Man in the middle attacks on IEC 60870-5-104

Pete Maynard

@pgmaynard
ORCID 0000-0002-6267-7530

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Introduction

- Pete Maynard
- PhD Student
- CSIT Queen's University Belfast, UK
- Industrial Control System Security
- Partnership with PRECYSE

What I do

- Attacks on SCADA protocols
  - Replay, MITM, DoS
- Develop detection and prevention methods
- Anomaly detection via machine learning

PRECYSE

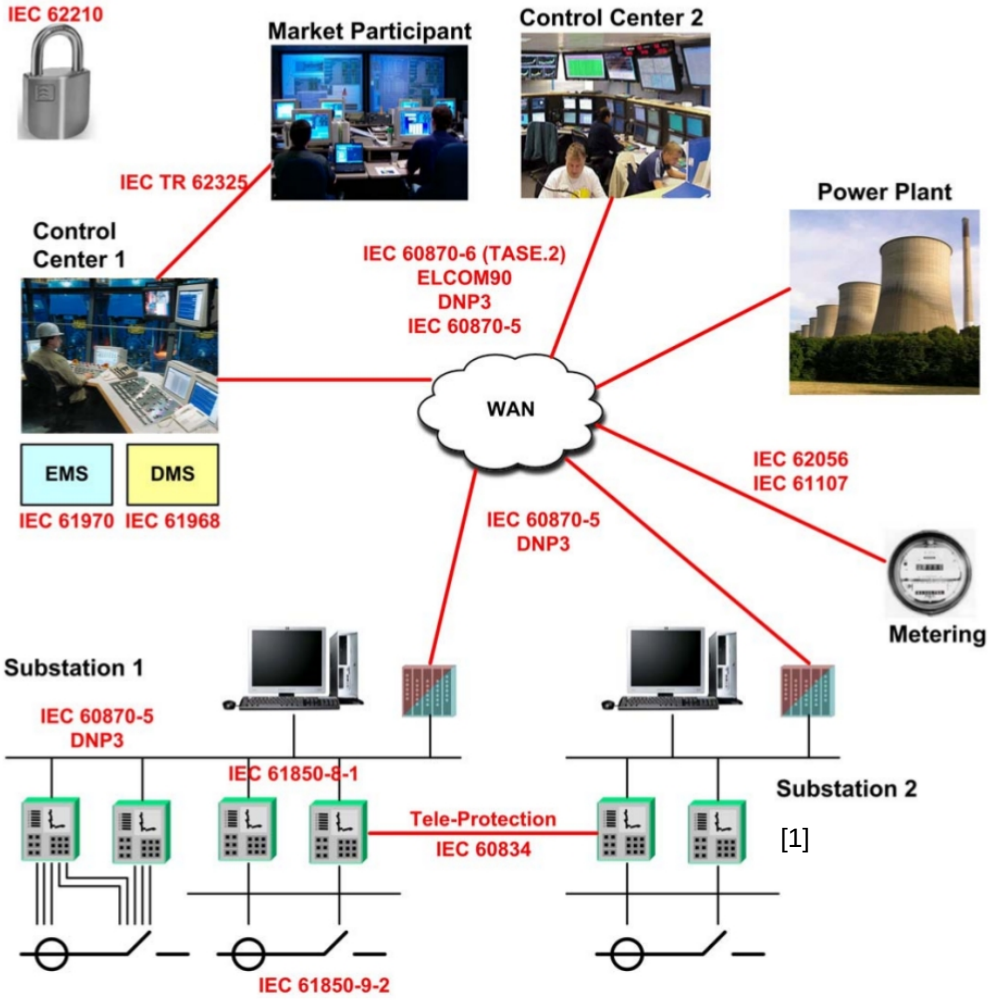
- European FP7 Project
- Prevention, protection and REaction to CYber attackS to critical infrastructurEs
- LINZ STROM GmbH (Electrical Distribution Operator)

Talk Overview

- What's SCADA Used for
- SCADA Threats
- Introduction IEC 104
- Attacking IEC 104

What's SCADA Used for?

