SCADA-Specific Intrusion Detection System

Kieran McLaughlin

CSIT, Queen's University Belfast

EU FP7 Programme Contract No. 608224

Outline

- Background & Motivation
- IEC 61850 environment
- Anticipated SCADA IDS outcomes
- Conclusions

Background

- SCADA protocols initially designed without considering cyber security
  - Plaintext message transmission
  - Authentication, encryption, etc. not commonly used
  - Legacy protocols still in use, still being rolled out
- Smart Grid systems are cyber-physical control systems
- Adding cyber security based only on IT security principles ignores SCADA system characteristics

EU FP7 Programme Contract No. 608224

SCADA Vulnerabilities

- Interconnected IT systems (e.g. office network) can provide ‘beachhead’ for attacks
- Intruders able to pivot to the SCADA network can:
  - Sniff, observe, learn, record, replay, tamper, launch man-in-the-middle attacks, exfiltrate data
- Attacks on SCADA threaten:
  - System availability
  - Data and control integrity
- Cyber attack =>

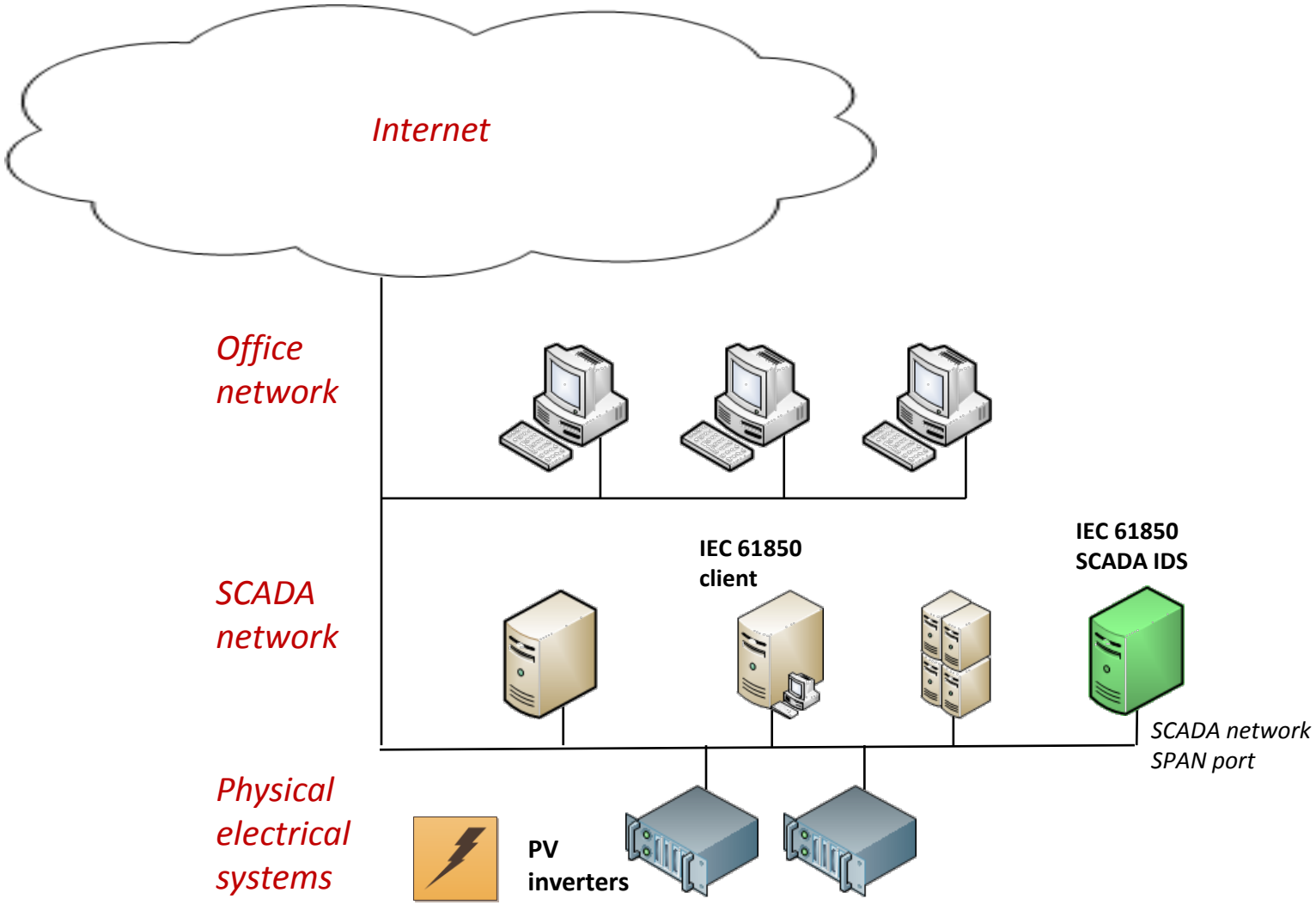
  Physical impact

Motivation

- Current cyber security deployments:
  - Generally lack awareness of power systems properties
  - Lack deep protocol analysis at SCADA application layer
  - NIST recommends further research on above, as well as whitelist enforcement
- Our aims:
  - Combine SCADA and power systems knowledge for protocol verification and correlation of application layer data
  - SCADA protocol verification, stateful analysis, and functional whitelisting
  - IDS platform monitoring multiple security attributes

EU FP7 Programme Contract No. 608224

IEC 61850 Environment

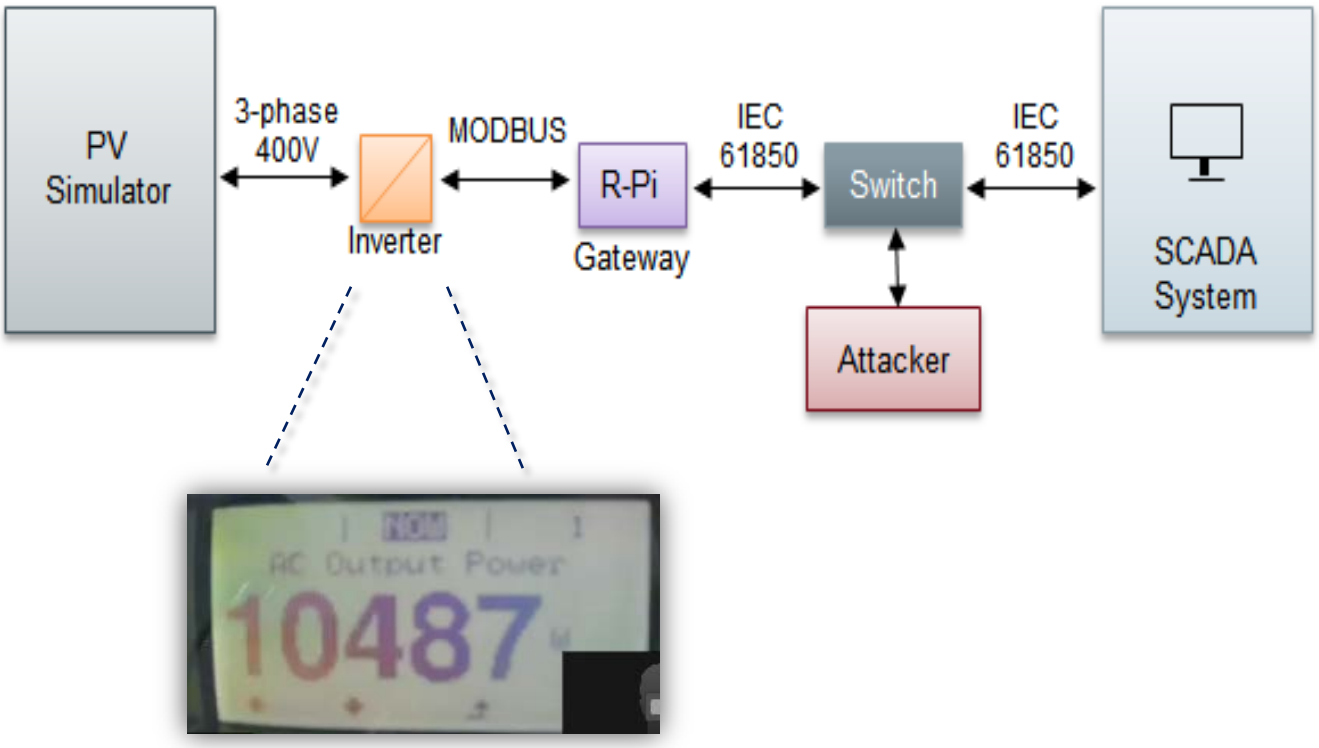


IEC 61850 Environment

- Target is AIT SmartEST Lab demonstration
  - Focus on IEC 61850 protocol
  - Standard for power utility automation
  - Scenario based on PV inverter control
- IEC1850 SCADA IDS to monitor communications
  - IEC 61850 server (inverter side)
  - IEC 61850 client (HMI)

