



SCADA-Specific Intrusion Detection System

Kieran McLaughlin

CSIT, Queen's University Belfast



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

SCADA Vulnerabilities

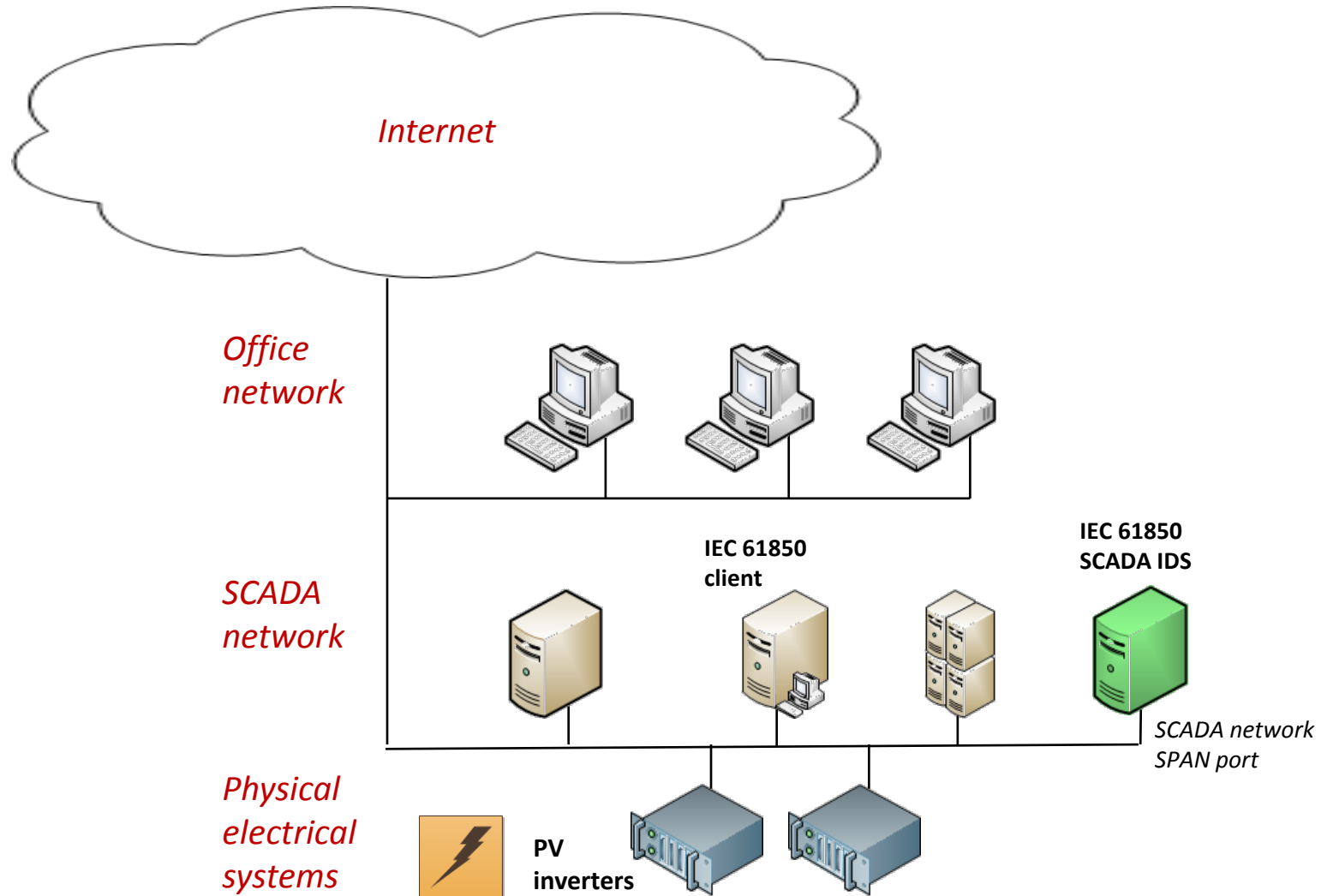
- Interconnected IT systems (e.g. office network) can provide ‘beachhead’ for attacks
- Intruders able to pivot to the SCADA network can:
 - Sniff, observe, learn, record, replay, tamper, launch man-in-the-middle attacks, exfiltrate data
- Attacks on SCADA threaten:
 - System availability
 - Data and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