How is SCADA used

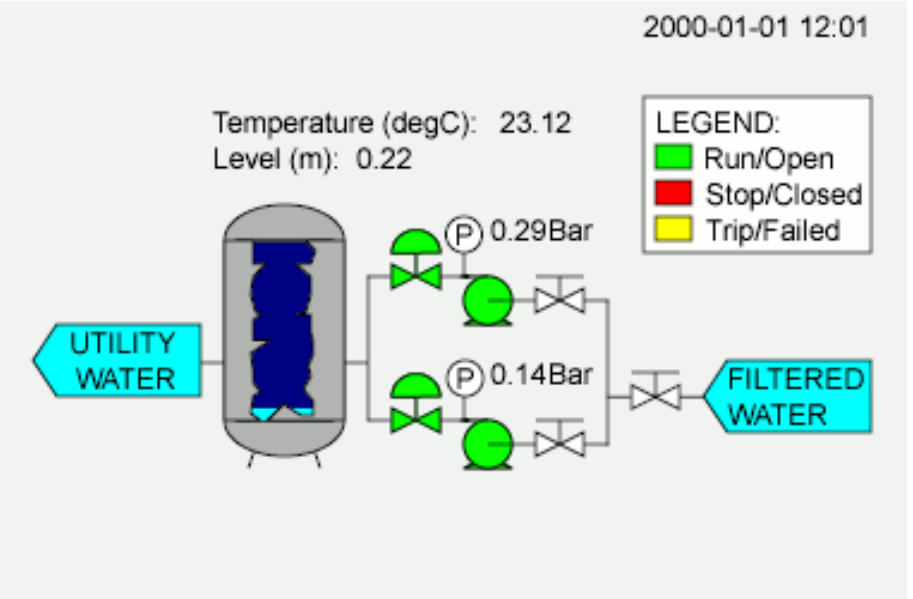


- MODBUS, DNP3, IEC104, 61850, Profibus …

[1] S. Mohagheghi, J. Stoupis, and Z. Wang. Communication protocols and networks for power systems-current status and future trends. In Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES, pages 1–9, March 2009.

What does it do?

- Telemetry control
- Change Settings
- Read/Write/Delete files and directories
- Update firmware



SCADA Threats

Attack Levels

Level	Example
1 Accident	Misconfigured, Firmware Update
2 Novice	Script kiddie, port scanning
3 Experienced	Replay attack, basic knowledge
4 Advanced	Stuxnet, ICS domain knowledge

Threats

- Havex Malware
- OPC to scan for SCADA devices
- Reports back to command and control server
- Recently detected July 2014
  - European ICS
  - Team Since 2011
- State sponsored?

Scanning for SCADA devices

- Readily available scanners
  - SCADA StrangeLove[1]
- Simple Python Script
- Return Device name, IP, software version

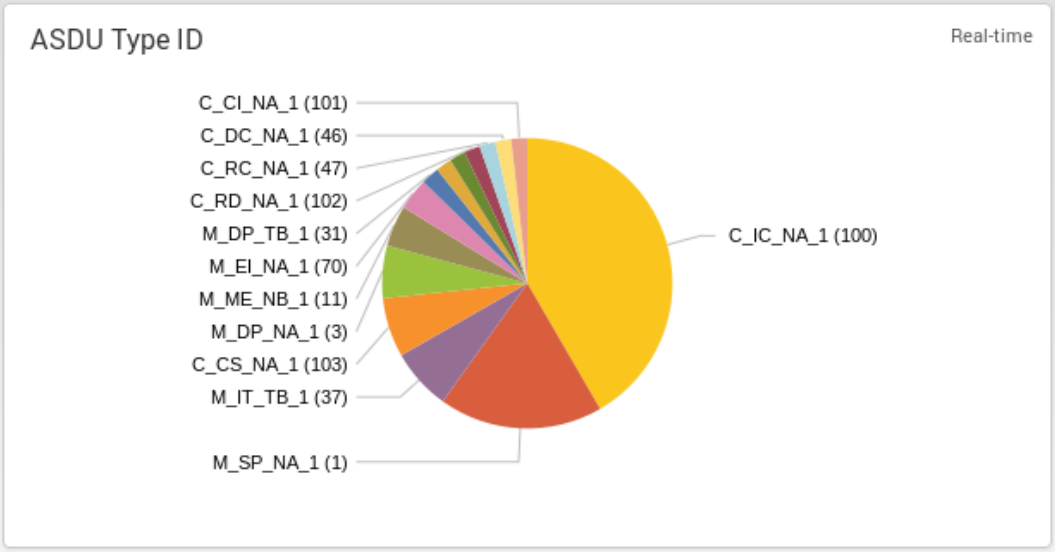
[1] https://github.com/atimorin/scada-tools

SCADA Fuzzers

- Protocol Fuzzers
- Project Robus[1]
  - DNP3
  - Identified many vulnerabilities
- Fuzzing can kill

