

# Common Flaws in Public and Private ICS Network Protocols

歷史共業 - 公開與私有工控通訊協定的共同缺陷

Mars Cheng

Selmon Yang

@marscheng\_

May 4, 2021

@CYBERSEC 2021



# Who are we?

A joint venture company of

**Trend Micro Inc.** and **Moxa Inc.**

30 years+ Cybersecurity Threat Intelligence

30 years+ OT Network Expertise



Industry  
Adaptive  
Solution

Threat  
Defense  
Expertise

OT-Focused  
Technology

## Keep the Operation Running



# Who are we?



**Mars Cheng**

**Threat Researcher at TXOne Networks**

- Spoke at Black Hat, HITB, HITCON, SecTor, ICS Cyber Security Conference, InfoSec Taiwan and etc.
- Instructor of Ministry of National Defense, Ministry of Education, Ministry of Economic Affairs and etc.
- General Coordinator of HITCON 2021
- Vice General Coordinator of HITCON 2020



**Selmon Yang**

**Staff Engineer at TXOne Networks**

- IT/SCADA Protocol Parsing
- Linux Kernel Programming
- Honeypot Deployment & Optimization

# Outline

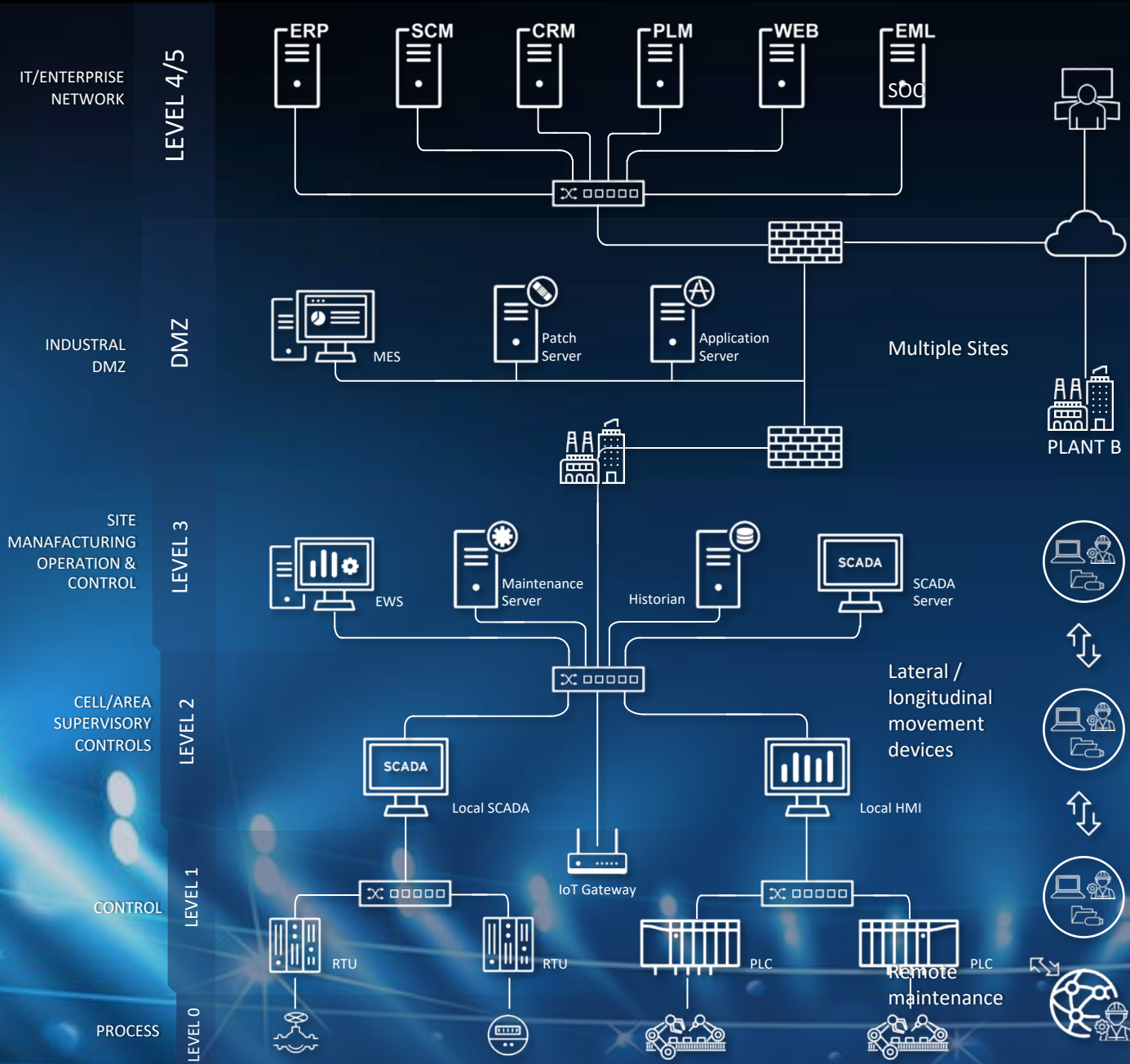
- ICS Architecture and Attack Vectors
- Public and Private: ICS Protocols
- Common Flaws in ICS Protocols
- How to Work Against ICS Network Protocol Attacks



# ICS Architecture and Attack Vectors



PURDUE REFERENCE ARCHITECTURE

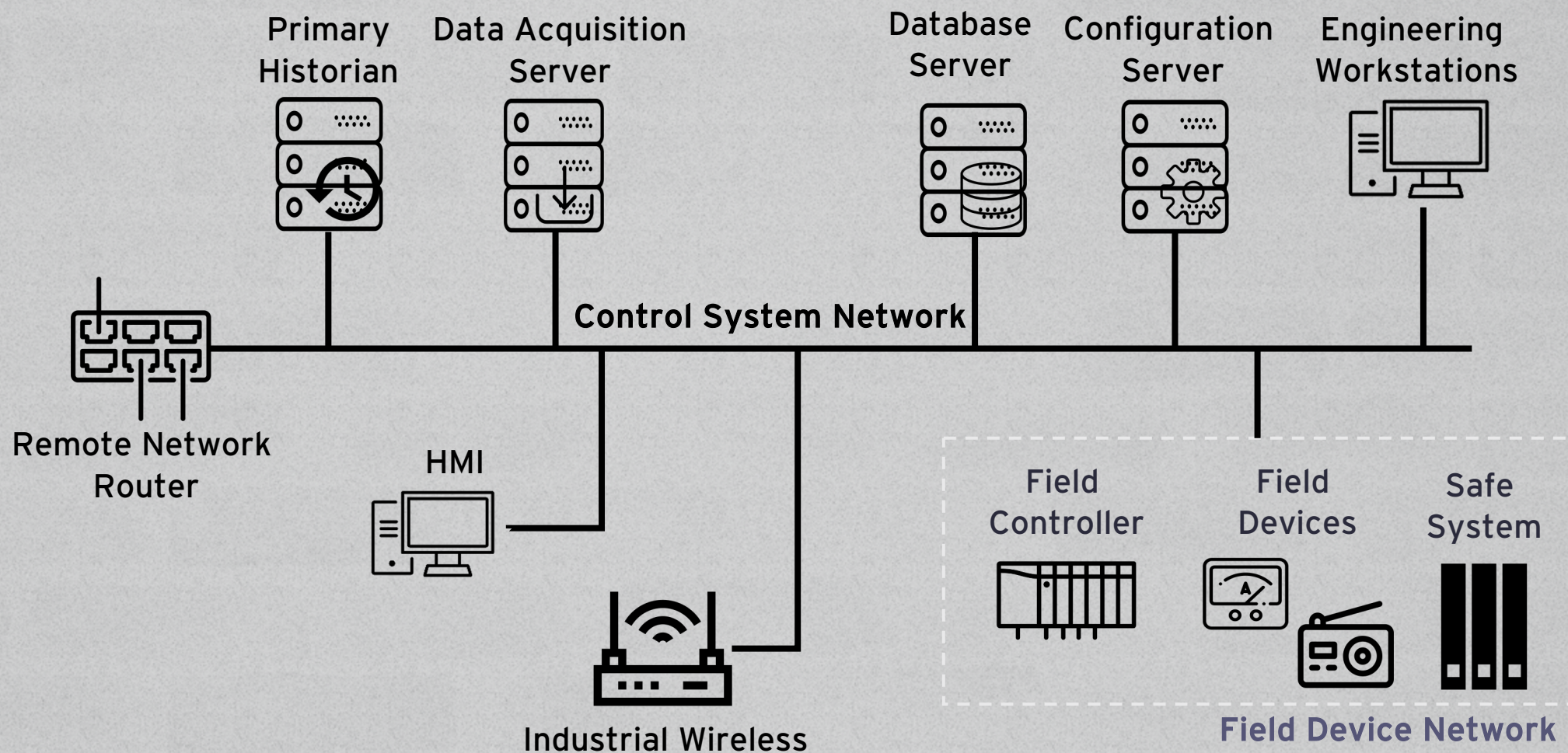


## Information Technology (IT)

## Operational Technology (OT)

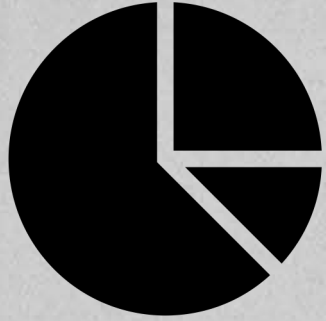


# Common ICS Architecture

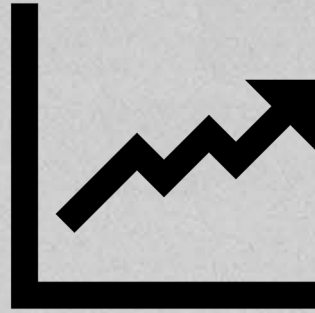




# ICS/SCADA Security Threat Situation



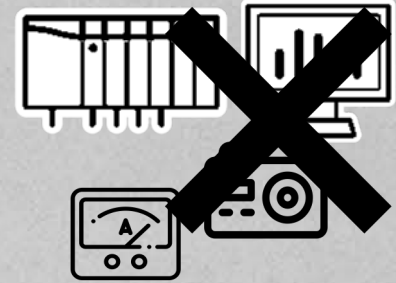
Vulnerabilities are mostly critical and high risk levels



