
# Intrusion Detection for SCADA Systems

Dr Kieran McLaughlin

CSIT, Queen's University Belfast


EU FP7 Programme Contract No. 608224

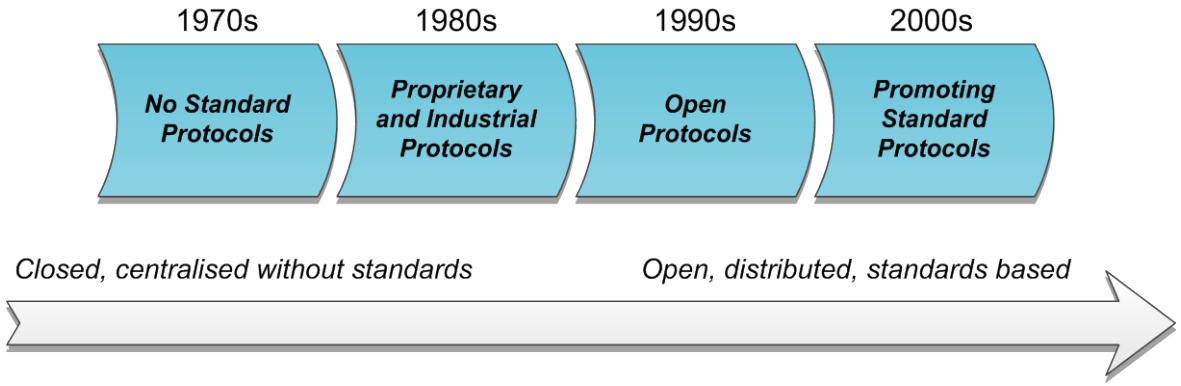
# Outline

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


EU FP7 Programme Contract No. 608224

# 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




*A brief history of SCADA protocols*

# 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

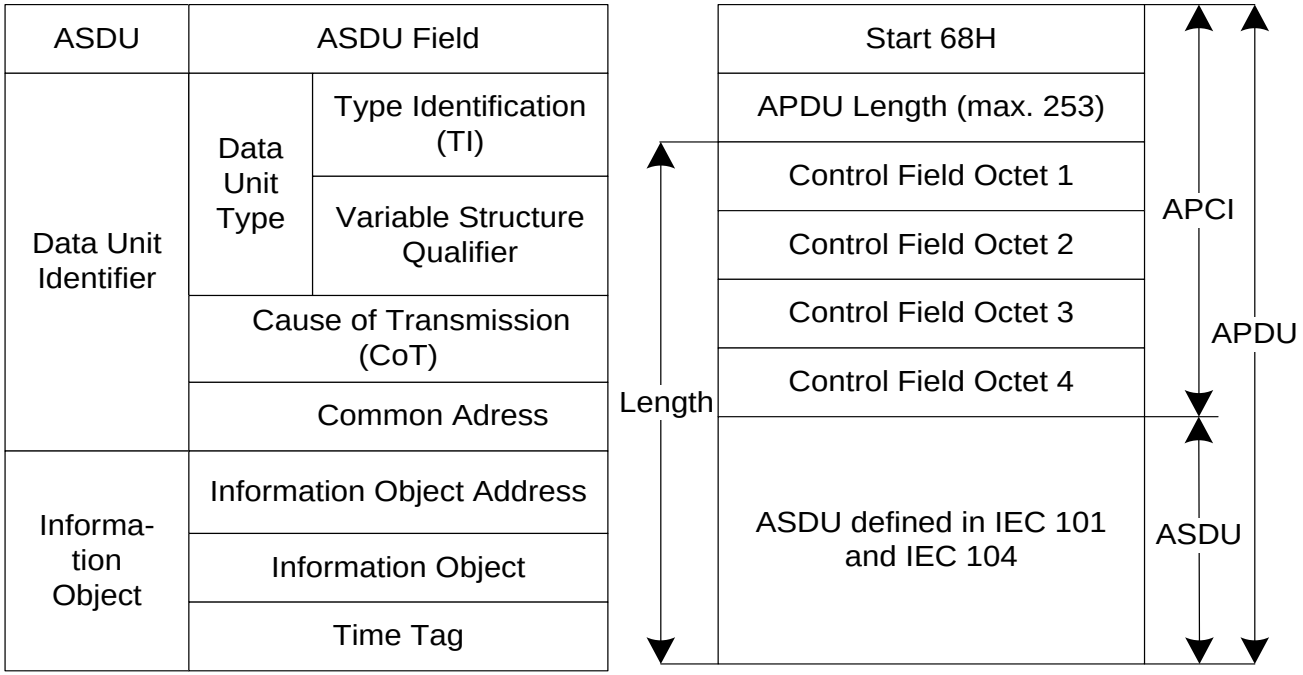

EU FP7 Programme Contract No. 608224

