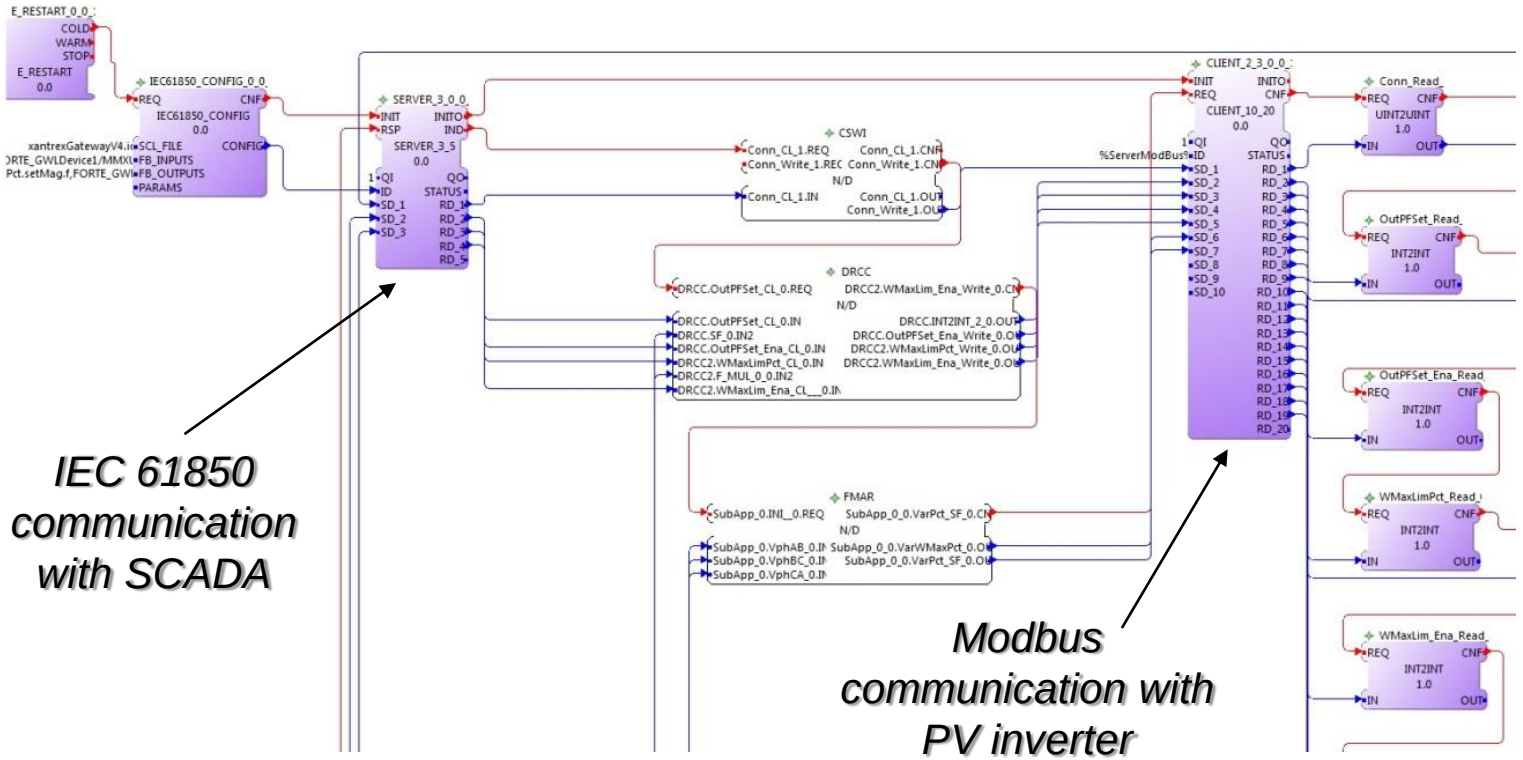
- 4DIAC implementation
  - IEC 61850 interface for PV inverters realized with IEC 61499/4DIAC



EU FP7 Programme Contract No. 608224

IEC 61850/61499 PV Remote Control

- 4DIAC implementation
  - IEC 61499 application using IEC 61850 and Modbus communication