IEC 61850 Environment

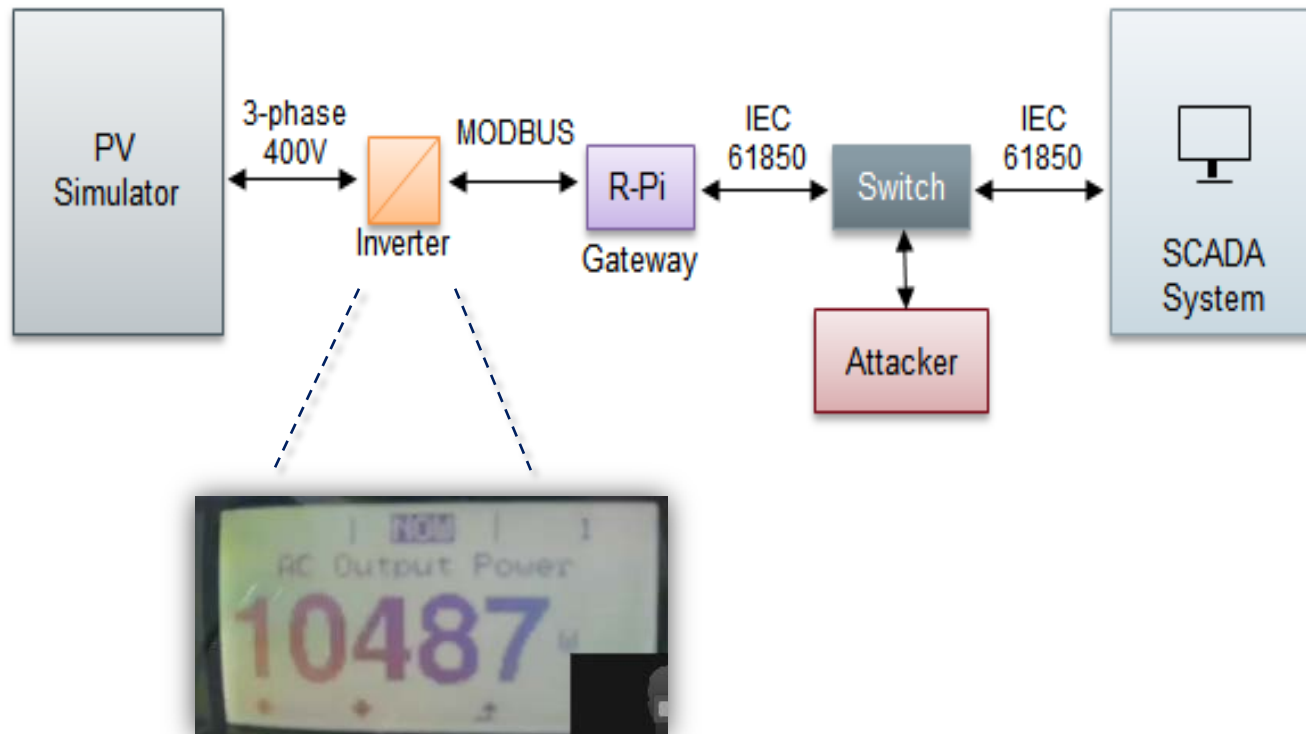


IEC 61850 Environment

- 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)