The number of vulnerability is rising year by year



The security incidents have a huge impact



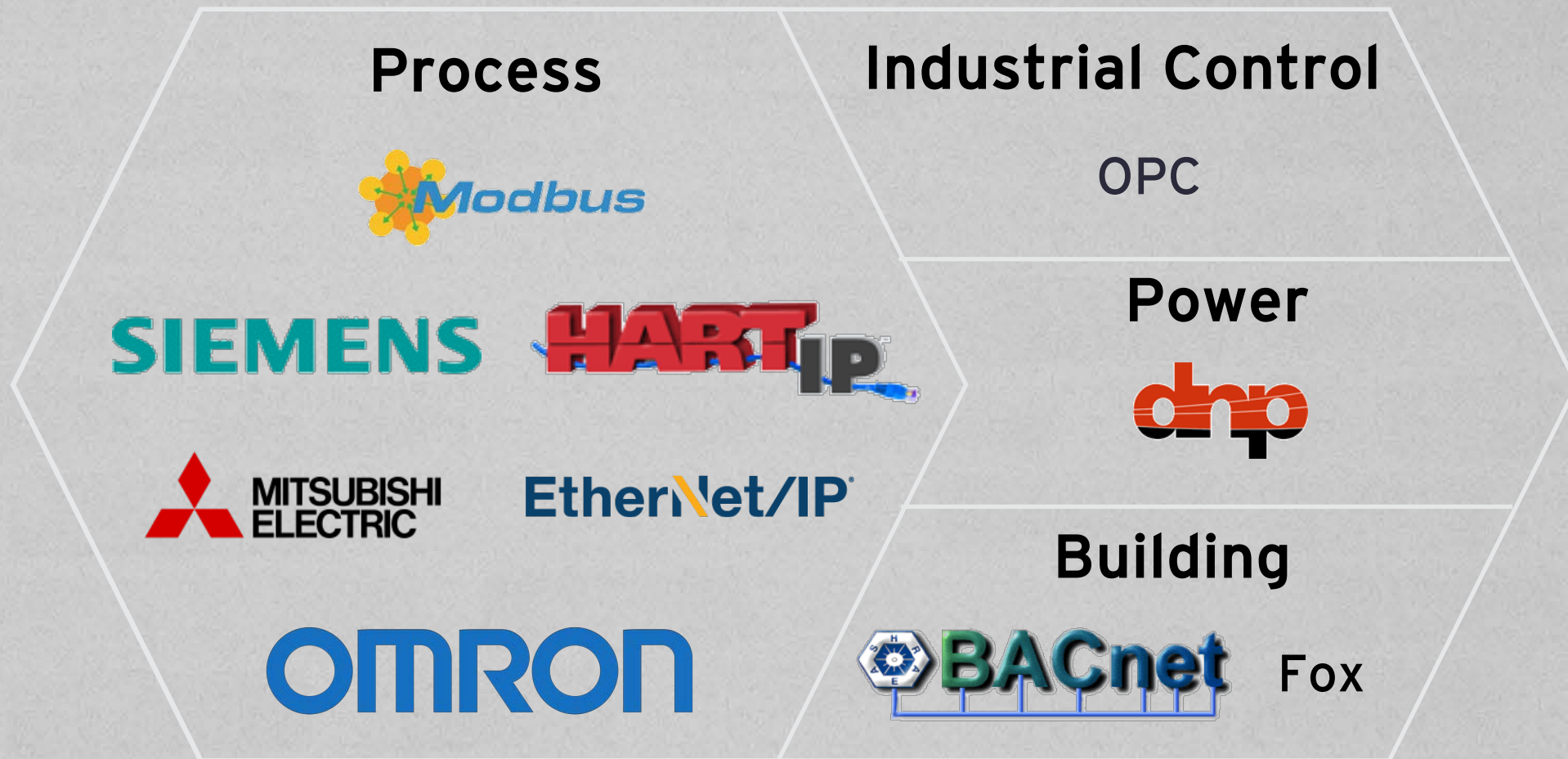
ICS/SCADA are not secure at all

**Critical**



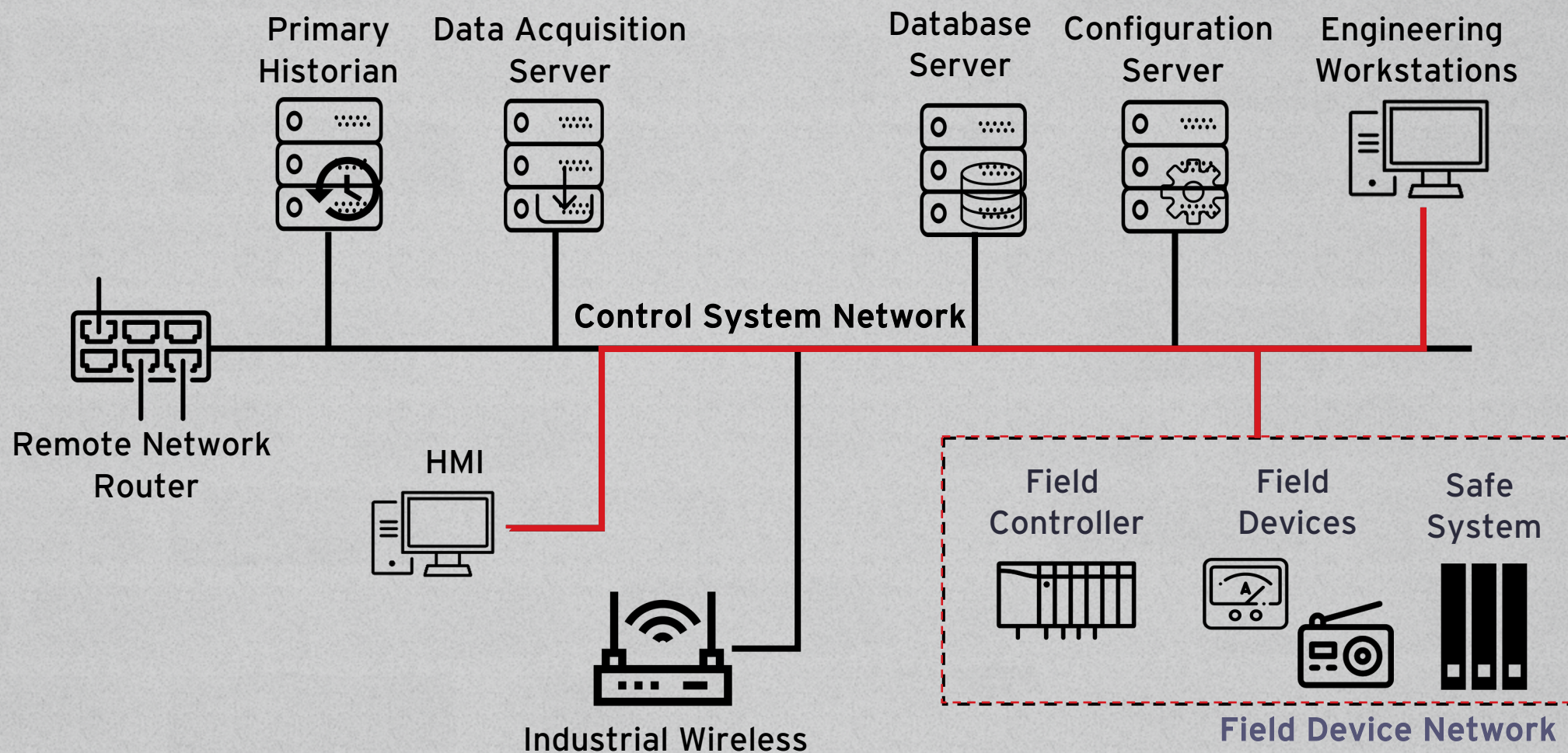
# ICS Protocols

## ICS Protocols



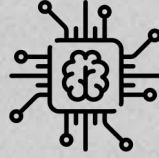


# Common ICS Architecture





# Critical Infrastructure Sectors (Taiwan)



High-Tech Park



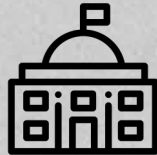
Energy



Traffic



Communications



Government



Water

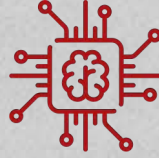


Finance



Medical

# Critical Infrastructure Sectors (Taiwan)



High-Tech Park



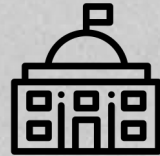
Energy



Traffic



Communications



Government



Water



Finance



Medical



# ICS Protocols and Critical Infrastructure Sectors (Singapore)



Aviation



Maritime



Water



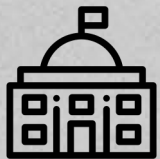
Transport



Healthcare



Energy



Government



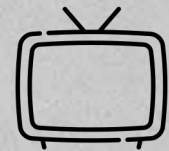
Security and Emergency Services



Banking and Finance



Infocom



Media



# ICS Protocols and Critical Infrastructure Sectors (Singapore)



Aviation



Maritime



Water



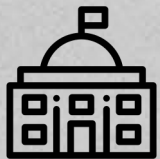
Transport



Healthcare



Energy



Government



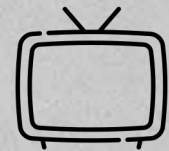
Security and Emergency Services



Banking and Finance



Infocomm



Media



# ICS Protocols and Critical Infrastructure Sectors (Japan)



Aviation



Financial



Airport



Gas



Water



Information and communication



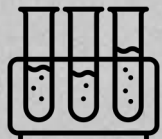
Medical



Electric power supply



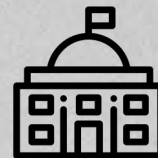
Railway



Chemical



Credit card



Government and administrative



Petroleum



Logistics

# ICS Protocols and Critical Infrastructure Sectors (Japan)



Aviation



Financial



Airport



Gas



Water



Information and communication



Medical



Electric power supply



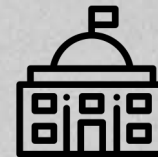
Railway



Chemical



Credit card



Government and administrative



Petroleum



Logistics



# ICS Protocols and Critical Infrastructure Sectors (US)



Chemical



Commercial Facilities



Communications



Critical Manufacturing



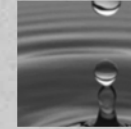
Emergency Services



Energy



Financial Services



Water and Wastewater Systems



Transportation Systems



Food and Agriculture



Defense Industrial Base Healthcare and Public Health



Nuclear Reactors, Materials, and Waste



Dams



Information Technology



Government Facilities

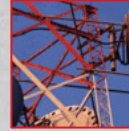
# ICS Protocols and Critical Infrastructure Sectors (US)



**Chemical**



**Commercial Facilities**



**Communications**



**Critical Manufacturing**



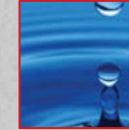
**Emergency Services**



**Energy**



**Financial Services**



**Water and Wastewater Systems**



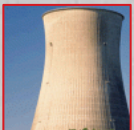
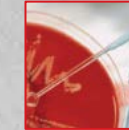
**Transportation Systems**