EU FP7 Programme Contract No. 608224

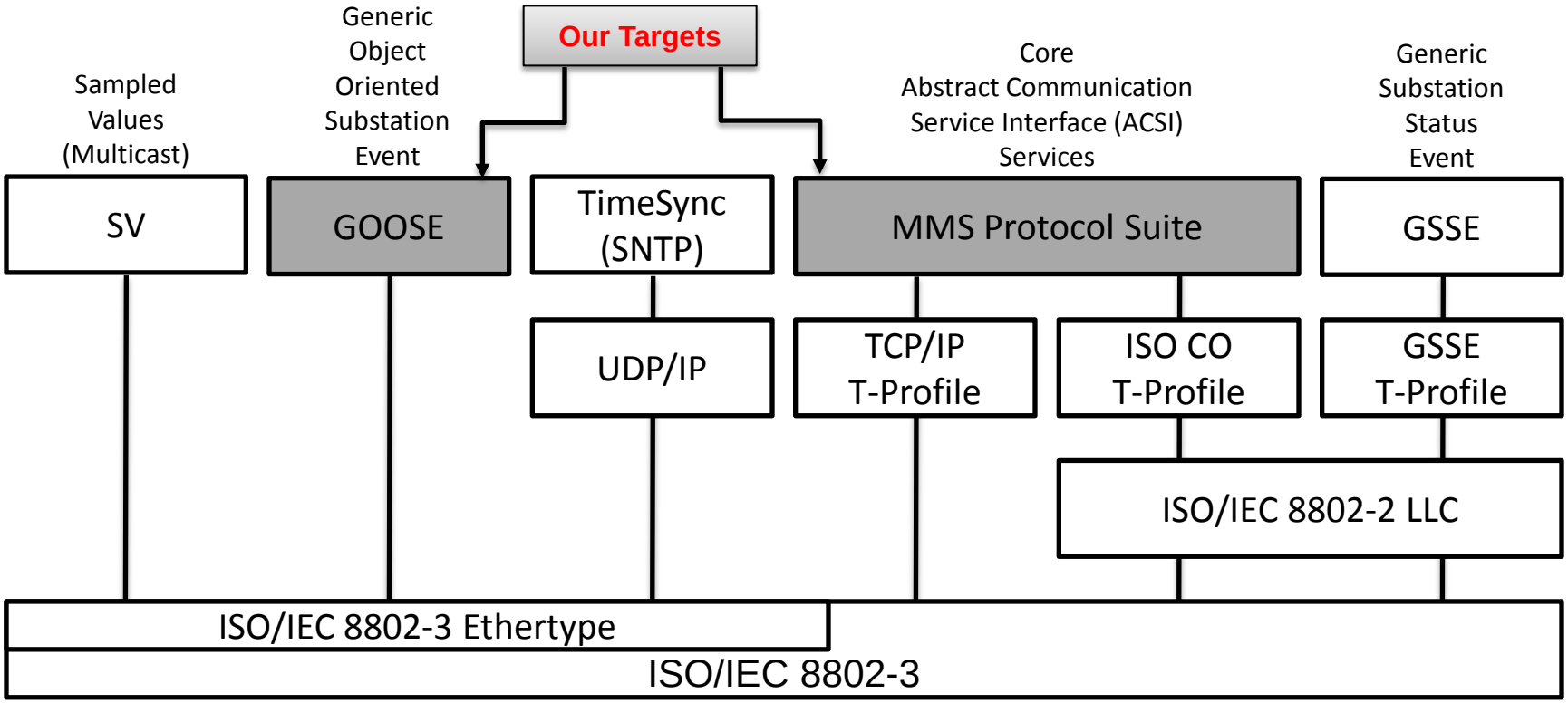
IEC 61850 Smart Grid Environment



EU FP7 Programme Contract No. 608224

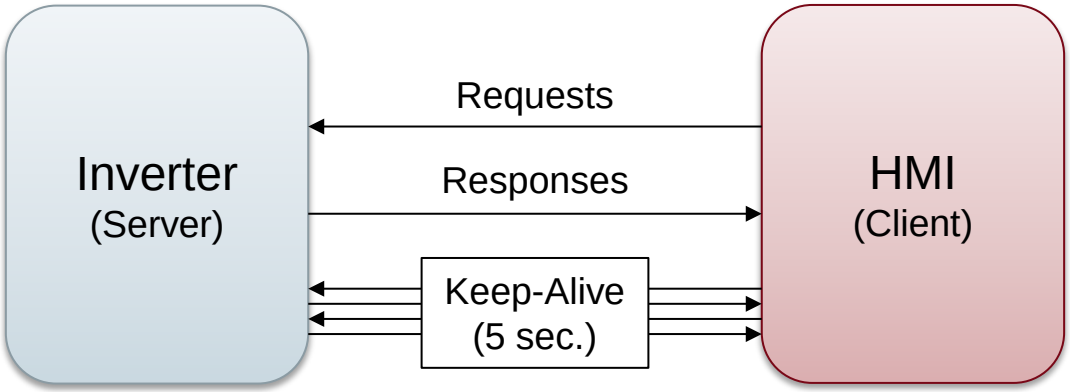
IEC 61850

- Communication Services
  - SV, GOOSE, GSSE and MMS



Protocol Analysis of Environment

- Communication between Inverter and HMI
  - Requests/Responses
    - getVariableAccessAttributes
    - read & write
  - Keep-alive packets if no message for 5 seconds