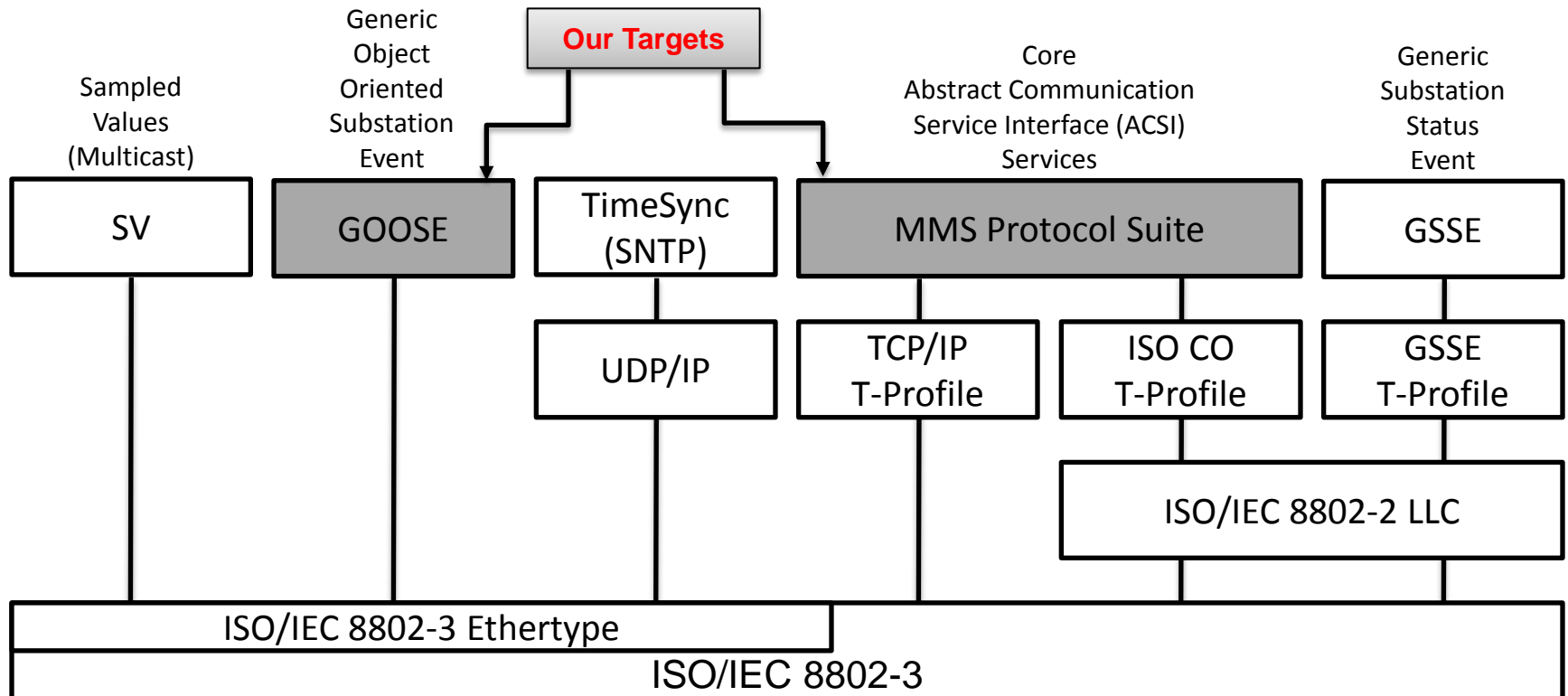


IEC 61850 Smart Grid Environment



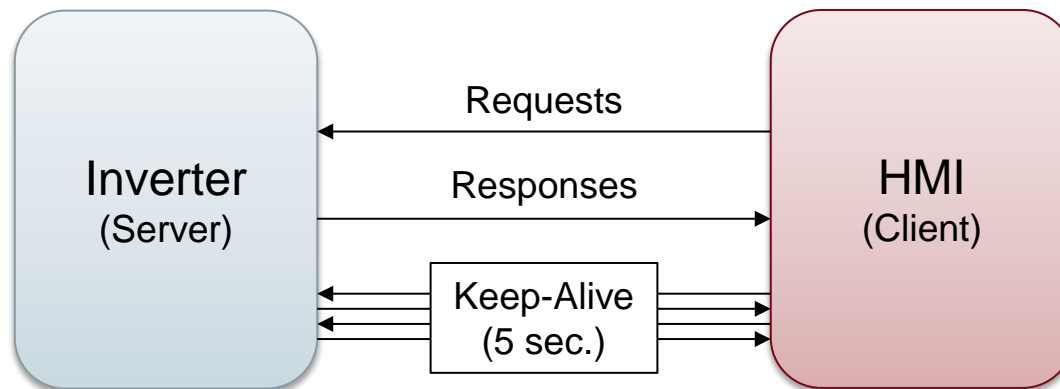
IEC 61850

- Communication Services
 - SV, GOOSE, GSSE and MMS