**Food and Agriculture**



**Defense Industrial Base Healthcare and Public Health**



**Nuclear Reactors, Materials, and Waste**



**Dams**



**Information Technology**



**Government Facilities**



# Public and Private: ICS Network Protocols

# Why Public vs. Private Protocols?

Public



Ethernet/IP®

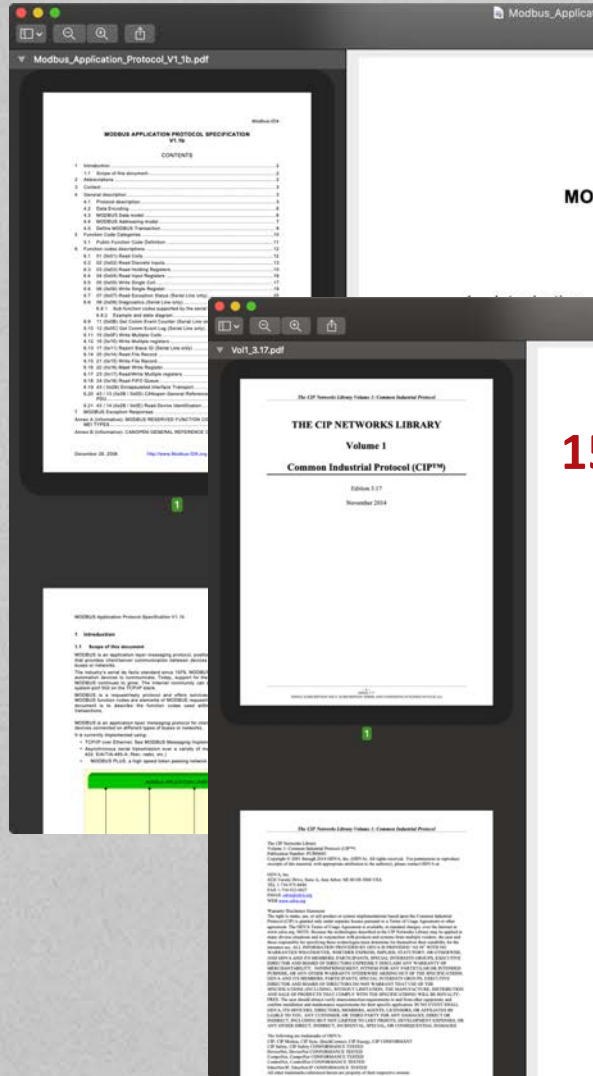
Private



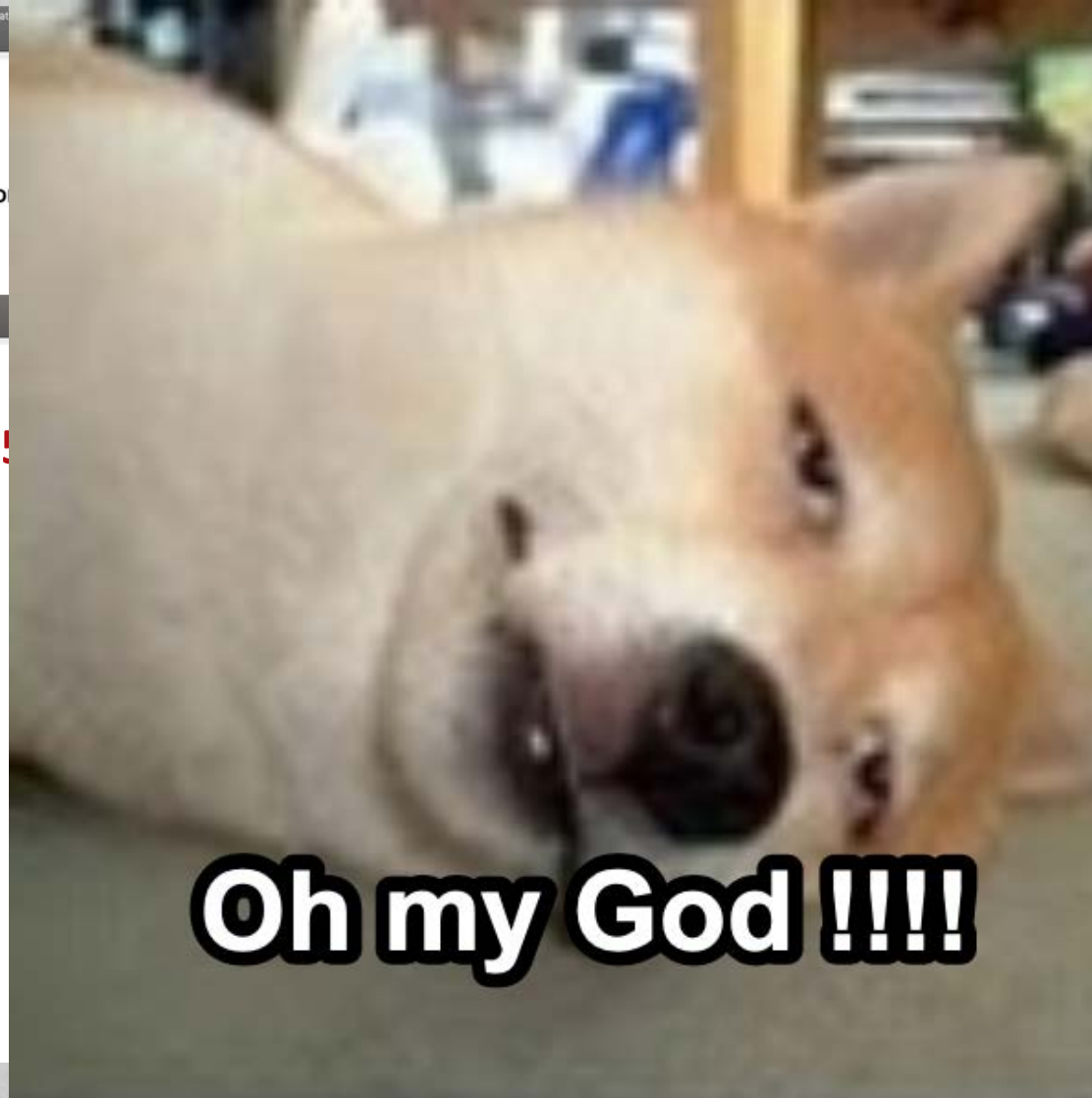
SIEMENS



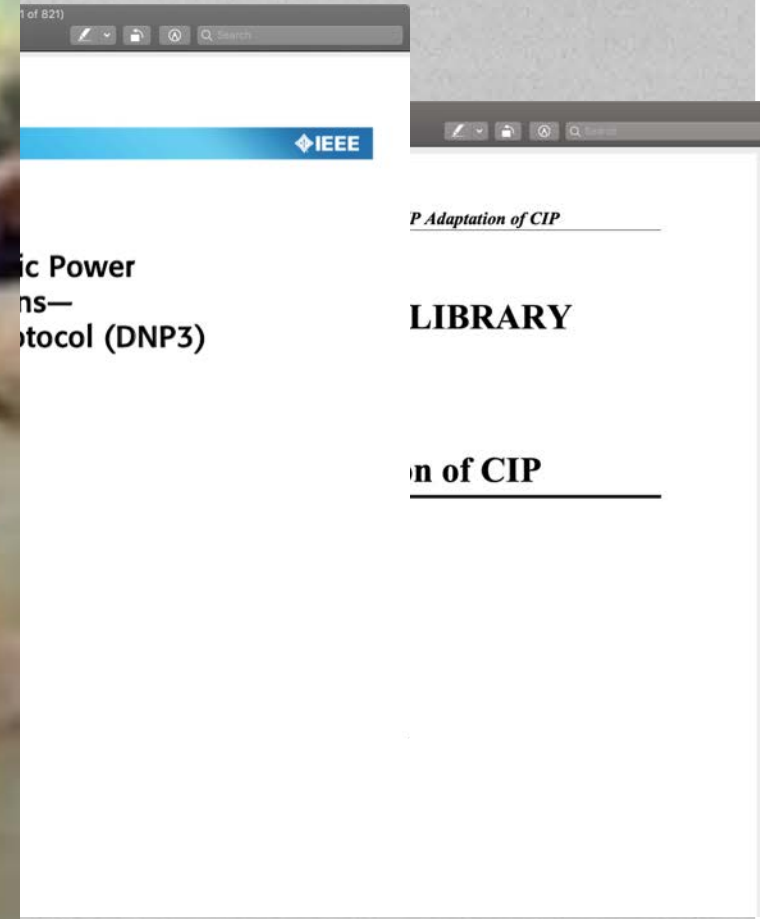
# The Specification of Public Protocols



15



Oh my God !!!!