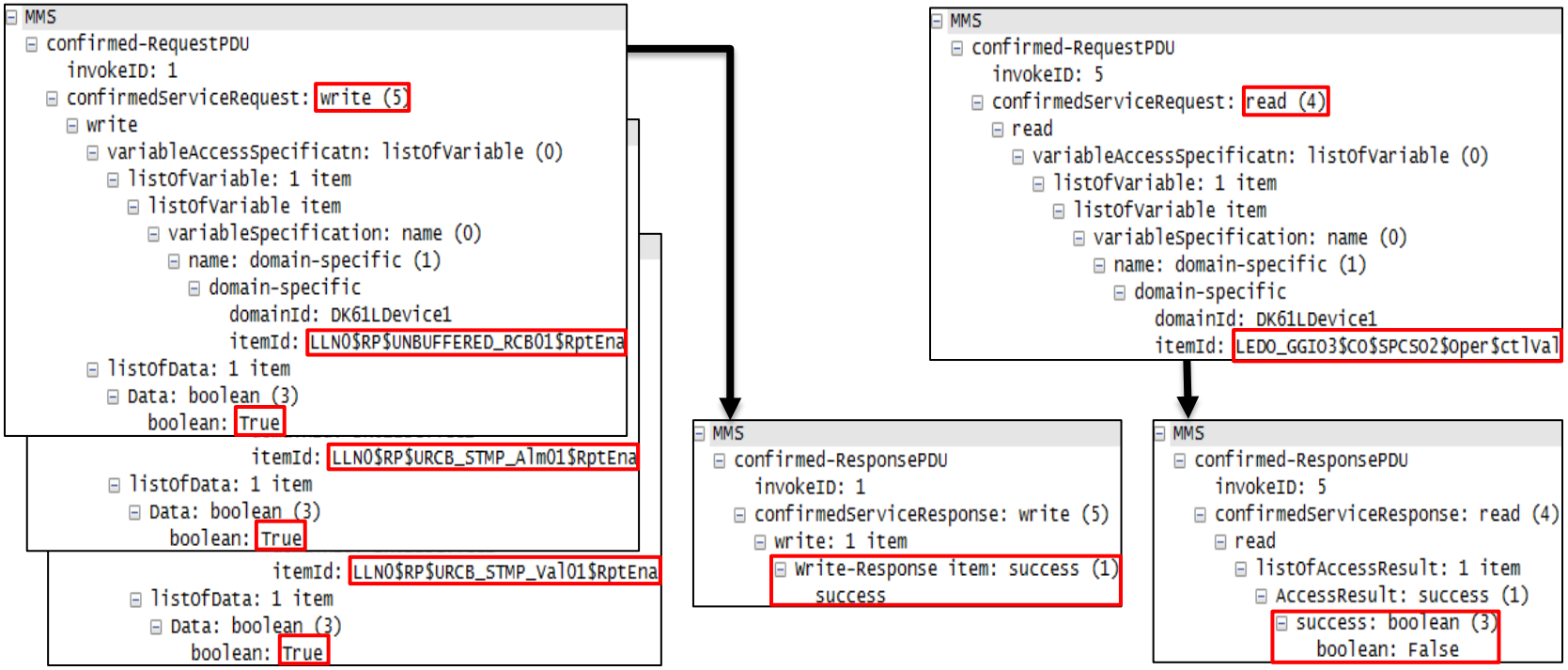


EU FP7 Programme Contract No. 608224

Protocol Analysis of Environment: MMS Request / Response

SMART GRID PROTECTION AGAINST CYBER ATTACKS

13	9.277471	192.168.17.243	192.168.17.246	MMS	141 confirmed-RequestPDU
14	9.278617	192.168.17.246	192.168.17.243	MMS	83 confirmed-ResponsePDU
15	9.386858	192.168.17.243	192.168.17.246	MMS	140 confirmed-RequestPDU
16	9.387904	192.168.17.246	192.168.17.243	MMS	83 confirmed-ResponsePDU
17	9.496374	192.168.17.243	192.168.17.246	MMS	140 confirmed-RequestPDU
18	9.497548	192.168.17.246	192.168.17.243	MMS	83 confirmed-ResponsePDU
19	9.683843	192.168.17.243	192.168.17.246	TCP	54 avocent-proxy > iso-tsap [ACK] Seq=473 Ack=272 Win=65264 Len=0