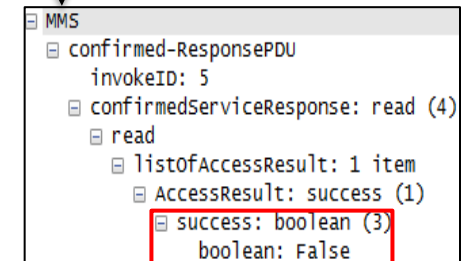
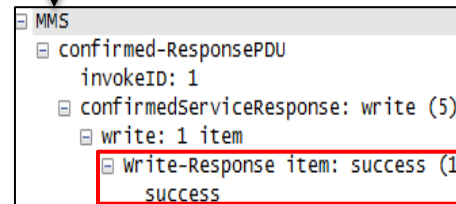
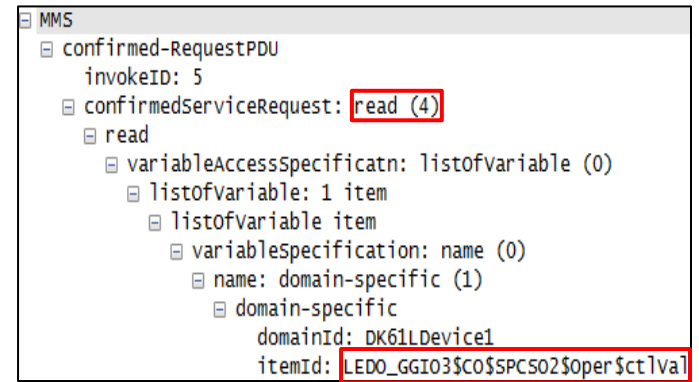
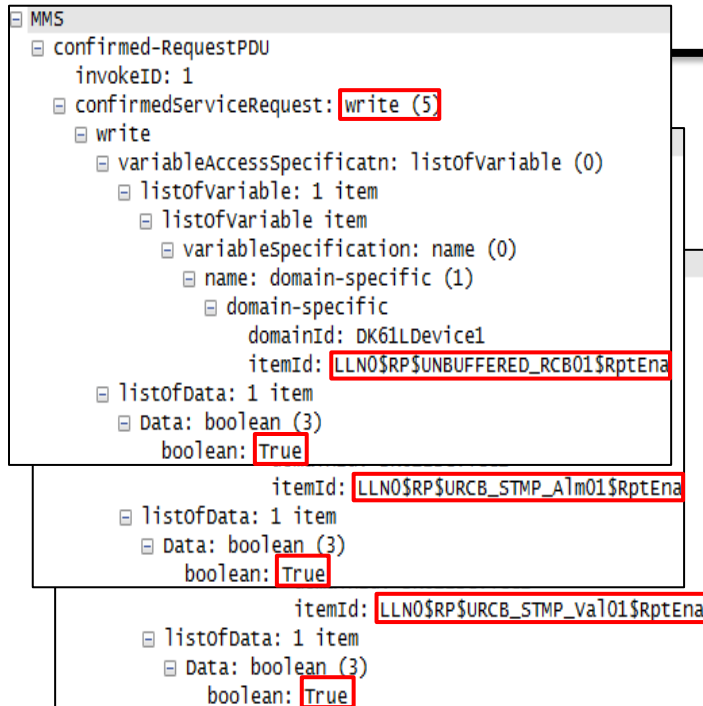
Protocol Analysis of Environment