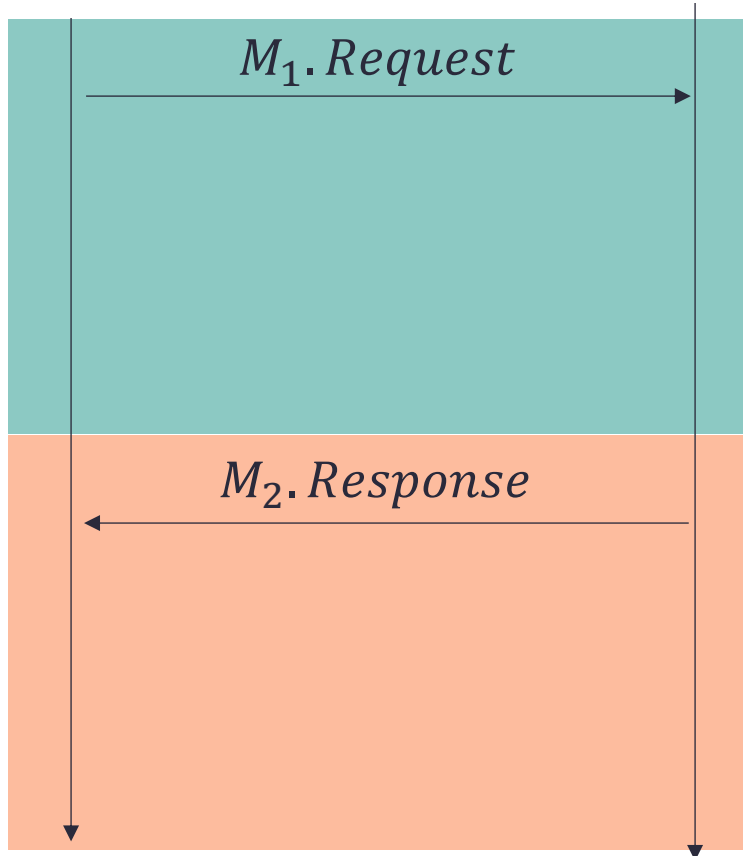
# Modbus/TCP Handshake Process



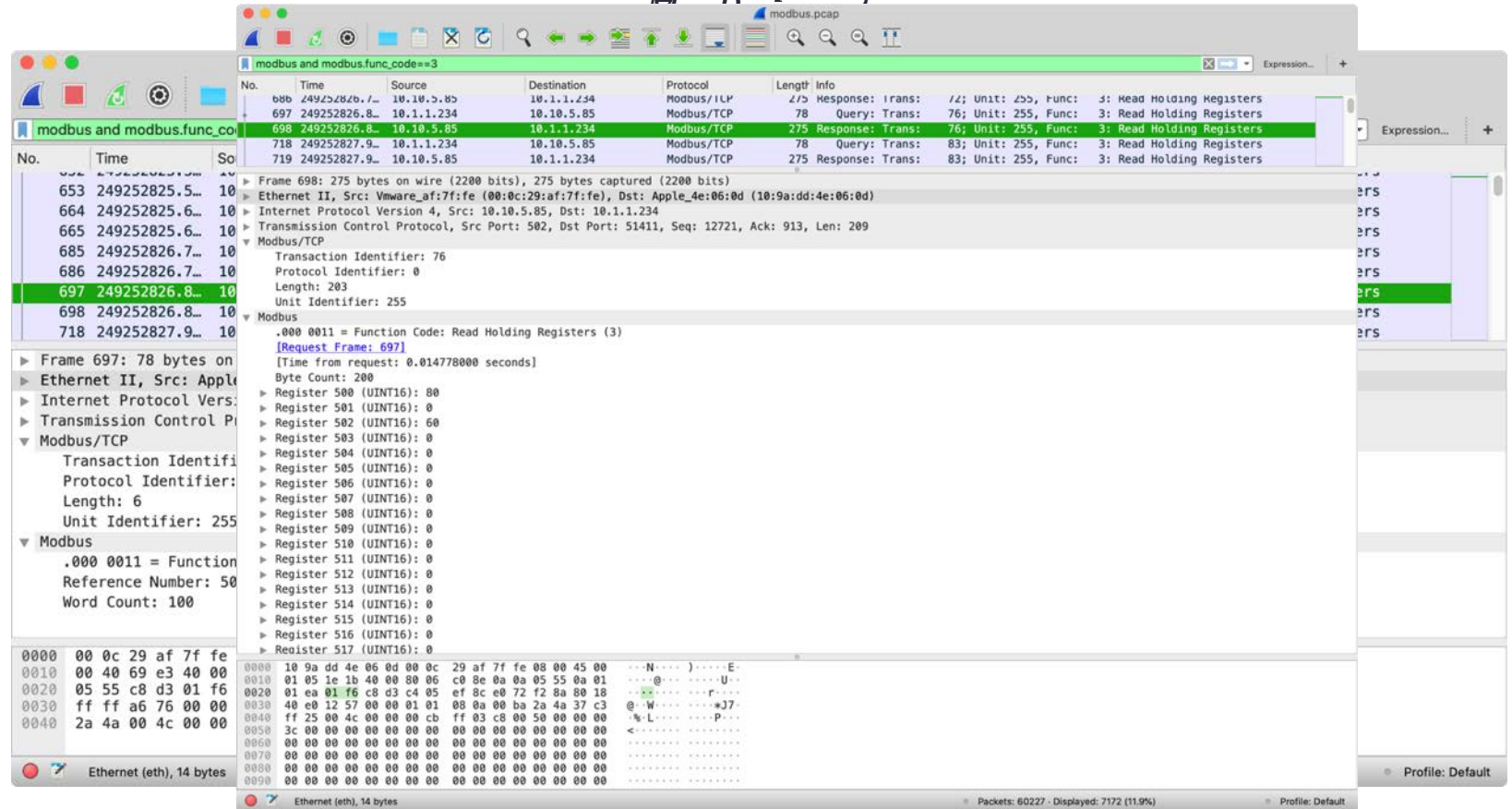
HMI



PLC

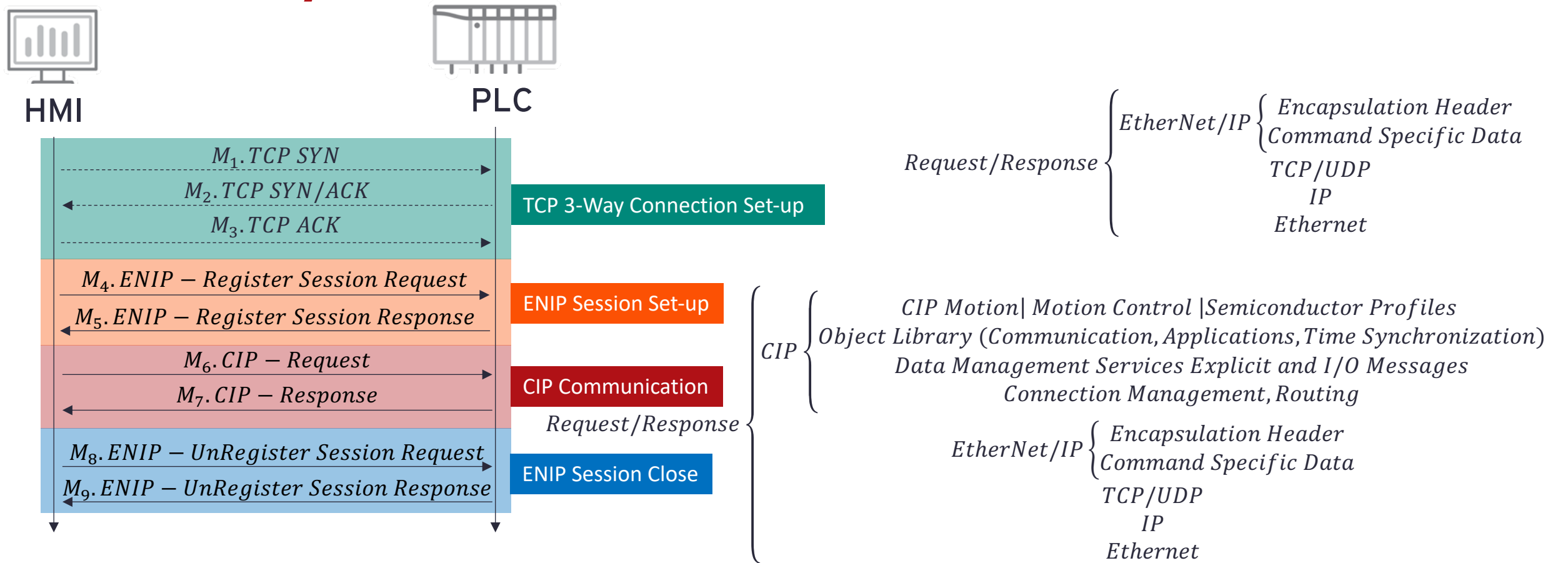


$M_2.Response$





# EtherNet/IP CIP Handshake Process



Command	Length	Session Handle	Status	Max Delay	Sender Context	Options	Command-specific Data
2 bytes	2 bytes	4 bytes	4 bytes	2 bytes	6 bytes	4 bytes	6 bytes

# Function Code

- Get Attributes All 0x01
- Set Attributes All 0x02
- Get Attribute List 0x03
- Set Attribute List 0x04
- Start 0x06
- Stop 0x07

The image shows a Wireshark packet capture of a CIP (Common Industrial Protocol) session. The top pane displays a list of 13 packets. Packet 9 is highlighted, showing a CIP 'Identity - Get Attribute List' response. The middle pane shows the packet details for this response, including the service code '0x03' and the request path 'Identity'. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.24.254.49	10.60.60.60	TCP	74	38878 → 44818 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1977658066 TSecr=0 WS=
2	0.000285	10.60.60.60	10.24.254.49	TCP	74	44818 → 38878 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2583860386
3	0.000303	10.24.254.49	10.60.60.60	TCP	66	38878 → 44818 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1977658066 TSecr=2583860386
4	0.000693	10.24.254.49	10.60.60.60	ENIP	94	Register Session (Req), Session: 0x00000000
5	0.000860	10.60.60.60	10.24.254.49	TCP	66	44818 → 38878 [ACK] Seq=1 Ack=29 Win=29056 Len=0 TSval=2583860387 TSecr=1977658066
6	0.002450	10.60.60.60	10.24.254.49	ENIP	94	Register Session (Rsp), Session: 0x12345678
7	0.002456	10.24.254.49	10.60.60.60	TCP	66	38878 → 44818 [ACK] Seq=29 Ack=29 Win=29312 Len=0 TSval=1977658068 TSecr=2583860388
8	0.003914	10.24.254.49	10.60.60.60	CIP	136	Identity - Get Attribute List
9	0.009653	10.60.60.60	10.24.254.49	CIP	201	Success: Identity - Get Attribute List
10	0.052108	10.24.254.49	10.60.60.60	TCP	66	38878 → 44818 [ACK] Seq=99 Ack=164 Win=30336 Len=0 TSval=1977658118 TSecr=2583860395
11	3.329832	10.24.254.49	10.60.60.60	TCP	66	38878 → 44818 [FIN, ACK] Seq=99 Ack=164 Win=30336 Len=0 TSval=1977661396 TSecr=2583860395
12	3.330282	10.60.60.60	10.24.254.49	TCP	66	44818 → 38878 [FIN, ACK] Seq=164 Ack=100 Win=29056 Len=0 TSval=2583863716 TSecr=1977661396
13	3.330310	10.24.254.49	10.60.60.60	TCP	66	38878 → 44818 [ACK] Seq=100 Ack=165 Win=30336 Len=0 TSval=1977661396 TSecr=2583863716

Frame 9: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)  
Ethernet II, Src: Dell\_c0:a2 (64:00:6a:cd:00:a2), Dst: Vmware\_f5:08:f1 (00:0c:29:f5:08:f1)  
Internet Protocol Version 4, Src: 10.60.60.60, Dst: 10.24.254.49  
Transmission Control Protocol, Src Port: 44818, Dst Port: 38878, Seq: 29, Ack: 99, Len: 135  
EtherNet/IP (Industrial Protocol), Session: 0x12345678, Send RR Data  
Common Industrial Protocol  
Service: Get Attribute List (Response)  
1... .... = Request/Response: Response (0x1)  
.000 0011 = Service: Get Attribute List (0x03)  
Status: Success  
[Request Path Size: 2 words]  