[1] http://www.automatak.com/robus/

Protocol Analysers




```
50876   0.000012    192.168.148.16      192.168.156.16      TCP         60 50876 > iec-104 [ACK] Seq=23 Ack=23 Win=1136 Len=0
                                        2.168.156.16        104asdu     70 13,145->1 C_IC_NA_1 ActCon IOA=0
                                        2.168.156.16        TCP         60 50876 > iec-104 [ACK] Seq=23 Ack=39 Win=1136 Len=0
                                        2.168.156.16        104apci     60 <-S(2)
                                        2.168.156.16        104asdu     79 13,145->1 M_SP_NA_1 Inrogen IOA=10010-10019 (10)
                                        2.168.156.16        TCP         60 50876 > iec-104 [ACK] Seq=29 Ack=64 Win=1136 Len=0
                                        2.168.156.16        104asdu     70 13,145->1 M_DP_NA_1 Inrogen IOA=15000
                                        2.168.156.16        TCP         60 50876 > iec-104 [ACK] Seq=29 Ack=80 Win=1136 Len=0
                                        2.168.156.16        104apci     60 <-S(4)
                                        2.168.156.16        104asdu     70 13,145->1 C_IC_NA_1 ActTerm IOA=0
                                        2.168.156.16        TCP         60 50876 > spearway [ACK] Seq=1 Ack=1 Win=568 Len=6
                                        2.168.156.16        104asdu    448 13,145->0 M_ME_NB_1 Spont IOA=39999 [Malformed Packet]
                                        2.168.156.16        TCP         60 50876 > iec-104 [ACK] Seq=35 Ack=114 Win=1136 Len=0
 bytes captured (560 bits)
:ab:01:10:f8), Dst: Motorola_40:5d:8c (00:1c:11:40:5d:8c)
.148.16 (192.168.148.16), Dst: 192.168.156.16 (192.168.156.16)
50876 (50876), Dst Port: iec-104 (2404), Seq: 7, Ack: 7, Len: 16
```

```
IEC 60870-5-104-Asdu: 13,145<-1 C_IC_NA_1 Deact_TEST   IOA=0 'interrogation command'
    TypeId: C_IC_NA_1 (100)
    .000 0001 = NumIx: 1
    ..00 1000 = CauseTx: Deact (8)
    .0.. .... = Negative: False
    1... .... = Test: True
    OA: 1
    Addr: 37133
    IOA: 0
```

```
0010  00 38 76 24 40 00 40 06  13 2a c0 a8 94 10 c0 a8   .8v$@.@. .*......
0020  9c 10 c6 bc 09 64 67 5c  a3 07 05 59 67 b9 50 18   .....dg\ ...Yg.P.
0030  02 38 52 c5 00 00 68 0e  00 00 00 00 64 01 88 01   .8R...h. ....d...
0040  0d 91 00 00 00 14                                  ......
```

Negative (104asdu.nega), 1 byte | Packets: 430 Displayed: 430 Marked: 0 Load time: 0:00.004 | Profile: Default