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

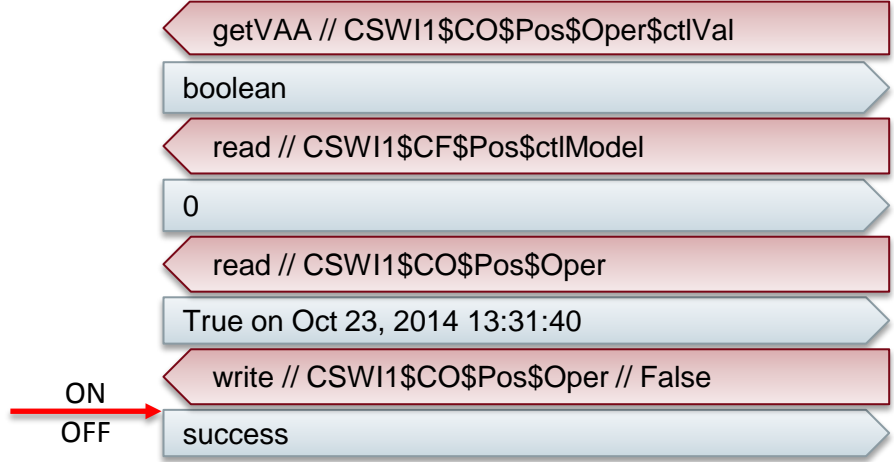
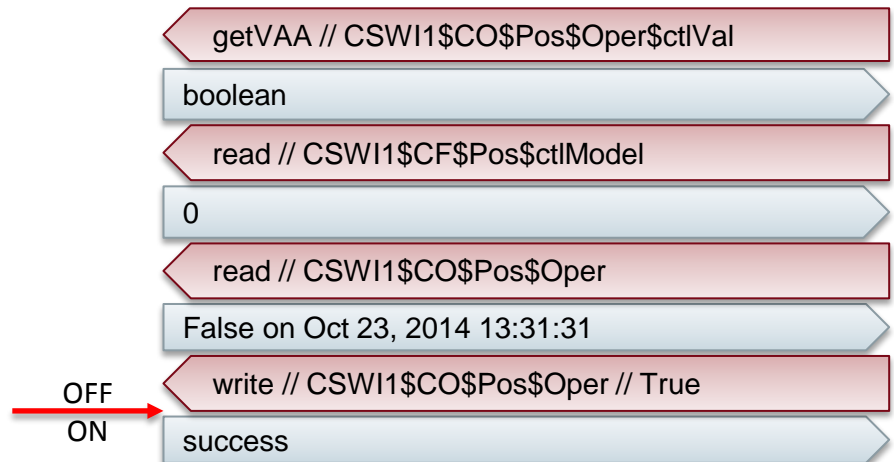
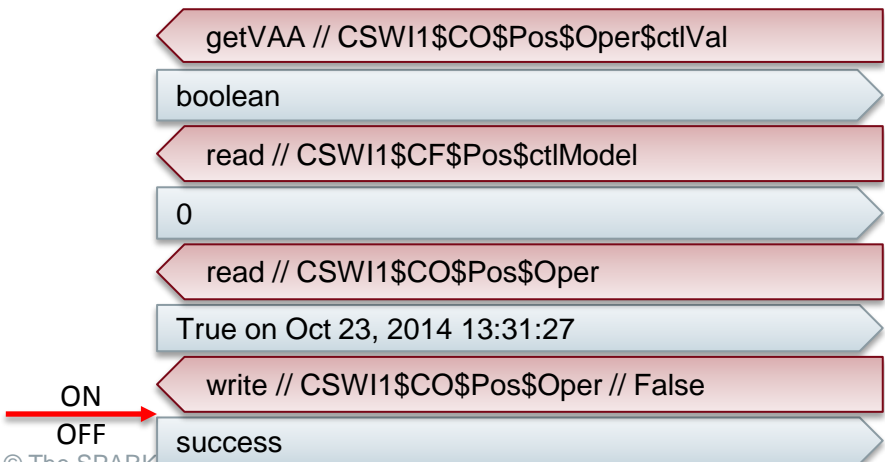
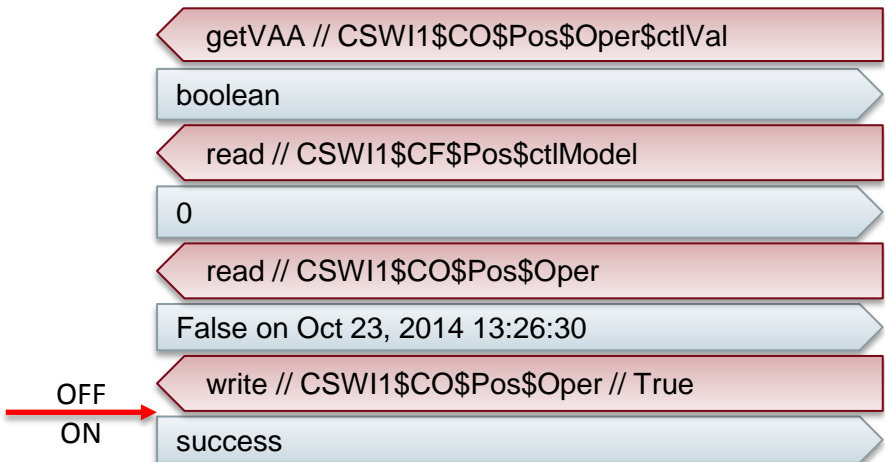
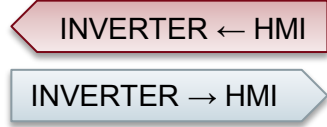