[Request Path: Identity, Instance: 0x01]

0000 00 0c 29 f5 08 f1 64 00 6a cd 00 a2 08 00 45 00 ..)....d.j.....E  
0010 00 bb fe ef 40 00 3f 06 ed 8b 0a 3c 3c 0a 18 ....@.7. ....<<<  
0020 fe 31 af 12 97 de cf ff 51 96 73 8e c7 4c 80 18 .1.....Q.s..L..  
0030 00 e3 1d 38 00 00 01 01 08 0a 9a 02 94 ab 75 e0 ..8.....u.....  
0040 aa d6 6f 00 6f 00 78 56 34 12 00 00 00 00 00 ..o.o.xV 4.....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....\_.x.....  
0060 02 00 00 00 00 00 b2 00 5f 00 83 00 00 00 0b 00 .....\_.x.....  
0070 01 00 00 00 01 00 02 00 00 00 0e 00 03 00 00 00 .....l.....  
0080 36 00 04 00 00 00 14 0b 05 00 00 00 60 31 06 00 6.....1.....  
0090 00 00 1a 06 6c 00 07 00 00 00 14 31 37 35 36 2d .....l.....1756-  
00a0 4c 36 31 2f 42 20 4c 4f 47 49 58 35 35 36 31 08 L61/B L0 GIX5561.  
00b0 00 00 00 ff 09 00 00 00 00 00 0a 00 00 00 00 0b .....TXON E  
00c0 00 00 00 05 54 58 4f 4e 45



# EtherNet/IP Traffic

The image shows a Wireshark packet capture of EtherNet/IP traffic. The main packet list displays 18 packets. Packet 8 is selected, showing a CIP Connection Manager - Forward Open (Message Router) message. The packet details pane shows the Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and EtherNet/IP (Industrial Protocol) layers. The EtherNet/IP layer shows a CIP Connection Manager Service: Forward Open (Request) message. The command specific data section includes priority, tick time, time-out ticks, actual time out, network connection IDs, connection serial number, originator vendor ID, originator serial number, connection timeout multiplier, reserved, and RPI.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.007583	192.168.1.10	192.168.1.250	TCP	60	44818 → 34248 [ACK] Seq=1 Ack=29 Win=8164 Len=0
6	0.007632	192.168.1.10	192.168.1.250	ENIP	82	Register Session (Rsp), Session: 0x00730001
7	0.007690	192.168.1.250	192.168.1.10	TCP	54	34248 → 44818 [ACK] Seq=29 Ack=29 Win=29312 Len=0
8	0.010134	192.168.1.250	192.168.1.10	CIP CM	142	Connection Manager - Forward Open (Message Router)
9	0.013060	192.168.1.10	192.168.1.250	TCP	60	44818 → 34248 [ACK] Seq=29 Ack=117 Win=8104 Len=0
10	0.022888	192.168.1.10	192.168.1.250	CIP CM	124	Success: Connection Manager - Forward Open
11	0.025812	192.168.1.250	192.168.1.10	CIP	112	Class (0x6b) - Get Attribute List
12	0.031916	192.168.1.10	192.168.1.250	TCP	60	44818 → 34248 [ACK] Seq=99 Ack=175 Win=8134 Len=0
13	0.035821	192.168.1.10	192.168.1.250	CIP	111	Success: Class (0x6b) - Get Attribute List
14	0.038979	192.168.1.250	192.168.1.10	CIP	113	Class (0x6b) - Set Attribute List
15	0.042754	192.168.1.10	192.168.1.250	TCP	60	44818 → 34248 [ACK] Seq=156 Ack=234 Win=8133 Len=0
16	0.049867	192.168.1.10	192.168.1.250	CIP	104	Privilege violation: Class (0x6b) - Set Attribute List
17	0.052599	192.168.1.250	192.168.1.10	CIP	112	Class (0x6b) - Get Attribute List
18	0.056473	192.168.1.10	192.168.1.250	TCP	60	44818 → 34248 [ACK] Seq=206 Ack=292 Win=8134 Len=0

Frame 8: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)