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Introduction IEC 104

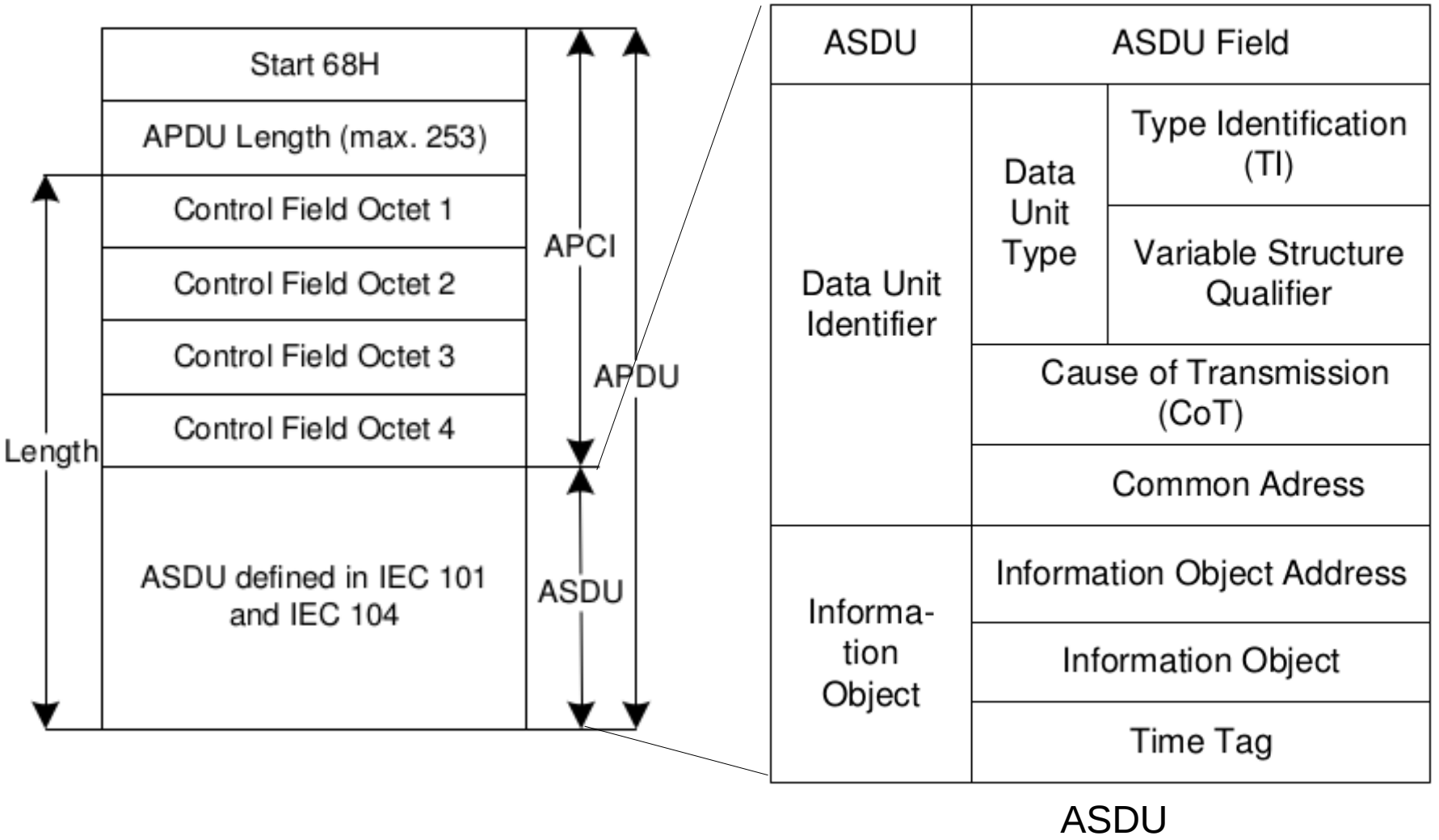
Introduction IEC 60870-5-104

- International Electrotechnical Commission (IEC)
- IEC 60870 developed periodically between the years 1988 and 2000
- 6 Main Parts and four companion sections
- Open Standard
- 60870-5-104 defines transmission over TCP/IP

IEC 60870-5-104 Security Issues

- Ported from serial links to TCP/IP
- No authentication
- No encryption
- Uses IP address white-list
  - Defined on the slave
- TLS encryption recommended
  - In practice **not** implemented

104 Payload



ASDU

Attacking IEC 104

Capturing Packets

- SPAN Port
- DNS Poisoning
- Content Addressable Memory (CAM) table overflow
- ARP Spoofing

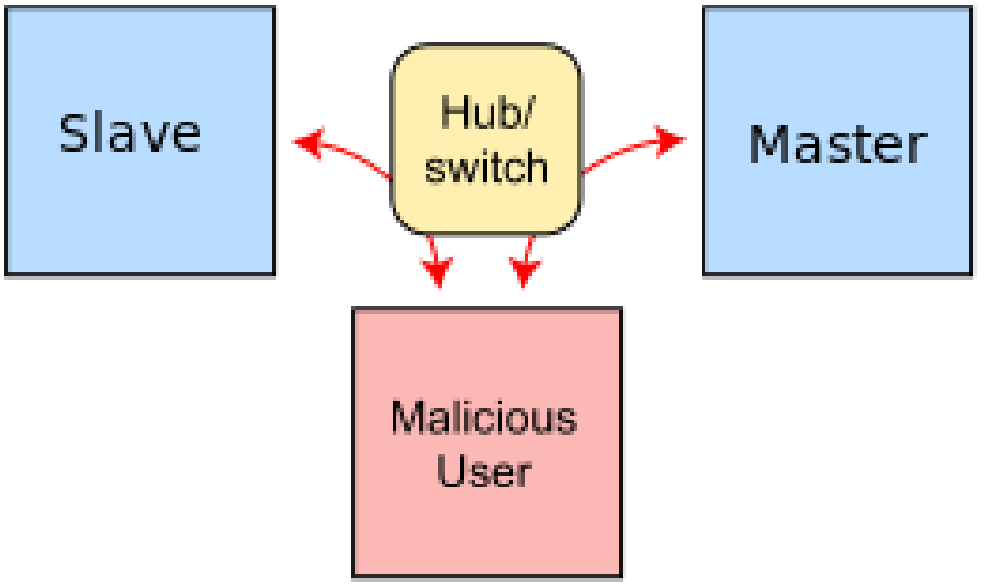
Replay Attack

- Novice level attack
- Capture and replay packets
  - Command, readings, alerts...
- Replayed packets dropped by kernel
- Tcpreplay alternatives to modify SEQ values

