



Intrusion Detection for SCADA Systems

Dr Kieran McLaughlin

CSIT, Queen's University Belfast

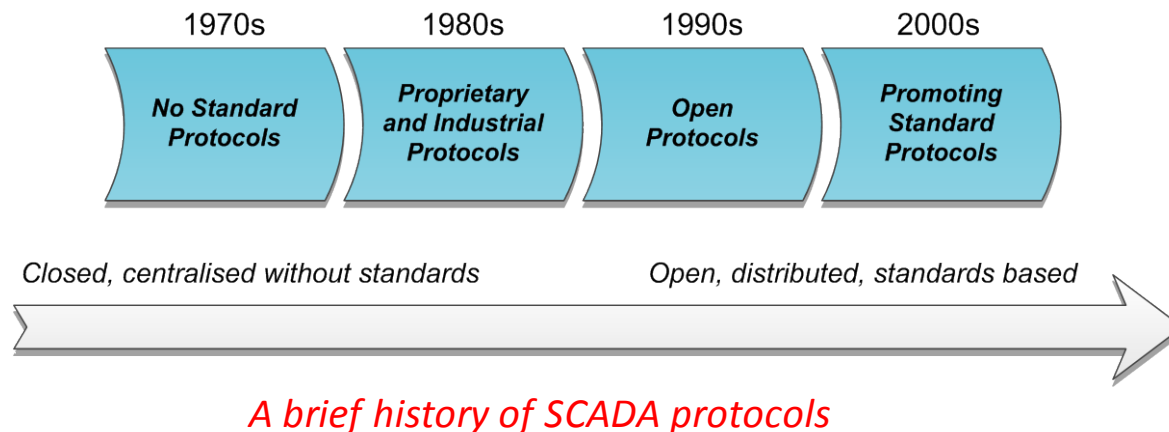


Outline

- Background & Motivation
- Experience with IEC 60870-5-104
- SCADA-IDS approach
- SPARKS mini-project targeting IEC 61850
- Questions...

SCADA Communications Security

- SCADA protocols (particularly legacy protocols) designed without considering cyber security
- Cyber security based only on IT security principles ignores SCADA system characteristics
- Smart Grid systems are cyber-physical control systems
- Due to critical nature of SCADA control, cyber security must consider availability and integrity



SCADA Vulnerabilities

- Interconnected IT systems can provide ‘beachhead’ for attacks
- Intruders with a foothold in the network can:
 - Sniff, observe, learn, record, replay, tamper, launch man-in-the-middle attacks, exfiltrate
- Plaintext message transmission
 - Authentication, encryption, etc. not commonly used
- Attacks on SCADA threaten:
 - System availability
 - Data and control integrity



Motivation for SCADA IDS

- Cyber security policies are derived from:
 - Expert knowledge of physical system
 - Communication requirements of SCADA network
- SCADA IDS technology
 - Can be deployed to support policy enforcement
 - Particularly policies “beyond IT”
 - Support monitoring for breaches
 - Provide enhanced “security sensor” data for event correlation