Ethernet II, Src: IntelCor\_5a:7f:f8 (80:19:34:5a:7f:f8), Dst: Rockwell\_c7:b0:70 (00:1d:9c:c7:b0:70)

Internet Protocol Version 4, Src: 192.168.1.250, Dst: 192.168.1.10

Transmission Control Protocol, Src Port: 34248, Seq: 29, Ack: 29, Len: 88

EtherNet/IP (Industrial Protocol), Session: 0x00730001, Send RR Data

Common Industrial Protocol

CIP Connection Manager

Service: Forward Open (Request)

0... .... = Request/Response: Request (0x0)

.101 0100 = Service: Forward Open (0x54)

Command Specific Data

...0 .... = Priority: 0

.... 0000 = Tick time: 0

Time-out ticks: 249

Actual Time Out: 249ms

0->T Network Connection ID: 0x80000031

T->0 Network Connection ID: 0x80fe0030

Connection Serial Number: 0x1337

Originator Vendor ID: Rockwell Software, Inc. (0x004d)

Originator Serial Number: 0xdeadbeef

Connection Timeout Multiplier: \*4 (0)

Reserved: 0x000000

0->T RPI: 8000.000ms

0->T Network Connection Parameters: 0x43f4

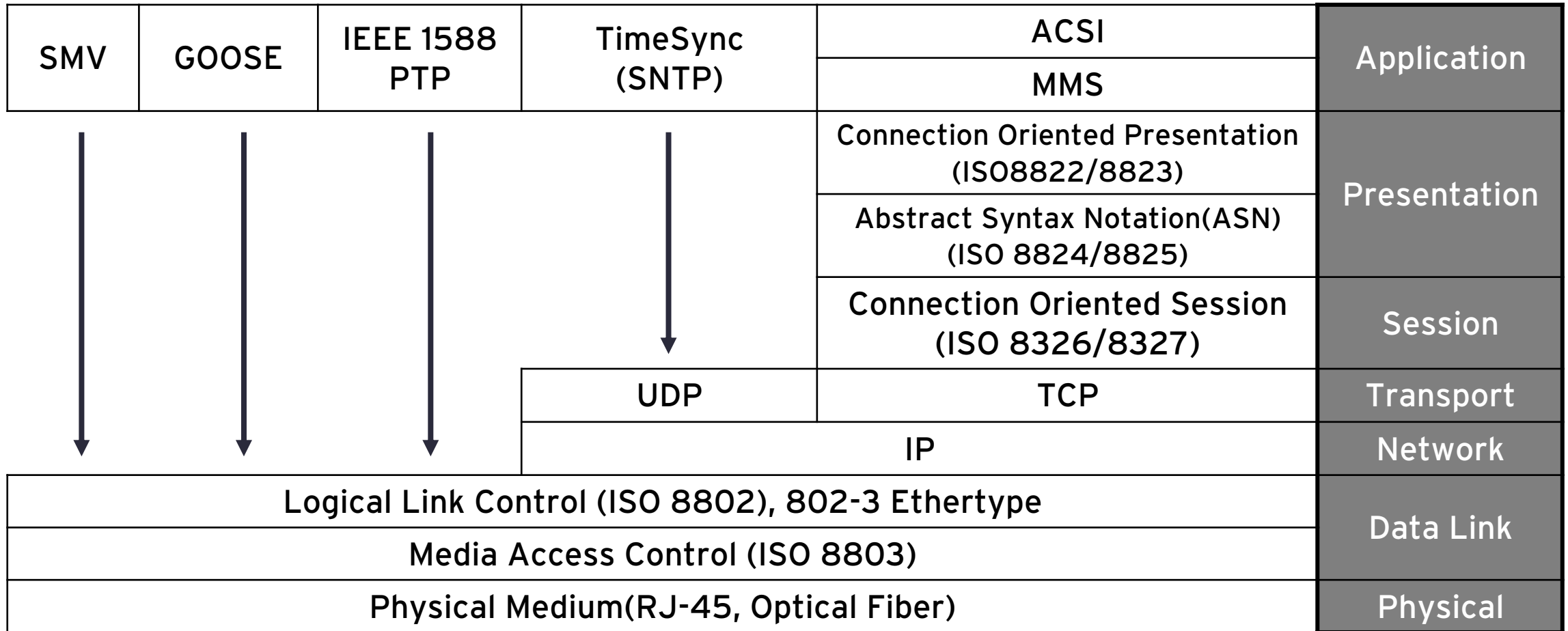
0050 00 00 00 00 02 00 00 00 00 00 b2 00 30 00 54 02 ..... 0..T.

0060 20 06 24 01 00 f9 31 00 00 80 30 00 fe 80 37 13 ..\$....1..0...7.

0070 4d 00 ef be ad de 00 00 00 00 00 12 7a 00 f4 43 M.....z...C

0080 00 12 7a 00 f4 43 a3 03 01 00 20 02 24 01 ...z...C...\$.</p></div>
<div data-bbox="890 917 975 957" data-label="Page-Footer">
<img alt="txOne networks logo" data-bbox="890 917 975 957"/>
</div>
<div data-bbox="17 943 145 963" data-label="Page-Footer">
 © 2021 TXOne Networks Inc.
</div>

# IEC 61850





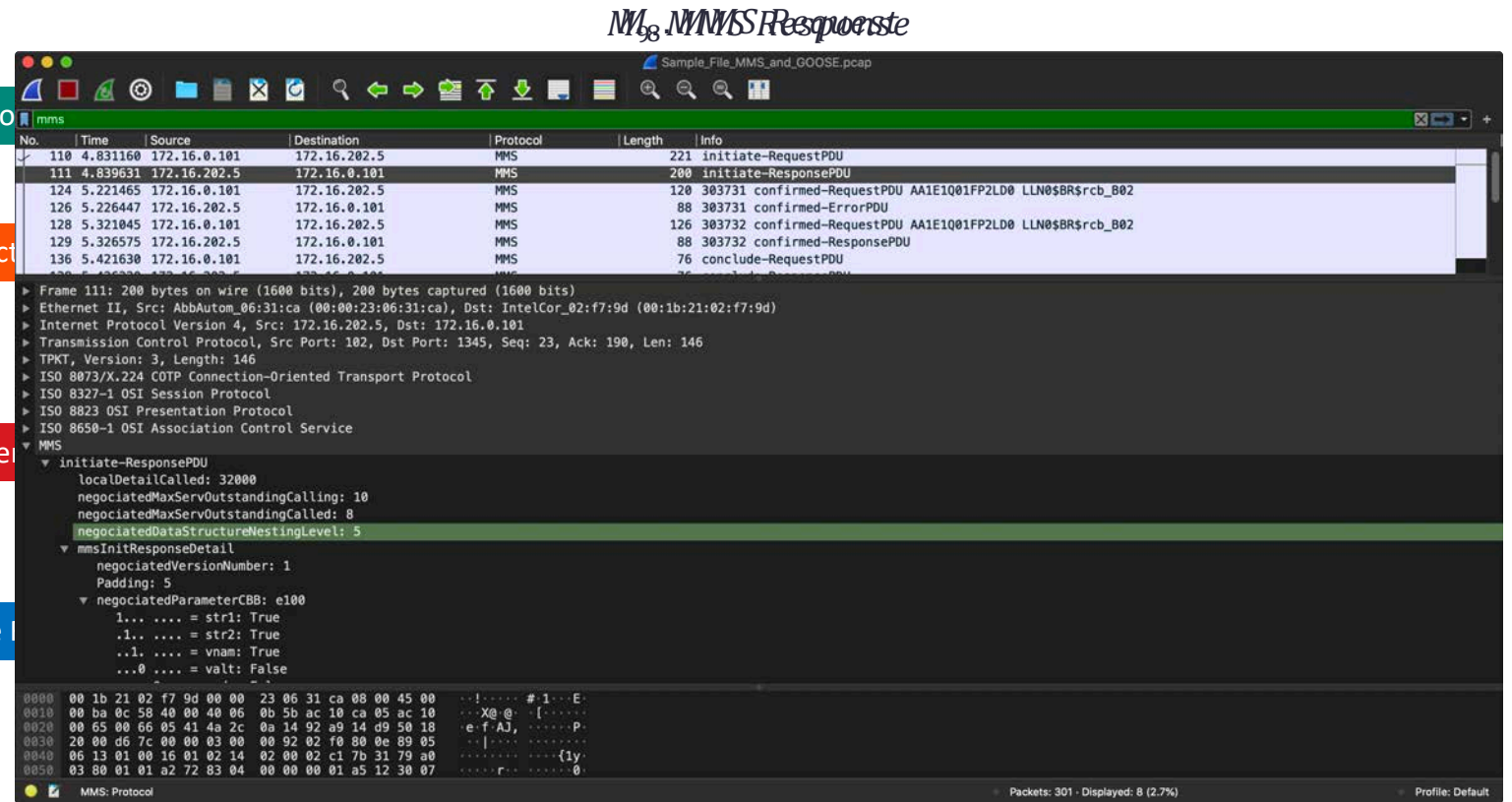
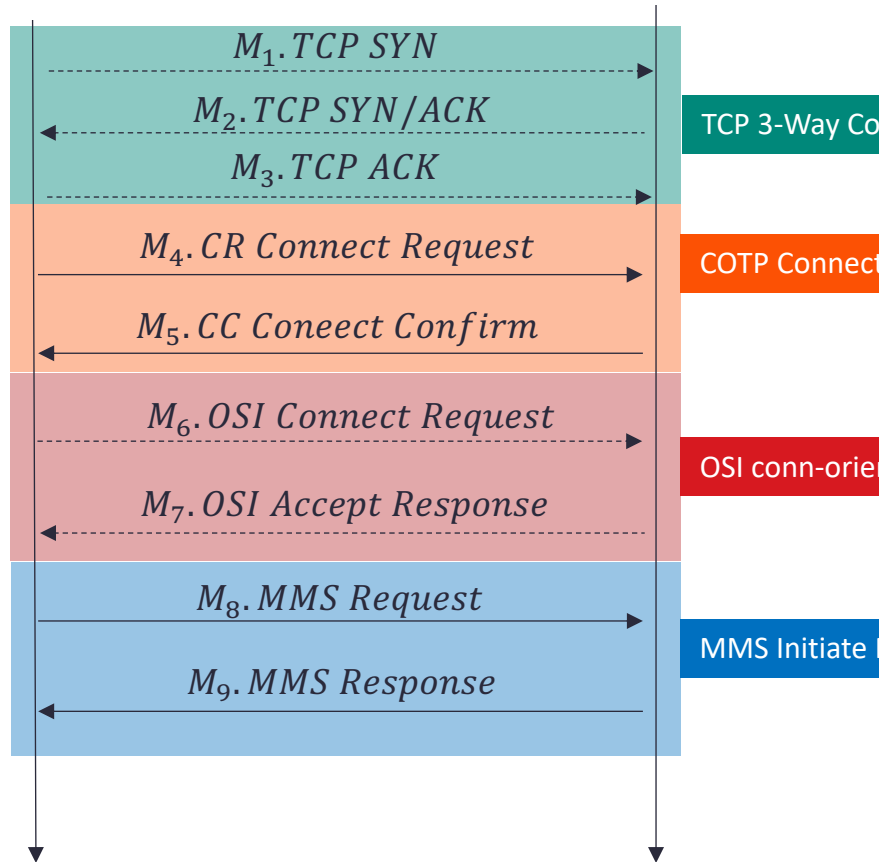
# IEC 61850 Manufacturing Message Spec (MMS)



