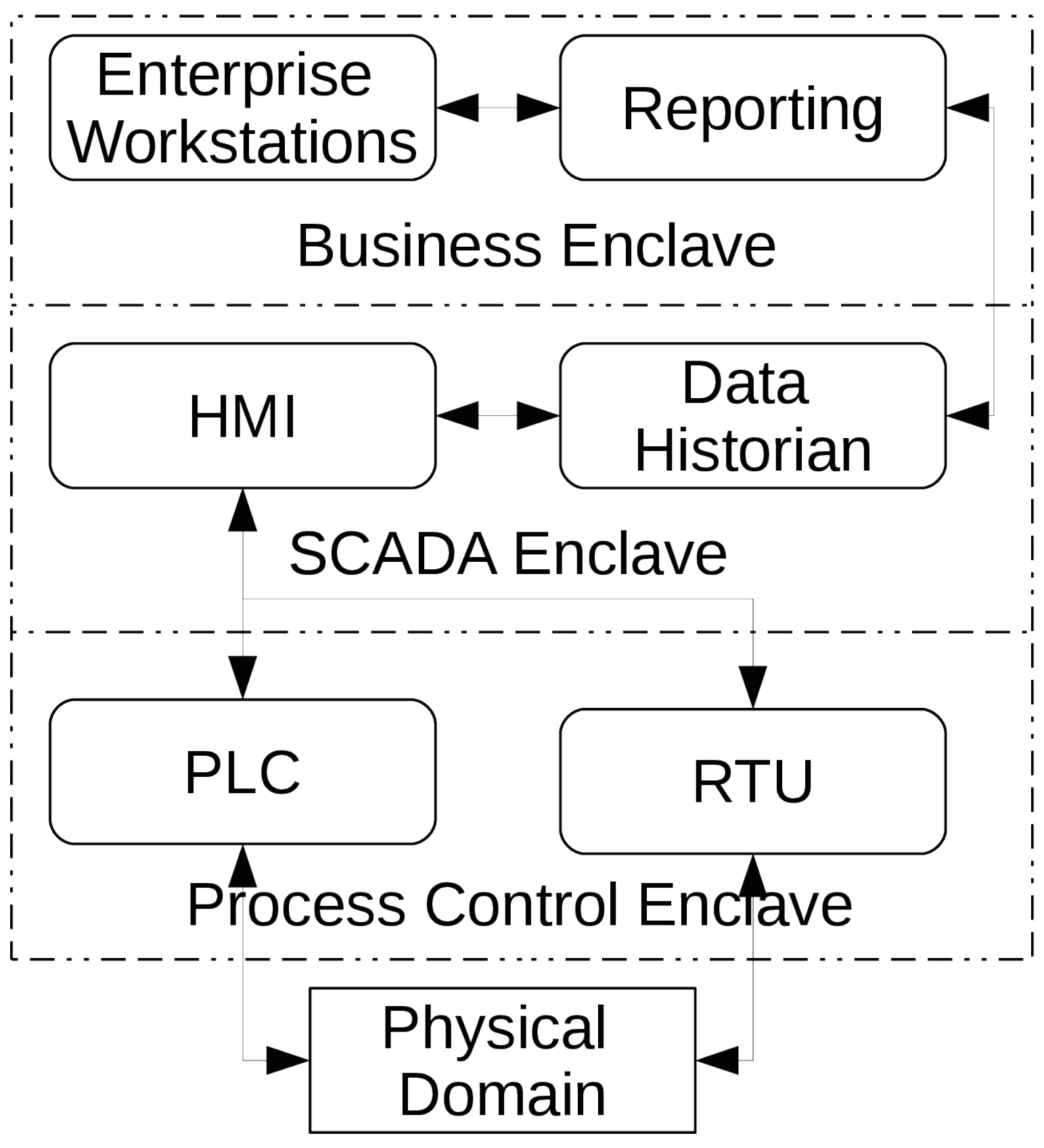
Using Application Layer Metrics to Detect Advanced SCADA Attacks