79 9.387334	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 iec-104 > 50876 [SYN, ACK] Seq=0 Ack=0 Win=765 L
80 9.387336	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 <ERR 6 bytes>
81 9.387338	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
82 9.387345	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
83 9.387349	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
84 9.387351	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
85 9.387354	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
86 9.387357	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
87 9.387360	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
88 9.387362	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
89 9.387365	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
90 9.387367	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
91 9.387371	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
92 9.387374	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
93 9.387378	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
94 9.387380	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 iec-104 > 50876 [ACK] Seq=1 Ack=6 Win=759 Len=0
95 9.387381	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 [TCP Dup ACK 94#1] iec-104 > 50876 [ACK] Seq=1 A
96 9.387384	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 [TCP Dup ACK 94#2] iec-104 > 50876 [ACK] Seq=1 A
97 10.682047	10.50.50.105	10.50.50.255	blackja	sentine	UDP	82 Source port: blackjack Destination port: sentir
98 10.682075	10.50.50.105	10.50.50.255	blackja	sentine	UDP	82 Source port: blackjack Destination port: sentir

Man In the Middle Attack

- Intercept communications between two or more devices
- Modify and inject packets
- Many tools available
  - ettercap
  - cain and abel
  - DSniff



104 MITM Lab Experiment

- Modify Cause of transmission (CoT) field
- Intercept and set an invalid CoT value
- Detection with SNORT

Cause of Transmission

```
▽ IEC 60870-5-104-Apci: ->I(1,1)
    ApduLen: 14
    .... ..00 = ApciType: I (0x00)
▽ IEC 60870-5-104-Asdu: 13,145->1 C_IC_NA_1 ActCon IOA=0 'interrogation command'
    TypeId: C_IC_NA_1 (100)
    .000 0001 = NumIx: 1
    ..00 0111 = CauseTx: ActCon (7)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 1
    Addr: 37133
    IOA: 0
```

```
0000  00 e0 ab 01 10 f8 00 1c  11 40 5d 8c 08 00 45 00   ........ .@]...E.
0010  00 38 00 09 00 00 3b 06  ce 45 c0 a8 94 10 c0 a8   .8....;. .E......
0020  9c 10 09 64 c6 bc 05 59  67 c9 67 5c a3 17 50 10   ...d...Y g.g\..P.
0030  02 fd ce e8 00 00 68 0e  02 00 02 00 64 01 07 01   ......h. ....d...
0040  0d 91 00 00 00 14                                 ......
```

- CoT values can use the following number ranges:
  - 1-13 and 20-41
  - 14-19 and 42-43 are reserved for future use.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Before and After Capture

```
Internet Protocol Version 4, Src: 10.50.50.105 (10.50.50.105), Dst: 10.50.50.75 (10.50.50.75)
Transmission Control Protocol, Src Port: iec-104 (2404), Dst Port: 55561 (55561), Seq: 1, Ack: 1, Len: 23
IEC 60870-5-104-Apci: ->I(3,1)
   ApduLen: 21
   .... ..00 = ApciType: I (0x00)
IEC 60870-5-104-Asdu: 0,0->0 M_SP_TB_1 Spont IOA=0 'single-point information with time tag CP56Time2a'
   TypeId: M_SP_TB_1 (30)
   .000 0001 = NumIx: 1
   ..00 0011 = CauseTx: Spont (3)
   .0.. .... = Negative: False
   0... .... = Test: False
   OA: 0
   Addr: 0
   IOA: 0
   IEC 60870-5-104-Asdu: Value
```

```
030  ff d7 76 ba 00 00 01 01  08 0a 00 00 6a 26 0e 2b   ..v
040  d8 2f 68 15 06 00 02 00  1e 01 03 00 00 00 00 00   ./h
050  00 01 26 5a 1c 0e 09 09  0e                        ..&
```

Before

```
Internet Protocol Version 4, Src: 10.50.50.105 (10.50.50.105), Dst: 10.50.50.75 (10.50.5
Transmission Control Protocol, Src Port: iec-104 (2404), Dst Port: 55561 (55561), Seq: 1
IEC 60870-5-104-Apci: ->I(3,1)
   ApduLen: 21
   .... ..00 = ApciType: I (0x00)
IEC 60870-5-104-Asdu: 0,0->0 M_SP_TB_1  <CauseTx=42> IOA=0 'single-point information wit
   TypeId: M_SP_TB_1 (30)
   .000 0001 = NumIx: 1
   ..10 1010 = CauseTx: Unknown (42)
   .0.. .... = Negative: False
   0... .... = Test: False
   OA: 0
   Addr: 0
   IOA: 0
   IEC 60870-5-104-Asdu: Value
      IOA: 0
      Value: ON - Status: Not blocked, Not Substituted, Topical, Valid
      14-09-09 (0) 14:28:23.078 (Valid)
```

```
020  32 4b 09 64 d9 09 f5 93  82 00 83 e3 6e 04 50 10   2K.d.... ....n.P.
030  7f ff 59 33 00 00 68 15  06 00 02 00 1e 01 2a 00   ..Y3..h. ......*.
040  00 00 00 00 00 01 26 5a  1c 0e 09 09 0e            ......&Z .....
```