Protocol Analysis of Environment: MMS Request / Response

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



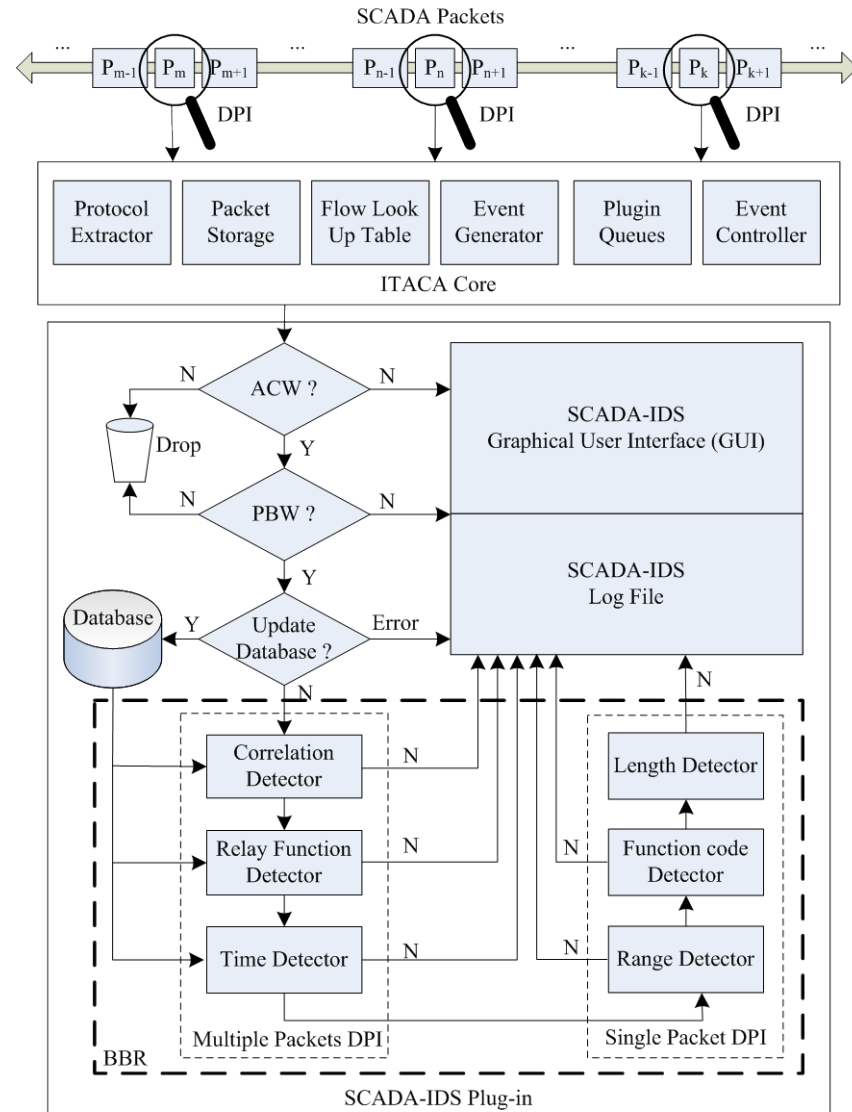
SCADA IDS Intended Outcomes

- 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

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



SGUIL-0.8.0 - Connected to localhost

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	JA-Ossec	15.5038	2014-02-18 08:33:01	0.0.0.0	0.0.0.0				[OSSEC] Changed network interface for ip addr
RT	26	JA-Ossec	15.5043	2014-02-18 08:33:37	0.0.0.0	0.0.0.0				[OSSEC] Arpswatch "Top flip" message: IP addr
RT	6	JA-SOSensor-eth1-1	10.219698	2014-02-18 08:34:38						[OSSEC] SCADA IDS: IEC 60870-5-104 - NonIEC
RT	9	JA-SOSensor-eth1-1	10.219699	2014-02-18 08:34:35	192.168.148.17	2404	192.168.156.16	58638	6	SCADA_IDS
RT	9	JA-Ossec	15.5054	2014-02-18 08:34:36	192.168.148.17	0.0.0.0				[OSSEC] SCADA IDS: IEC 60870-5-104 - NonIEC
RT	8	JA-Ossec	15.5059	2014-02-18 08:35:25	0.0.0.0	0.0.0.0				[OSSEC] SNOOT IDS Alerts
RT	3	JA-SOSensor-eth1-1	10.219706	2014-02-18 08:36:41	192.168.192.13		192.168.156.16		254	sensitive_data: sensitive data global threshold