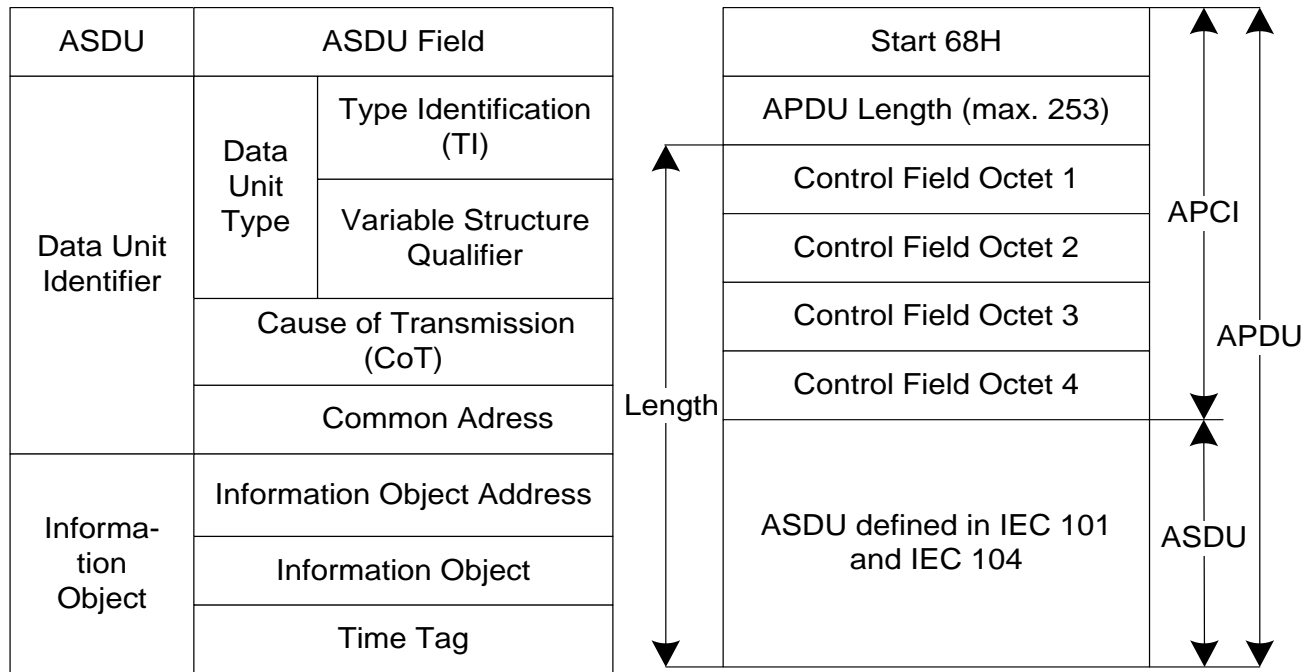
Experience with IEC 60870-5-104

- Water, gas, electricity telecontrol operations
 - Widely used in Europe
- Development of “104”
 - Started life in 1990’s as a serial communication standard
 - Released in 2000 as a TCP/IP standard
- Interconnection of IP networks raises risks
 - Cyber security risk
 - Control operation risk
 - Business risk



Experience with IEC 60870-5-104

- IP packet payload: “104” SCADA data...



ASDU structure

APDU structure



Designing Custom-104 IDS

- Protocol-Based Models

$$\forall P \in 104(I) \text{ format} \cdot TIField(P) \in \{45, 46\} \Rightarrow lenField(P) = 14$$

- Cross-field data correlation

$$\forall P \in 104Response \cdot TIField(P) = \{45 - 48, 100, 101\} \Rightarrow CoTField(P) = \{7, 10\}$$

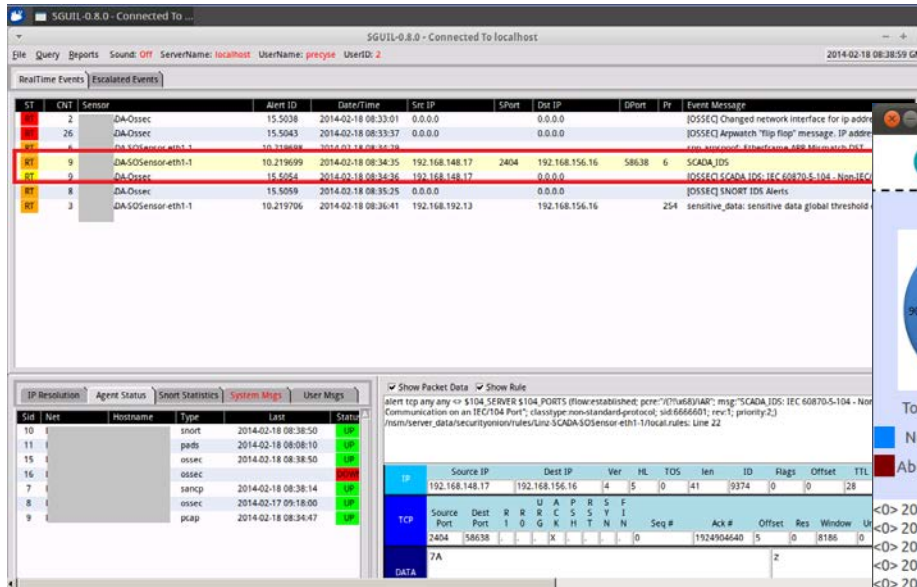
- Stateful protocol analysis of all packets in a flow