Peter Maynard, Kieran McLaughlin, Sakir Sezer

Queen's University Belfast

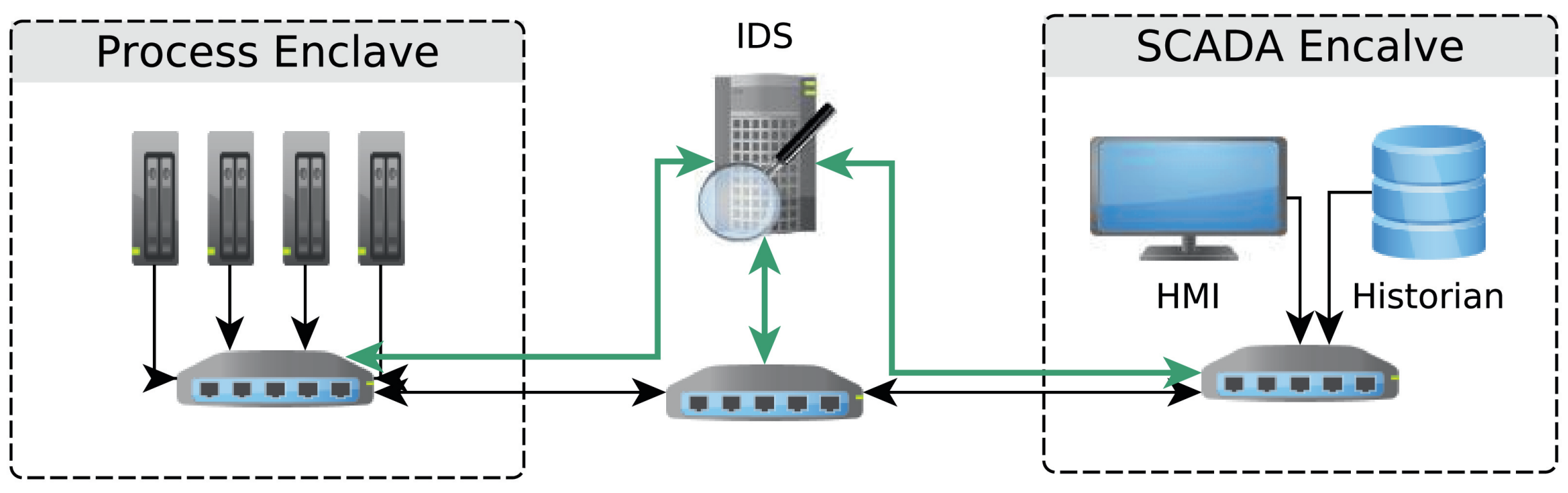
Industrial Control Systems



- Network Separation
  - **Business** - Microsoft Windows, Email, Office
  - **SCADA** - Specialised control and monitoring
  - **Process Control** - Specialised propitiatory hardware and software
- ICS hardware and software have a long life cycle
- Vendors restrict changes once deployed
- Each industrial site is complex and unique
- Critical networks are segmented into enclaves
- Commercial off-the-shelf equipment more frequent

Network Intrusion Detection Systems

- Unable to deploy host based agents
- Active scanning may cause issued within an ICS enclave
- Five-Tuple features (protocol, IP src/dst and port src/dst) are unable to detect advanced attacks



Application Layer Metrics

- Monitoring protocol fields provides superior insight over 5-Tuple data into network events
- A passive operation that introduces no additional latency
- Able to detect subtle changes and covert events

Metric 0 - Generic Protocol

- Active Network Scanning
- TCP/UDP Spam
- Firmware Tampering

Metric 1 - Firmware Update

- Firmware Tampering
- Malicious Firmware

Metric 7 - Response Type

- Device/Protocol Scan
- Report Server Information
- Command Replay/Injection
- Remote Clear Registers
- Remote Restart
- Stealthy Deception Attack

Metric 12 - Avg. Information Objects

- Read Device Identification
- Covert Communication

Metric 4 - Accepted Command

- Unauthorised Write
- Unauthorised Read
- Remote Restart
- Stealthy Deception Attack