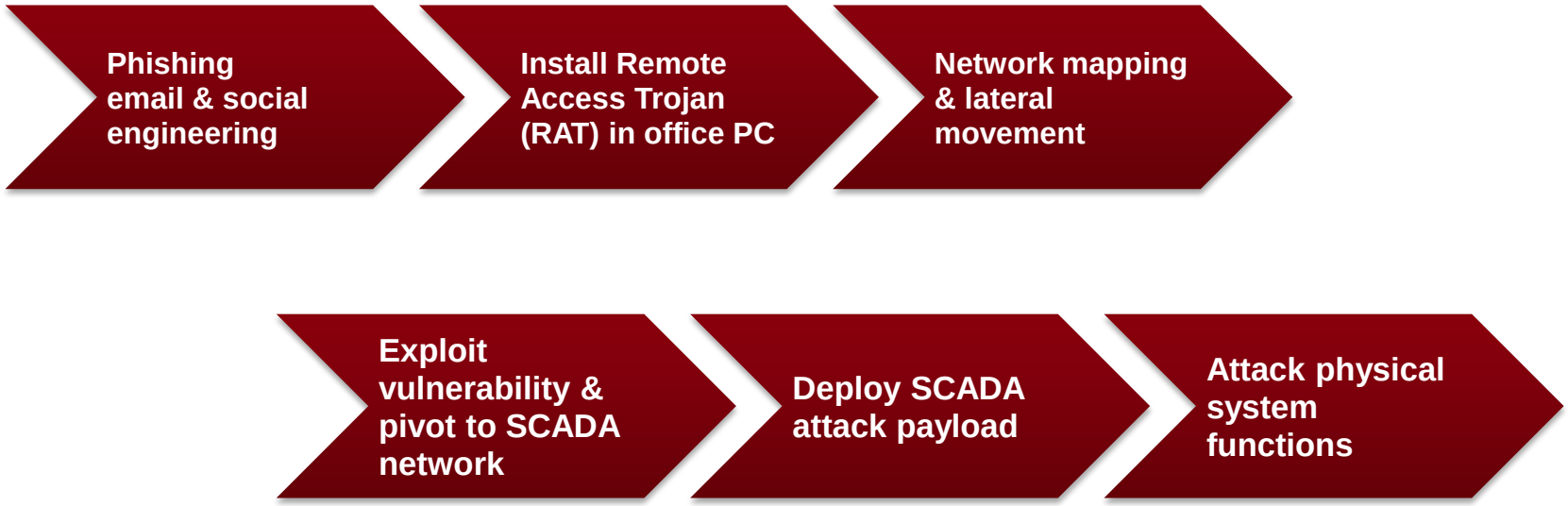
IEC 61850/61499 PV Remote Control

- Used validation setup with the Raspberry Pi

EU FP7 Programme Contract No. 608224

Cyber-Attack Scenario

- SPARKS demonstration scenario ...

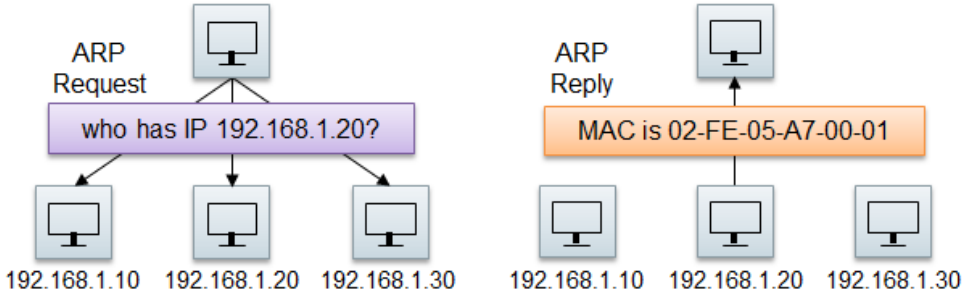


→ *Details are provided at the SPARKS website*

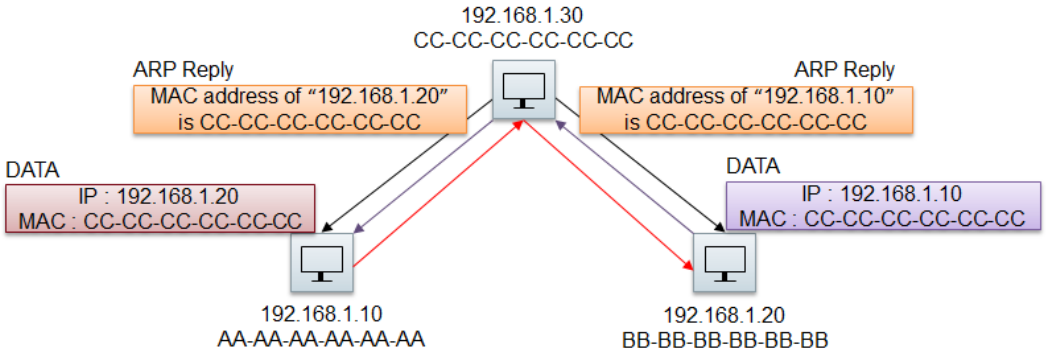
Cyber-Attack Scenario

- Man-in-the-middle (MITM) attack

Address Resolution Protocol (ARP)