- Benefits:

- Better situational awareness in SCADA network
- Increased visibility of attack steps being executed
- Use for traceability, forensic analysis
- Detects attacks standard IT cyber security tools cannot



SCADA IDS results

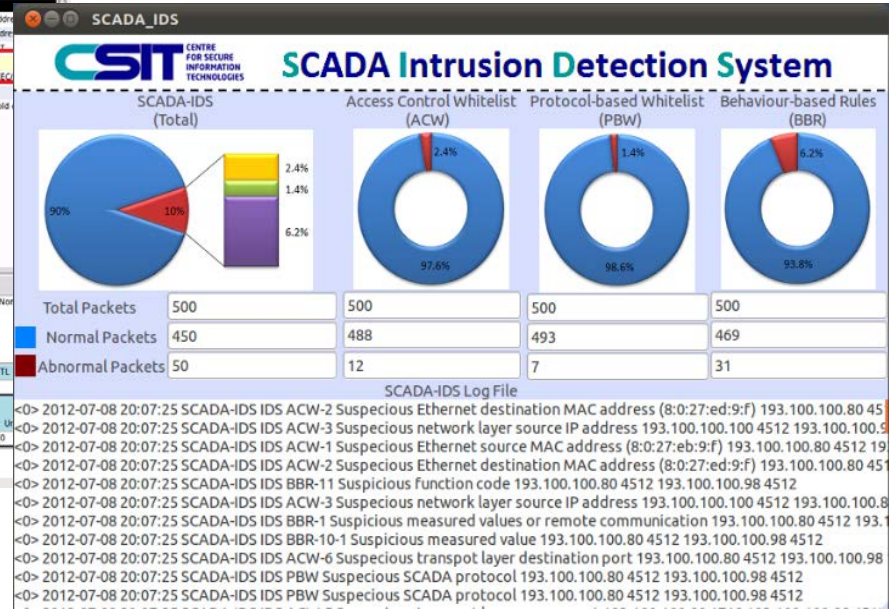


SGUIL-0.8.0 - Connected to localhost

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] Arpwatch "Top flip" message: IP addr
RT	6	JA-SOSensor-eth1-1	10.319698	2014-02-18 08:34:36						[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					[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

Alert top any any ↔ \$104 SERVER \$104 PORTS (flow-established: pcre:"(?!not\$)IAR":msg:"SCADA_IDS: IEC 60870-5-104 - NonIEC Communication on an IEC/104 Port", class-type:non-standard-protocol, sid:6666601, rev:1, priority:2) /!m/server_data/security/snort/rules/Line SCADA-SOSensor-eth1-1/local.rules: Line 22

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL
TCP	192.168.148.17	192.168.156.16	4	5	0	41	9374	0	0	28
Port	2404	58638								
Seq#							1924904640			
Res								0	8186	0
Window										
Urg										
DATA										



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 193.100.100.80
<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



SPARKS Mini-Project



- State of the art tools:
 - Generally lack awareness of power systems properties
 - Lack stateful 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 temporal / physical data
 - SCADA protocol verification, stateful analysis, and functional whitelisting
 - Unified platform monitoring multiple security attributes