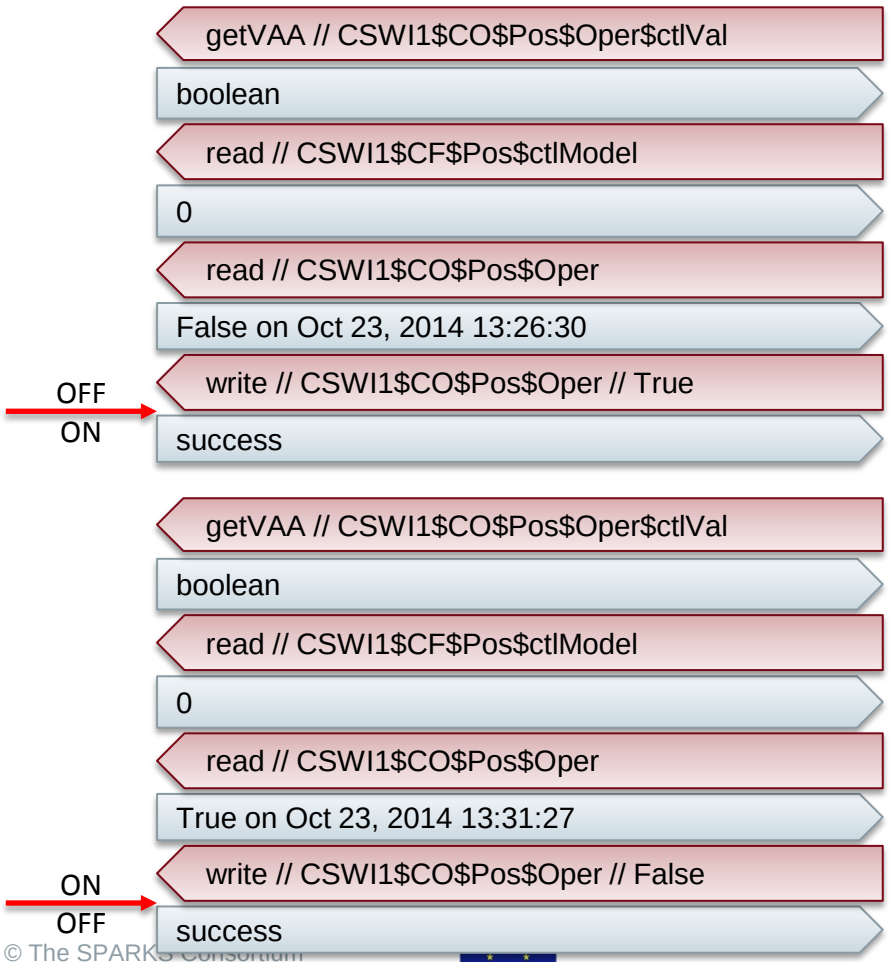


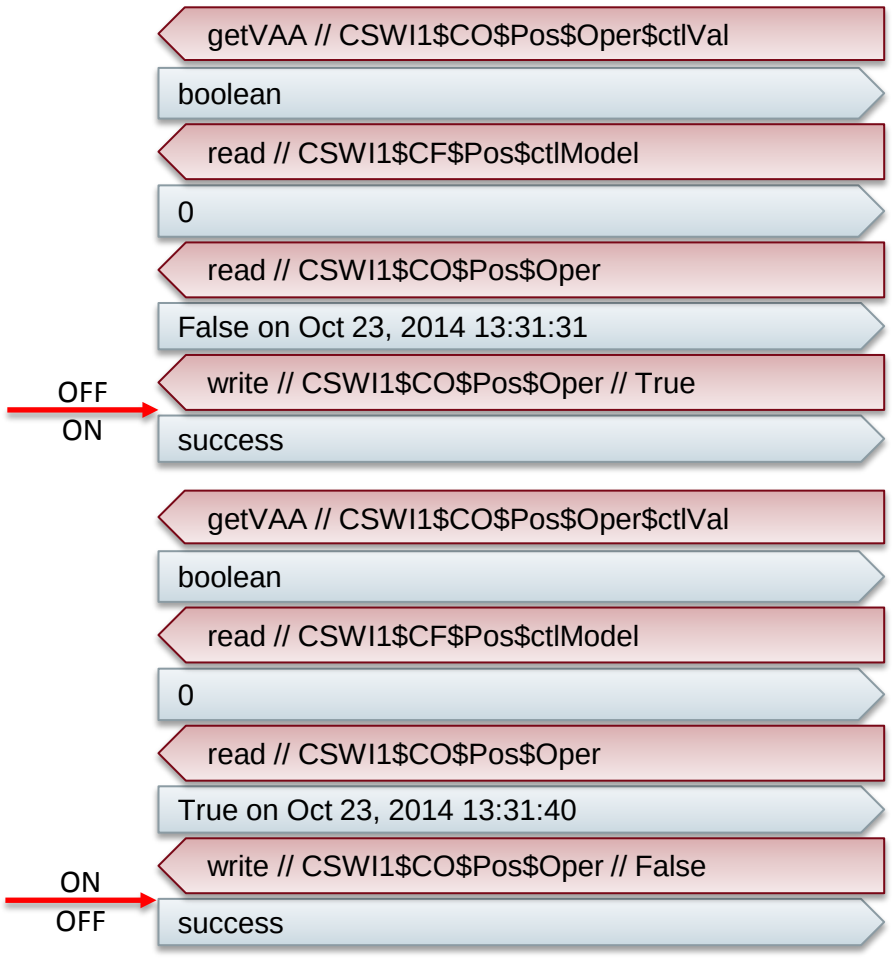
Protocol Analysis of Environment: On-Off Command