ARP Poisoning

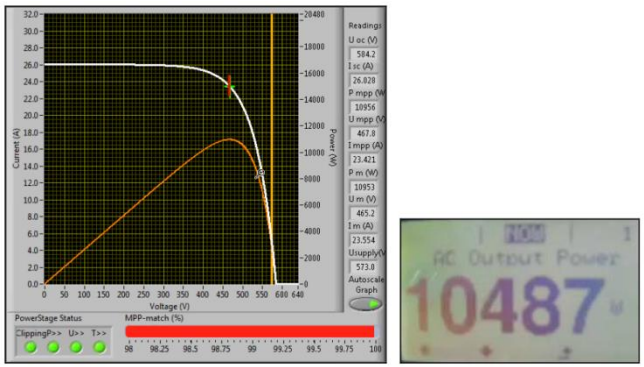



```
[1] 10.55.55.121 -> 10.55.55.111
[2] 10.55.55.111 -> 10.55.55.121
[3] 10.55.55.121 -> 10.55.55.111
[4] 10.55.55.111 -> 10.55.55.121

!!!Injection : 10.55.55.121 -> 10.55.55.111

[5] 10.55.55.111 -> 10.55.55.121

!!!Packet Drop


!!!Injection : 10.55.55.121 -> 10.55.55.111

[6] 10.55.55.111 -> 10.55.55.121

!!!Packet Drop

[7] 10.55.55.121 -> 10.55.55.111
[8] 10.55.55.111 -> 10.55.55.121
```

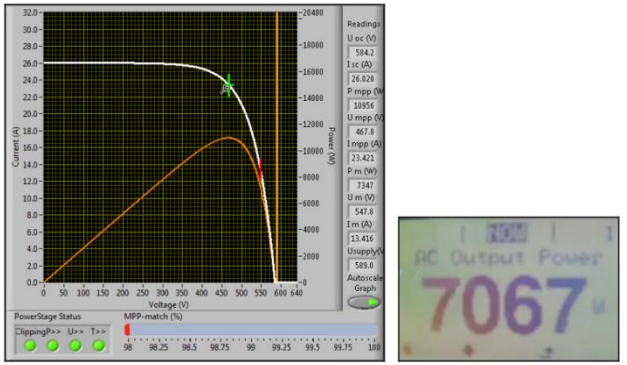
Attacker Interface (based on Ettercap)

Cyber-Attack Scenario

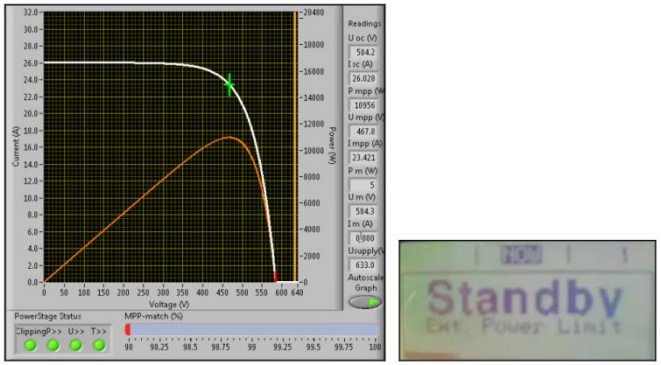
- Physical impact on PV inverter
  - Attack (manipulation) of inverter set-points (active power)



(a) 100% of power limitation by the operator



(b) 60% of power limitation by the operator



(c) 10% of power limitation by the attacker

Conclusions

- Recent cyber-attacks showed
  - Control systems are being specifically targeted
  - Attackers display technical knowledge of underlying communications, control systems and physical systems
  - Trajectory is towards selective intrusions and tailored attacks
- Better understand the physical consequences of cyber-attacks needed
- Analysis of cyber-attacks in the laboratory context in FP7 SPARKS
  - IEC 61850/61499 gateway implementation for cost-affective upgrade possibility of PV inverters implemented in 4DIAC
  - Existing PV inverters become IEC 61850 compliant
  - Cyber-attack scenario made in the AIT SmartEST lab