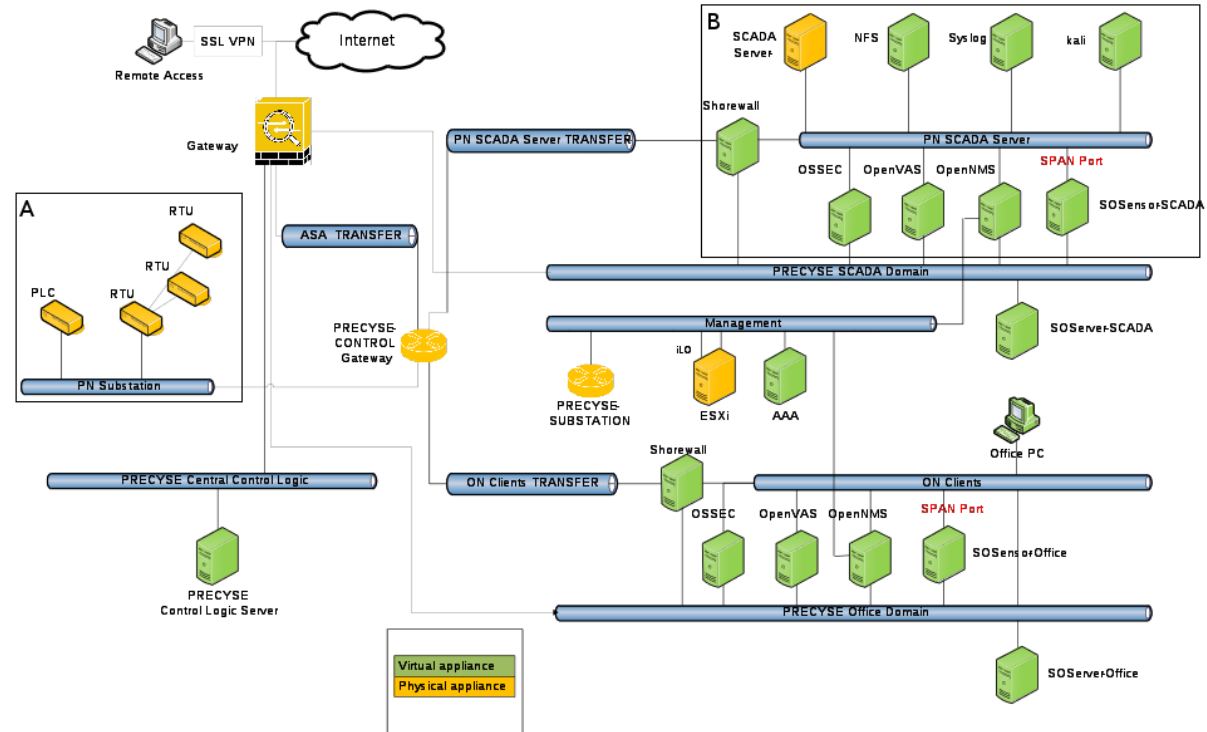
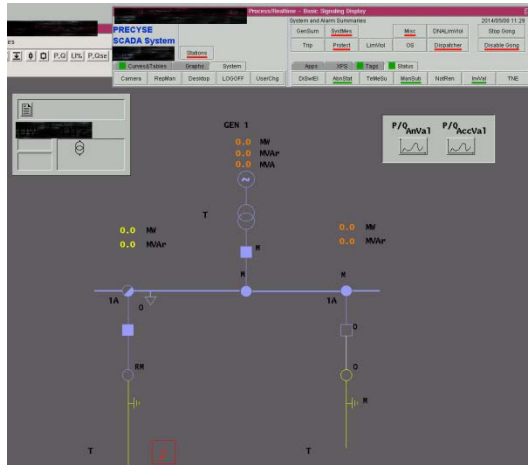
SPARKS Mini-Project

- Target is AIT SmartEST Lab demonstration
 - Focus on IEC 61850 protocol
 - Custom SCADA IDS
 - Also develop attack use cases
- 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



Attack Demonstrations

- Build on previous experience attacking “104” (below)
- In SPARKS we will attack 61850
 - Data injection, Replay, Man-in-the-Middle



Questions

- Which SCADA protocols are currently in use within your networks?
 - e.g. IEC 60870, IEC 61850, DNP3, etc.
- What information do you have regarding cyber-risks specific to such protocols?
 - What are your sources? (e.g. from manufacturers, standards, risk analysis approaches)
- Do you believe cyber-attacks on SCADA communications to be:
 - High probability – low probability?
 - High operational impact – low operational impact?
- Security measures in place:
 - Are these protocols implemented with any validation/authentication features?
 - How do you defend/protect networks using these protocols? (e.g. firewalls, etc)?
 - How do you monitor for attacks or anomalies in the SCADA communications?
 - Have you carried out any penetration testing of related systems?
- How critical is the secure operation of SCADA communications to your overall systems?
 - What are the consequences for system operations if there is corrupt / untrustworthy data, or deliberately manipulated sensor data?