SMART GRID PROTECTION AGAINST CYBER ATTACKS

INVERTER ← HMI

INVERTER → HMI





EU FP7 Programme Contract No. 608224

SCADA IDS Intended Outcomes

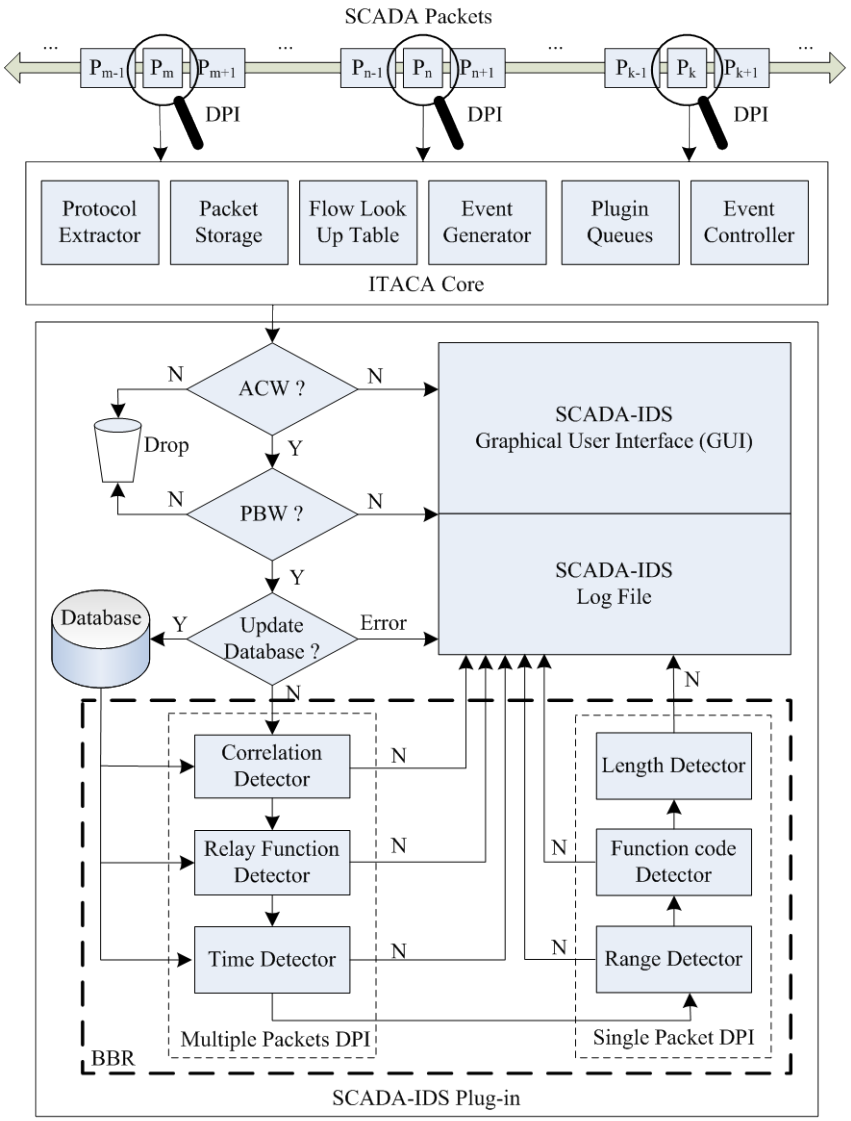
- Enforce cyber security policies derived from analysis:
  - Expert knowledge of physical system
  - Communication requirements of SCADA network
- Development of a multi-attribute SCADA-IDS
  - Identify permitted and non-permitted devices, connections, and protocols
  - Enhanced payload inspection to detect permitted and non-permitted operations and behaviours
  - Whitelist, stateful and behavioural analysis based on 61850 features and SmartEST demo physical system attributes