HMI



PLC



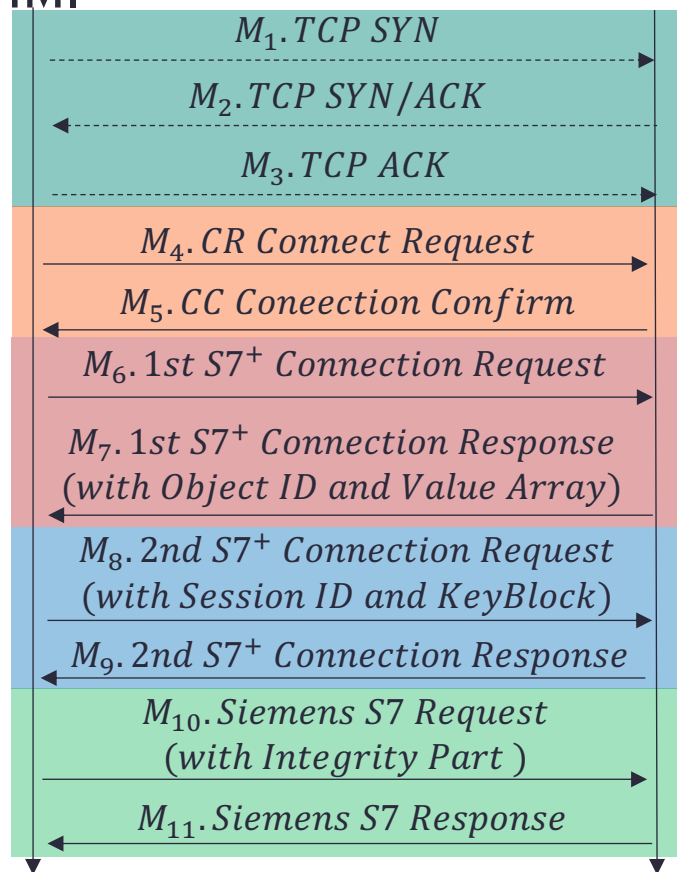
# Siemens S7 Plus Handshake Process



HMI



PLC



*M4. CR Connect Request*  
*M5. CC Conection Confirm*  
*M6. 1st S7+ Connection Request*  
*M7. 1st S7+ Connection Response (with Object ID and Value Array)*  
*M8. 2nd S7+ Connection Request (with Session ID and KeyBlock)*  
*M9. 2nd S7+ Connection Response*

S7-1511\_db3\_var1\_HMI.pcap

No.	Time	Source	Destination	Protocol	Length	Info
31	0.677669	192.168.25.146	192.168.25.139	TCP	54	56181 → 102 [ACK] Seq=1 Ack=1 Win=64240 Len=0
32	0.677764	192.168.25.146	192.168.25.139	COTP	104	CR TPDU src-ref: 0x0089 dst-ref: 0x0000
33	0.678287	192.168.25.139	192.168.25.146	COTP	104	CC TPDU src-ref: 0x000c dst-ref: 0x0089
34	0.678730	192.168.25.146	192.168.25.139	S7COMM-PLUS	297	+56181 Ver:[V1] Seq=1 [Req CreateObject] ObjectServerSessionContainer ClassServerSession / GetNewRIDOnServer ClassSubscri...
35	0.682726	192.168.25.139	192.168.25.146	TCP	60	102 → 56180 [ACK] Seq=298 Ack=734 Win=4096 Len=0
36	0.682731	192.168.25.139	192.168.25.146	TCP	60	102 → 56179 [ACK] Seq=298 Ack=734 Win=4096 Len=0
37	0.686677	192.168.25.139	192.168.25.146	S7COMM-PLUS	269	+56181 Ver:[V1] Seq=1 [Res CreateObject] Retval=OK ObjId=Unknown (908), Unknown (909)
38	0.686875	192.168.25.146	192.168.25.139	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
39	0.718073	192.168.25.146	192.168.25.139	S7COMM-PLUS	480	+56181 Ver:[V2] Seq=2 [Req SetMultiVariables] ObjId=Unknown (908)
40	0.772641	192.168.25.139	192.168.25.146	S7COMM-PLUS	86	+56181 Ver:[V2] Seq=2 [Res SetMultiVariables] Retval=OK
41	0.772835	192.168.25.146	192.168.25.139	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
42	0.773741	192.168.25.146	192.168.25.139	S7COMM-PLUS	151	+56179 Ver:[V2] Seq=3 [Req GetVarSubStreamed]
43	0.776052	192.168.25.139	192.168.25.146	S7COMM-PLUS	177	+56179 Ver:[V2] Seq=3 [Res GetVarSubStreamed] Retval=OK
44	0.776166	192.168.25.146	192.168.25.139	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]

> Frame 43: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)  
 > Ethernet II, Src: Siemens\_13:41:73 (00:1b:1b:13:41:73), Dst: Vmware\_34:60:5d (00:50:56:34:60:5d)  
 > Internet Protocol Version 4, Src: 192.168.25.139, Dst: 192.168.25.146  
 > Transmission Control Protocol, Src Port: 102, Dst Port: 56179, Seq: 298, Ack: 831, Len: 123  
 > TPkt, Version: 3, Length: 123  
 > ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
 > S7 Communication Plus  
 > Header: Protocol version=V2  
 > Data: Response GetVarSubStreamed  
 > Opcode: Response (0x32)  
 > Reserved: 0x0000  
 > Function: GetVarSubStreamed (0x0586)  
 > Reserved: 0x0000  
 > Sequence number: 3  
 > Transport flags: 0x34, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?  
 > Response Set  
 > Return value: 0x0000000000000000, Error code: OK, Generic error code: OK  
 > Response unknown 1: 0x00  
 > Item Value (DInt) Sparsearray = 250, 2000, 204800, 20, 54, 10240, 50, 0, 10240...  
 > Integrity part  
 > Integrity Id: 4  
 > Digest Length: 32  
 > Packet Digest: d69ccd76ead9c1b6da084c27bcd8fc93c01aba9531d746c3...  
 > Trailer: Protocol version=V2



# Siemens S7 Plus Version

## V1

21	0.150399	192.168.1.191	192.168.1.35	COTP
22	0.151095	192.168.1.35	192.168.1.191	S7COMM-PLUS
23	0.207101	192.168.1.191	192.168.1.35	S7COMM-PLUS
24	0.207326	192.168.1.35	192.168.1.191	COTP
25	0.207608	192.168.1.35	192.168.1.191	S7COMM-PLUS

< >

> Frame 22: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits)  
> Ethernet II, Src: Vmware\_44:2d:17 (00:0c:29:44:2d:17), Dst: Siemens\_08:e7:db (00:1c:06:00:08:e7:db)  
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.191  
> Transmission Control Protocol, Src Port: 49179, Dst Port: 102, Seq: 37, Ack: 37, Len: 25  
> TPkt, Version: 3, Length: 251  
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
v S7 Communication Plus  
v Header: Protocol version=V1  
Protocol Id: 0x72  
Protocol version: V1 (0x01)  
Data length: 236  
> Data: Request CreateObject  
> Trailer: Protocol version=V1