# 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

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Protocol-Based Models

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

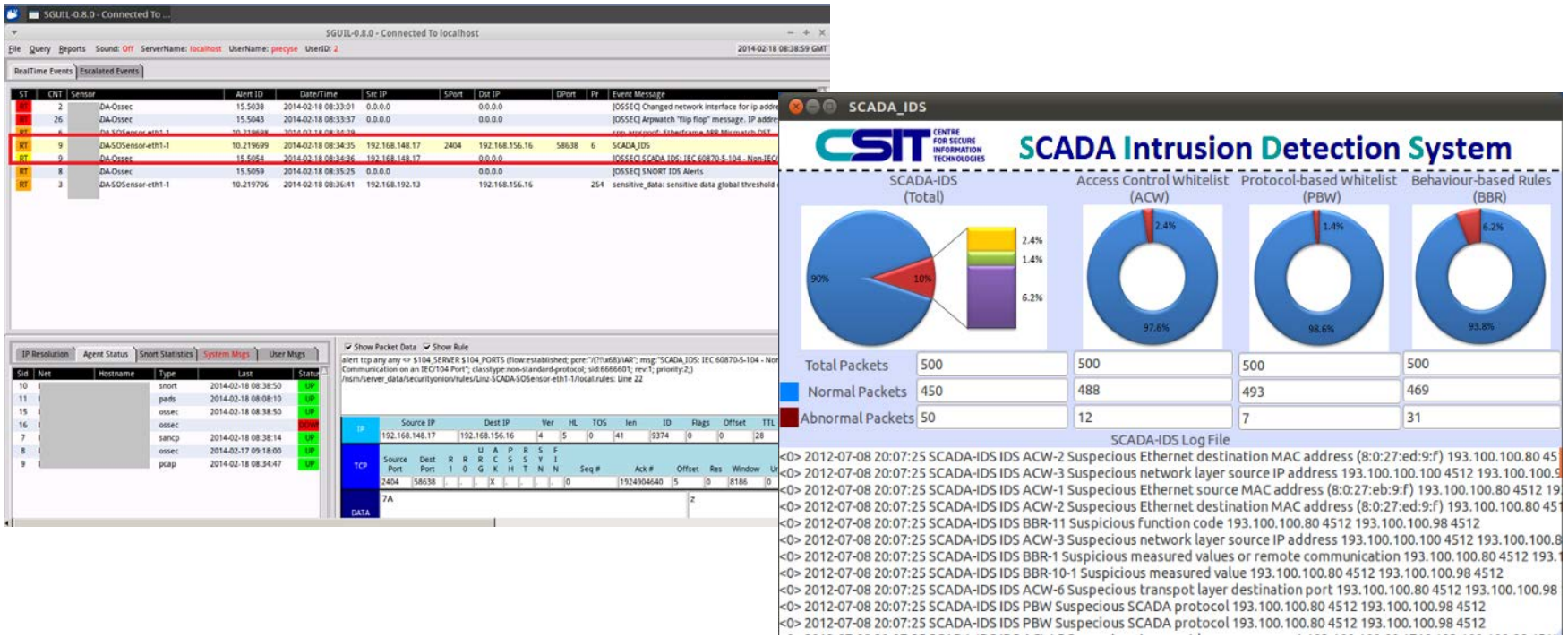
- Cross-field data correlation

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

- 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




(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

# SPARKS Mini-Project

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- 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