Metric 5 - Rejected Command

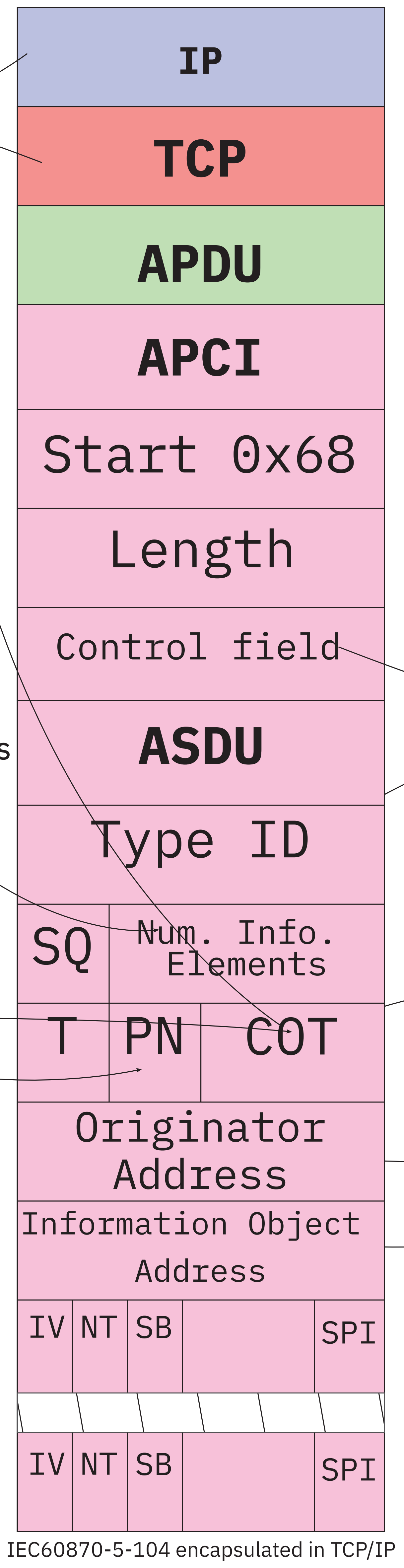
- Command Replay
- Command Injection
- Malicious Firmware

Metric 2 - Set Value

- Unauthorised Write
- Stealthy Deception Attack

Metric 3 - Get Value

- Device/Protocol Scan
- Report Server Information
- Unauthorised Read
- Stealthy Deception Attack



IEC60870-5-104 encapsulated in TCP/IP

Metric Mapping

- Proposed metrics are mapped to the IEC60870-5-104 field bus protocol
- Most deploy non-encrypted plain text protocols, perfect for passive analysis
- Each field of the protocol can be measured and used to detect abnormal activities on the network

Metric 6 - Command Type

- Device/Protocol Scan
- Report Server Information
- Remotely Clear Registers
- Remote Restart

Metric 11 - Cause of Transmission

- Covert Communication
- Malicious Firmware
- Firmware Tampering

Metric 8,9,10 - Addressing

- Rouge Device
- Covert Communications
- Malicious Firmware

Threat Actors

- **Individual**
  - On-site employee; remote contractor; partner
  - Low threat level; Depending on persons skills
- **Group**
  - Ad-hock (Recreational) or established (Hacktivist)
  - Moderate threat level; Low technical skills
- **Organisation**
  - Industrial competitors; Suppliers; Customers
  - Moderate threat level; High technical skills
- **Nation-State**
  - State actors; Covert and targeted attacks
  - High threat level; High technical skills

Attack Stages	Individual	Group	Organisation	Nation-State
	Reconnaissance			
Network Scan	•	•	•	•
Device/Protocol Scan	-	•	•	•
Report Server Information	-	-	•	•
Read Device Identif cation	-	-	•	•
	Interference			
Command Replay	-	•	•	•
Command Injection	-	•	•	•
Unauthorised Write	-	-	•	•
Unauthorised Read	-	•	•	•
Clear Counter/Diagnostic Registers	-	•	•	•
Rouge Device	-	-	•	•
Firmware Tampering	-	-	•	•
	Denial of Service			
TCP/UDP Spam	•	•	•	•
Remote Restart	-	-	•	•
Force PLC into Listen Mode	-	-	•	•
	Covert			
Covert Comms.	-	-	-	•
Stealthy Deception Attack	-	-	-	•
Malicious Firmware	-	-	•	•

Contributions

- An analysis of industrial threat actors and their capabilities
- A Review of the current state-of-the-art metrics for ICS
- Proposed novel metrics that enable deeper insight into the Process Control Network

EPSRC
Engineering and Physical Sciences Research Council
Project ADAMA reference EP/N022866/1.

Peter Maynard	p.maynard@qub.ac.uk
Kieran McLaughlin	kieran.mclaughlin@qub.ac.uk
Sakir Sezer	s.sezer@qub.ac.uk

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ESTD 1845