SCADA Intrusion Detection System

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Category	Total	Normal	Abnormal
SCADA-IDS (Total)	500	450	50
Access Control Whitelist (ACW)	500	488	12
Protocol-based Whitelist (PBW)	500	493	7
Behaviour-based Rules (BBR)	500	469	31

SCADA-IDS Log File

```

<0> 2012-07-08 20:07:25 SCADA-IDS IDS ACW-2 Suspicious Ethernet destination MAC address (8:0:27:ed:9:f) 193.100.100.80 4512
<0> 2012-07-08 20:07:25 SCADA-IDS IDS ACW-3 Suspicious network layer source IP address 193.100.100.100 4512 193.100.100.80
<0> 2012-07-08 20:07:25 SCADA-IDS IDS ACW-1 Suspicious Ethernet source MAC address (8:0:27:eb:9:f) 193.100.100.80 4512 193.100.100.80
<0> 2012-07-08 20:07:25 SCADA-IDS IDS ACW-2 Suspicious Ethernet destination MAC address (8:0:27:ed:9:f) 193.100.100.80 4512
<0> 2012-07-08 20:07:25 SCADA-IDS IDS BBR-11 Suspicious function code 193.100.100.80 4512 193.100.100.80 4512
<0> 2012-07-08 20:07:25 SCADA-IDS IDS ACW-3 Suspicious network layer source IP address 193.100.100.100 4512 193.100.100.80
<0> 2012-07-08 20:07:25 SCADA-IDS IDS BBR-1 Suspicious measured values or remote communication 193.100.100.80 4512 193.100.100.80
<0> 2012-07-08 20:07:25 SCADA-IDS IDS BBR-10-1 Suspicious measured value 193.100.100.80 4512 193.100.100.98 4512
<0> 2012-07-08 20:07:25 SCADA-IDS IDS ACW-6 Suspicious transpot layer destination port 193.100.100.80 4512 193.100.100.98
<0> 2012-07-08 20:07:25 SCADA-IDS IDS PBW Suspicious SCADA protocol 193.100.100.80 4512 193.100.100.98 4512
<0> 2012-07-08 20:07:25 SCADA-IDS IDS PBW Suspicious SCADA protocol 193.100.100.80 4512 193.100.100.98 4512
    
```

(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

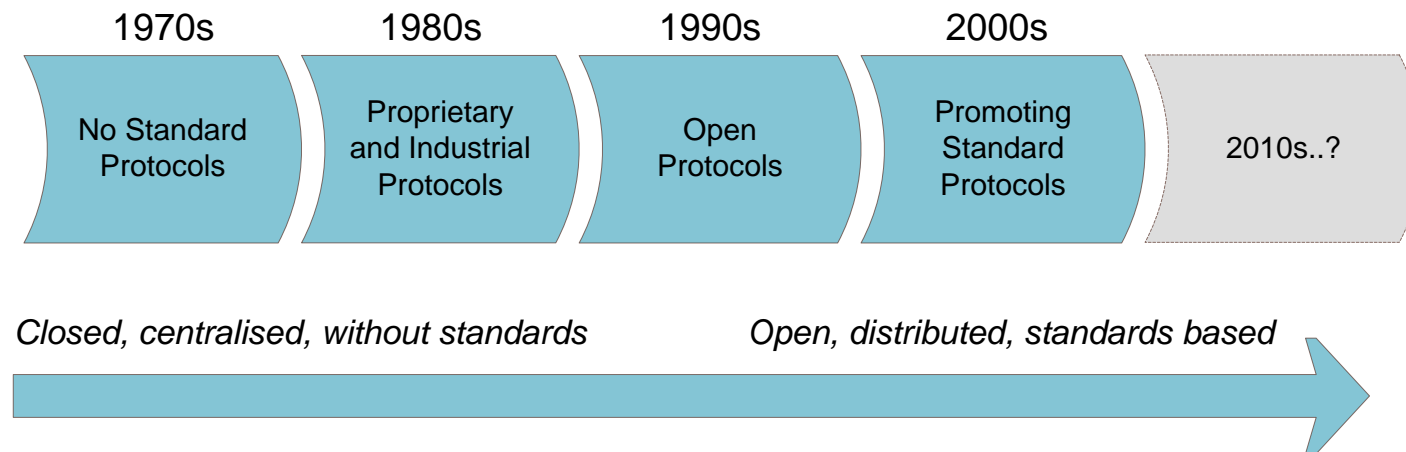


Conclusions

- 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



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