EU FP7 Programme Contract No. 608224

# SPARKS Mini-Project

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

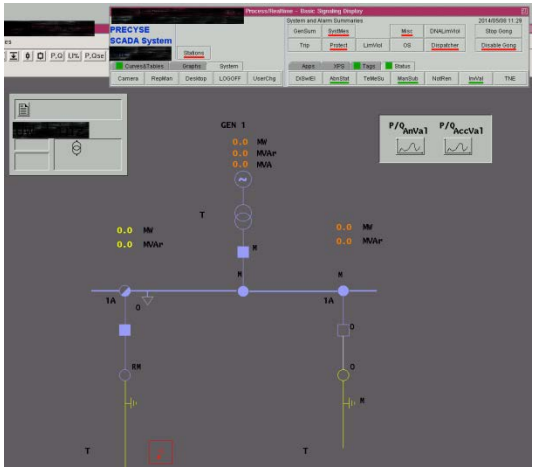
- Development of a multi-attribute SCADA-IDS
  - Identify permitted and non-permitted devices, connections, and protocols
  - Enhanced payload inspection to detect permitted and non-permitted operations and behaviours
  - Whitelist, stateful and behavioural analysis based on 61850 features and SmartEST demo physical system attributes

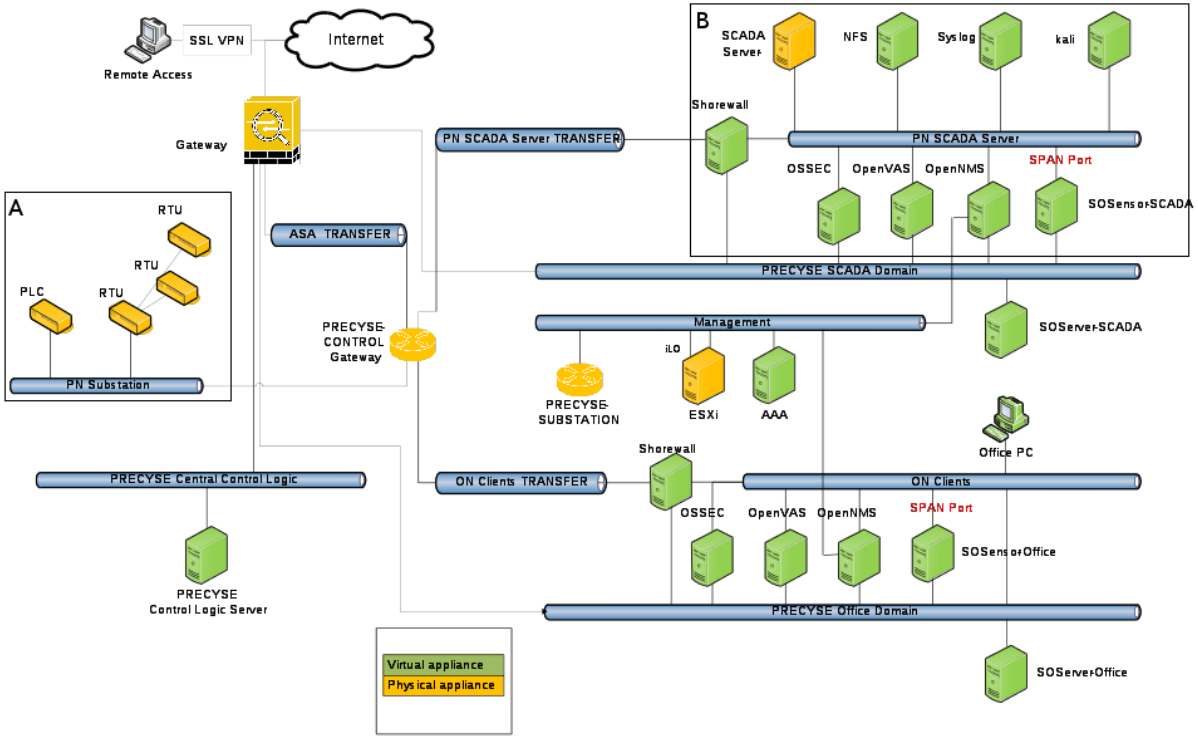
# Attack Demonstrations

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

Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE







EU FP7 Programme Contract No. 608224

# 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?


EU FP7 Programme Contract No. 608224