After

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SNORT Alert

Rule

```
alert tcp $104_CLIENT any -> $104_SERVER $104_PORTS (flow: established; content:"|68|"; offset:0; depth:1; pcre:"/[\S\s]{5}(\x2D|\x2E|\x2F|\x30|\x64|\x65)/iAR"; content:!"|06|"; offset: 8; depth: 1; msg:"17: SCADA_IDS: IEC 60870-5-104 – Suspicious Value of Transmission Cause Field"; classtype:bad-unknown; sid:6666617; rev:1; priority:2;)
```

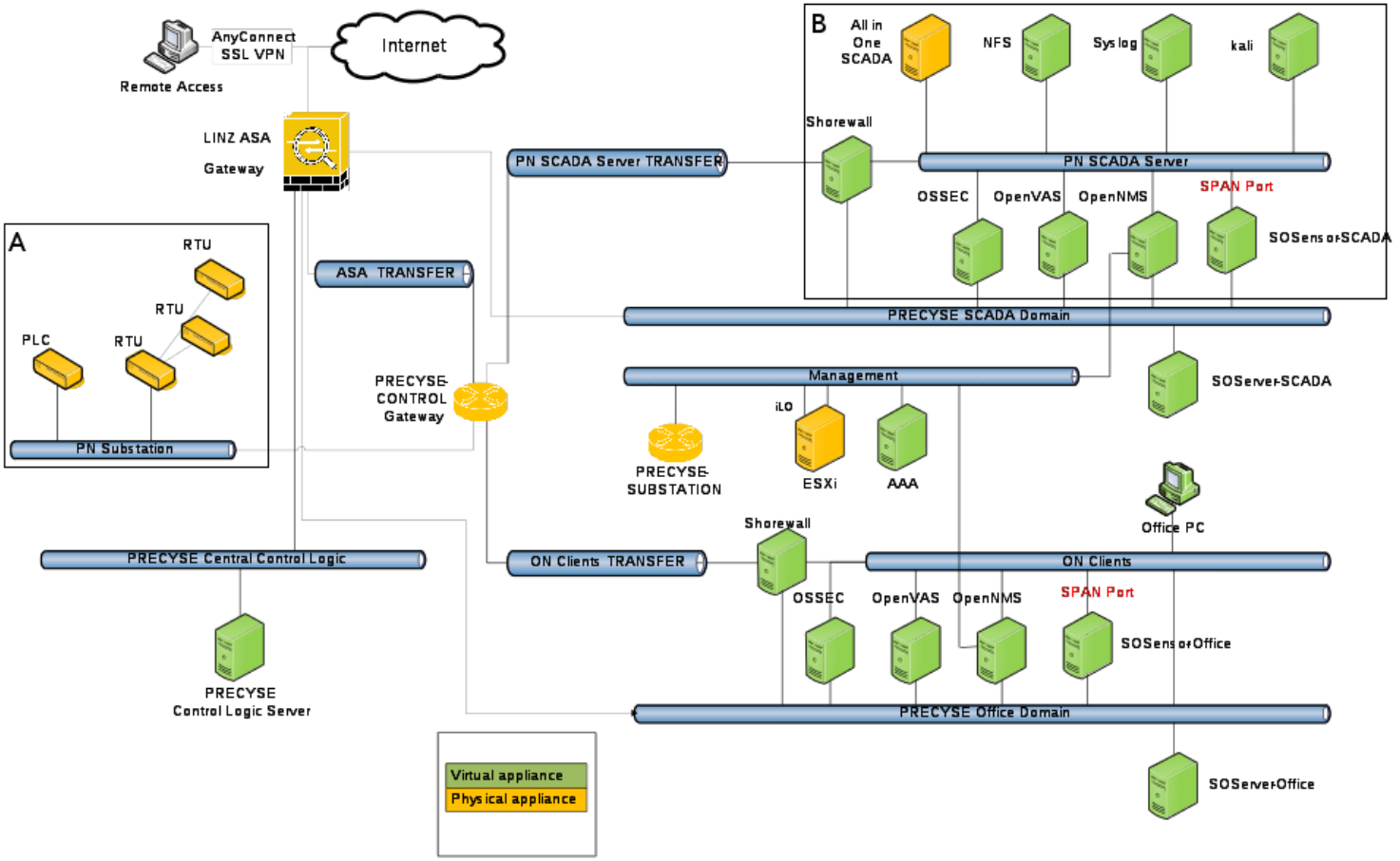
Alert

[**] [1:6666617:1] 17: SCADA_IDS: IEC 60870-5-104 – **Suspicious Value of Transmission Cause Field** [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
09/09-14:06:10.462288 10.50.50.105:40734 -> 10.50.50.75:22
TCP TTL:64 TOS:0x0 ID:60033 IpLen:20 DgmLen:60 DF
******S* Seq: 0x9A0C38A1 Ack: 0x0 Win: 0x3908 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1382076960 0 NOP WS: 7