EU FP7 Programme Contract No. 608224

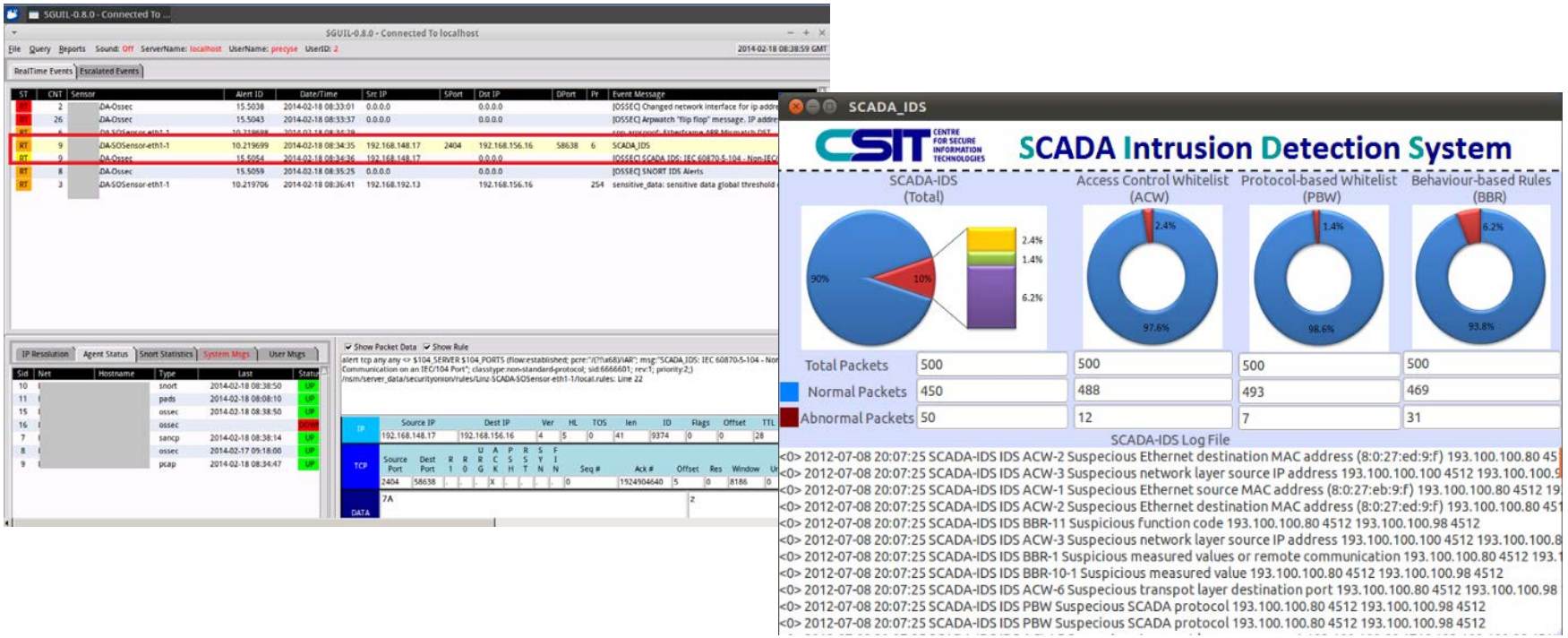
SCADA IDS Intended Outcomes

Build on current CSIT IDS toolkit capabilities for IEC61850:

- Access control whitelists
- Protocol based whitelists: applying deep packet inspection to SCADA application layer
- Stateful protocol analysis of packet flows
- Behaviour based rules: timing, communications modelling



SCADA IDS Intended Outcomes



(Left) Custom IDS rules developed for standard open source tools such as Snort

(Right) Custom SCADA IDS tool incorporates custom Snort rules, plus stateful analysis which Snort cannot provide

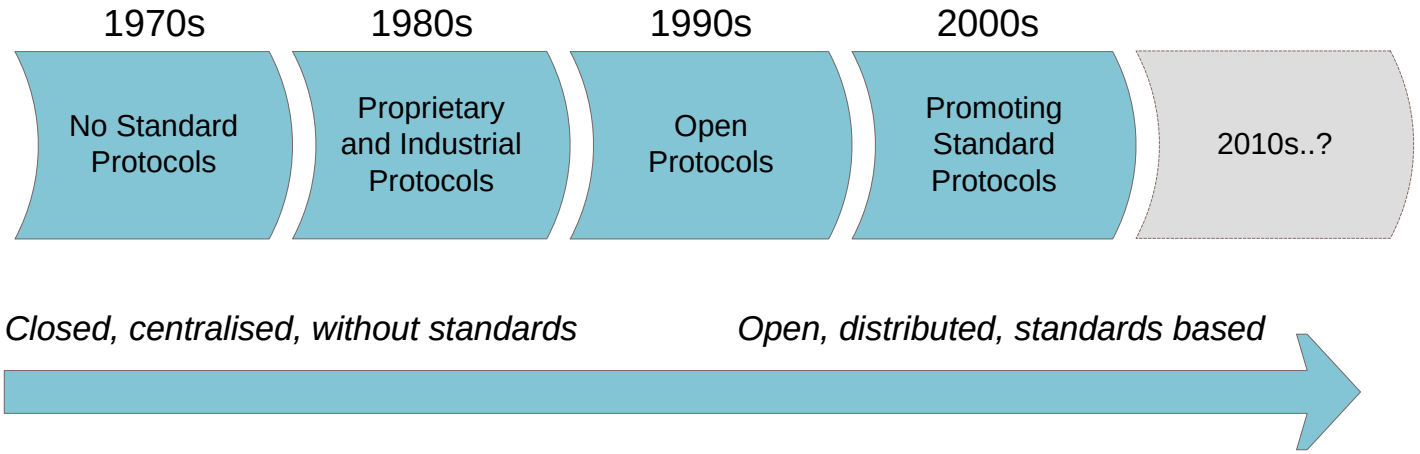
EU FP7 Programme Contract No. 608224

Conclusions

- Need fundamental “low-level” alerts directly linked to SCADA
  - Increased visibility of attack steps being executed
  - Detect SCADA-specific attacks that standard IT approaches cannot
- Detect malformed or malicious packets
  - Due to replay or protocol fuzzing
  - Even if the attack is ineffective, something is wrong
- Can indicate wider problems
  - IT assets may already be compromised (e.g. by 0-day)
  - Misconfiguration, abnormalities
- Combine with other alerts to form view of wider attacks
  - Provide enhanced “security sensor” data for event correlation
  - Use for traceability, forensic analysis

EU FP7 Programme Contract No. 608224

Conclusions



A brief history of SCADA communication protocols

- Prediction: 2010s the decade when open and standard –*but obscure*– SCADA protocols become known by attackers
- Our work contributes to mitigating the impact of likely consequent attacks in the SCADA domain