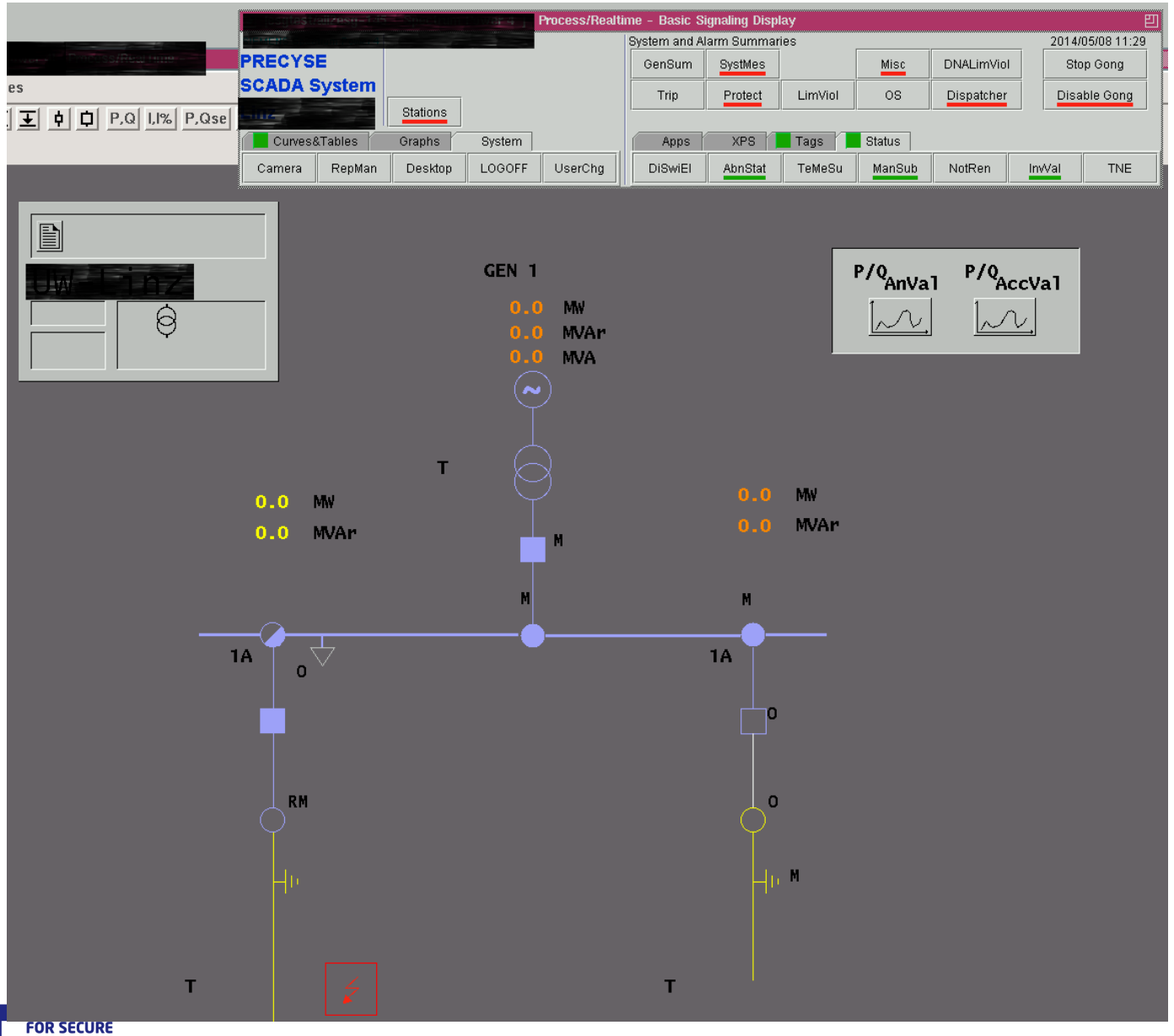
Earth Fault

- Real world situation where an earth fault in the physical electrical grid occurs

Linz Test-bed

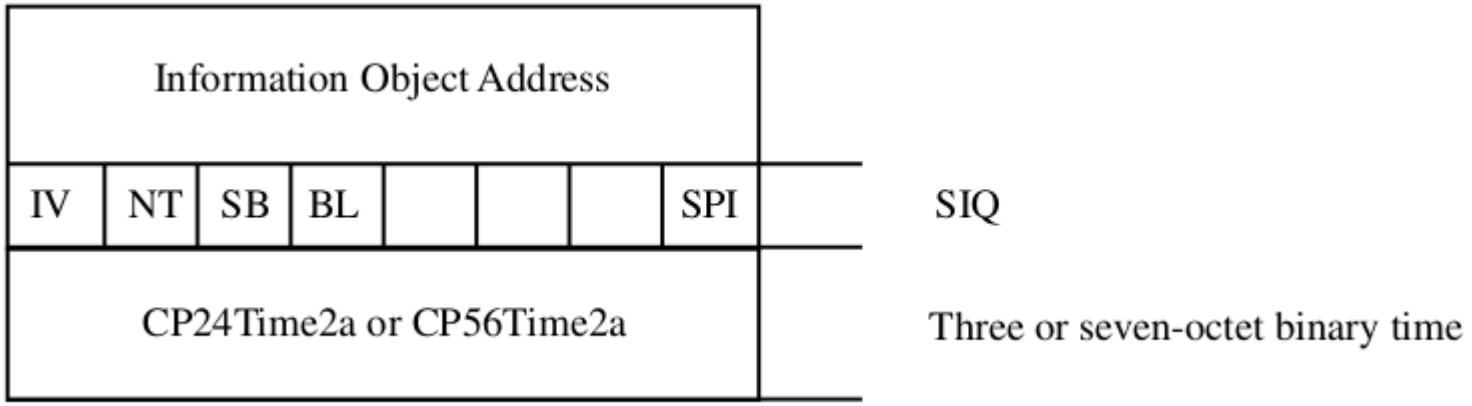


Operator View



104 MIM TestBed Environment

- Intercept value, so operators unable to view fault
- 104's Information Objects, M_SP_TB_1 stores the 'ON/OFF' value
- First bit of the SIQ is the SPI field, storing the ON/OFF value.



ON/OFF Value Modification

```
▷ Internet Protocol Version 4, Src: 10.50.50.105 (10.50.50.105), Dst: 10.50.50.75 (10.50.50.75)
▷ Transmission Control Protocol, Src Port: iec-104 (2404), Dst Port: 55561 (55561), Seq: 168, Ack: 25, Len: 23
▽ IEC 60870-5-104-Apci: ->I(11,1)
    ApduLen: 21
    .... ..00 = ApciType: I (0x00)
▽ IEC 60870-5-104-Asdu: 0,0->0 M_SP_TB_1 Spont IOA=0 'single-point information with time tag CP56Time2a'
    TypeId: M_SP_TB_1 (30)
    .000 0001 = NumIx: 1
    ..00 0011 = CauseTx: Spont (3)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 0
    IOA: 0
  ▽ IEC 60870-5-104-Asdu: Value
      IOA: 0
      Value: ON - Status: Not blocked, Not Substituted, To
      14-09-09 (0) 14:31:40.948 (Valid)
```

```
0030  ff b3 43 ab 00 00 01 01  08 0a 00 00 71 e0 0e 2d   ..
0040  21 79 68 15 16 00 02 00  1e 01 03 00 00 00 00 00   !y
0050  00 01 f4 9f 1f 0e 09 09  0e                        .
```

Before

```
▷ Internet Protocol Version 4, Src: 10.50.50.105 (10.50.50.105), Dst: 10.50.50.75 (10.50.50
▷ Transmission Control Protocol, Src Port: iec-104 (2404), Dst Port: 55561 (55561), Seq: 16
▽ IEC 60870-5-104-Apci: ->I(11,1)
    ApduLen: 21
    .... ..00 = ApciType: I (0x00)
▽ IEC 60870-5-104-Asdu: 0,0->0 M_SP_TB_1 Spont IOA=0 'single-point information with time ta
    TypeId: M_SP_TB_1 (30)
    .000 0001 = NumIx: 1
    ..00 0011 = CauseTx: Spont (3)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 0
    IOA: 0
  ▽ IEC 60870-5-104-Asdu: Value
      IOA: 0
      Value: OFF - Status: Not blocked, Not Substituted, Topical, Valid
      14-09-09 (0) 14:31:40.948 (Valid)
```

```
0020  32 4b 09 64 d9 09 f5 93  82 c4 83 e3 6e 28 50 10   2K.d.... ....n(P.
0030  7f ff 9e 06 00 00 68 15  16 00 02 00 1e 01 03 00   ......h. ........
0040  00 00 00 00 00 00 f4 9f  1f 0e 09 09 0e            ........ .....
```

After

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Conclusion

- Attackers with varying skill levels can compromise SCADA systems
  - Man-In-The-Middle attacks hiding an earth fault
- New implementations of ICS need to take precautions
- Monitor logs, network, everything
- Enable attack mitigations

Future Work

- Identify features of the IEC104 protocol for anomaly detection
- Propose to develop an Anomaly Detection module for the IEC104 protocol
  - Detect similar network attacks
- Work on MITM attack for IEC 61850

Questions