## V3

1890	29.536238	10.24.103.251	10.24.103.200	S7COMM-PLUS
1891	29.536389	10.24.103.251	10.24.103.200	S7COMM-PLUS
1892	29.536413	10.24.103.200	10.24.103.251	TCP
1893	29.536512	10.24.103.251	10.24.103.200	TCP

< >

> Frame 1890: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)  
> Ethernet II, Src: Vmware\_a4:ca:98 (00:0c:29:a4:ca:98), Dst: LcfcHefe\_d6:ee:43 (50:7b:9d:d6:ee:43)  
> Internet Protocol Version 4, Src: 10.24.103.251, Dst: 10.24.103.200  
> Transmission Control Protocol, Src Port: 46818, Dst Port: 102, Seq: 415738, Ack: 1, Len: 1448  
> [2 Reassembled TCP Segments (1882 bytes): #1888(1172), #1890(710)]  
> TPkt, Version: 3, Length: 1882  
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
v S7 Communication Plus  
v Header: Protocol version=V3  
Protocol Id: 0x72  
Protocol version: V3 (0x03)  
Data length: 1867  
v Integrity part  
Digest Length: 32  
Packet Digest: 2e99d6b10d0581984adb5a684a2cb226771c0d173d03928d...  
> Data: Request GetMultiVariables  
> Trailer: Protocol version=V3

## V2

42	53.710232	192.168.25.146	192.168.25.139	TCP
43	53.712034	192.168.25.139	192.168.25.146	S7COMM-PLUS
44	53.715816	192.168.25.146	192.168.25.139	COTP
45	53.715827	192.168.25.146	192.168.25.139	TCP
46	53.877113	192.168.25.139	192.168.25.146	TCP

< >

> Frame 43: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)  
> Ethernet II, Src: Siemens\_13:41:73 (00:1b:1b:13:41:73), Dst: Vmware\_34:60:5d (00:50:56:34:60:5d)  
> Internet Protocol Version 4, Src: 192.168.25.139, Dst: 192.168.25.146  
> Transmission Control Protocol, Src Port: 102, Dst Port: 55863, Seq: 564, Ack: 1169, Len: 66  
> TPkt, Version: 3, Length: 66  
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
v S7 Communication Plus  
v Header: Protocol version=V2  
v Data: Response GetMultiVariables  
Opcode: Response (0x32)  
Reserved: 0x0000  
Function: GetMultiVariables (0x054c)  
Reserved: 0x0000  
Sequence number: 6  
> Transport flags: 0x34, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?  
v Response Set  
v Integrity part  
Integrity Id: 10  
Digest Length: 32  
Packet Digest: c6bf255aaec1f182c3ee8fe37ca48ac577a008ae3a520112...  
> Trailer: Protocol version=V2



# Common Flaws in ICS Network Protocols



# Insecure by Design

Type	Protocols	Handshake	Authentication	Message Encryption
Public	Modbus/TCP	TCP Connection	×	×
	DNP3/TCP	TCP Connection	×	×
	EtherNetIP/CIP	ENIP Connection based	×	×
	IEC104	TCP Connection + STARTDT	×	×
	IEC 61850	TCP Connection	×	×
Private	Melsec/TCP	TCP Connection	×	×
	Melsoft/TCP	TCP Connection	✓ (EWS <-> PLC)	×
	OMRON FINS/TCP	TCP Connection + FINS/TCP session based	×	×
	S7COMM	TCP Connection + COTP + S7COMM Session	×	△(when EWS compile PLC program)
	S7COMM Plus	TCP Connection + COTP + S7COMM+ Session	V1	×
			V2	✓(HMAC-SHA256)
			V3	✓(HMAC-SHA256)

# Attacks on ICS Protocols

? Unknown

Type	Protocols		T814 Denial-of-Service	T836 Modify Parameter	T856 Spoof Reporting Message	T843 Program Download	T855 Unauthorized Command Message
Public	Modbus/TCP		✓	✓	✓	?	✓
	DNP3/TCP		✓	✓	✓	?	✓
	EtherNetIP/CIP		?	✓	✓	✓	✓
	IEC104		✓	✓	✓	?	✓
	IEC 61850		?	✓	✓	?	✓
Private	Melsec/TCP		?	✓	✓	✓	✓
	Melsoft/TCP		?	✓	✓	✓	✓
	OMRON FINS/TCP		?	✓	✓	✓	✓
	S7COMM		✓	✓	✓	✓	✓
	S7COMM Plus	V1	?	✓	?	✓	✓
		V2	?	✓	?	✓	✓
		V3	?	✓	?	✓	✓



# ICS ATT&CK Matrix map to ICS Protocols Attack

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial Comm Port	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

11 Tactics  
81 Techniques

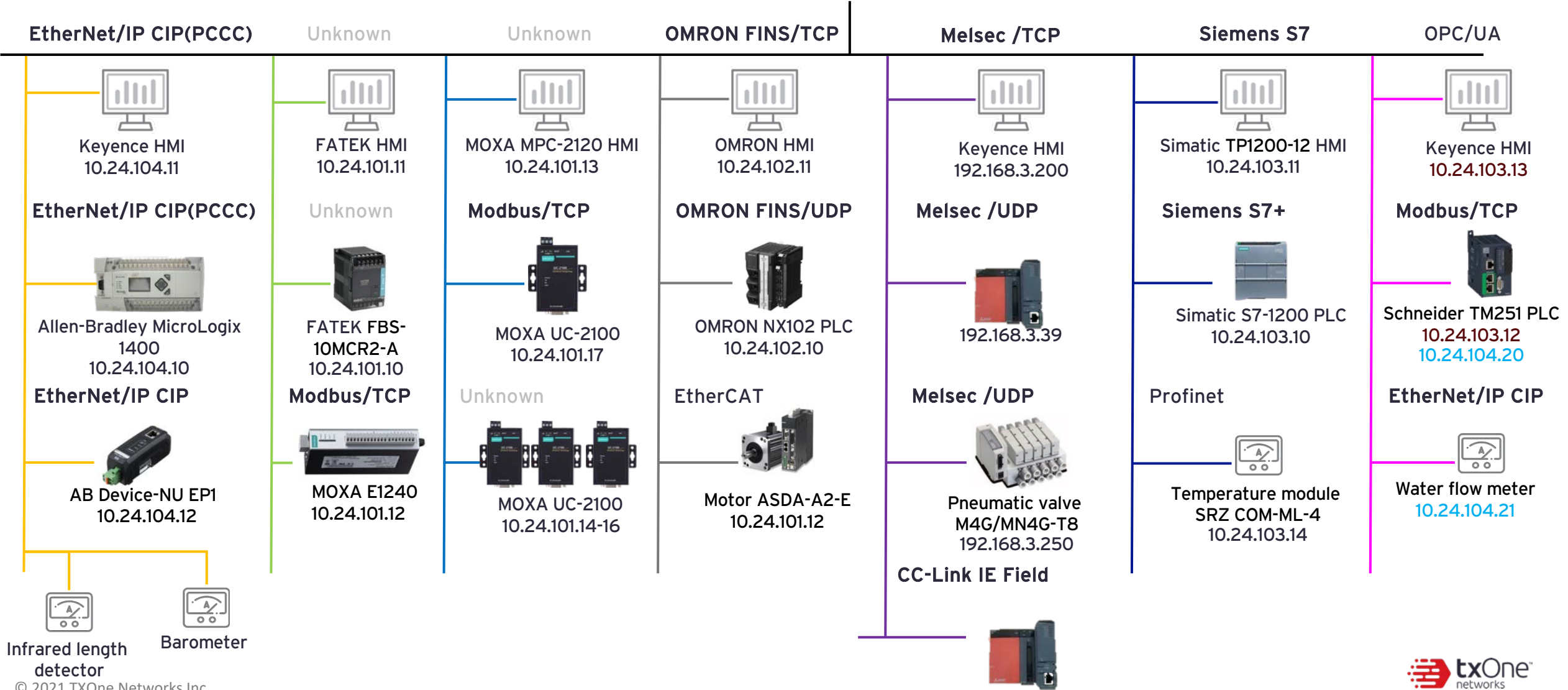
# Demo Time



# TXOne's ICS Lab



Windows 7 VM  
Software: In touch  
10.24.100.10



# **T836-Modify Parameter with Mitsubishi Melsec Protocol**





# T836-Modify Parameter

lab\_plc\_command\_injection.pcap

mc\_proto

Source	Destination	Protocol	Length	Info
192.168.3.87	192.168.3.39	M_Protocol	77	Melsec 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	Melsec 3E Binary Response
192.168.3.87	192.168.3.39	M_Protocol	77	Melsec 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	Melsec 3E Binary Response
192.168.3.87	192.168.3.39	M_Protocol	77	Melsec 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	Melsec 3E Binary Response
192.168.3.87	192.168.3.39	M_Protocol	77	Melsec 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	Melsec 3E Binary Response

Sub Header  
Data Len: 0x000e (14)  
Timer: 0x000a (10)  
Command: 0x1401 (Batch Write Device)  
Sub-Command: 0x0000  
Request Data: 640000a801000a00  
Head device number: 0x000064 (100)  
Device code: 0xa8  
Number of device points: 0x0001 (1)  
Write data: 0a00

0020 03 27 dc a6 1e 6c 73 f8 d6 09 00 34 42 e8 50 18 ...ls...4B.P  
0030 ff ff 93 29 00 00 50 00 00 ff ff 03 00 0e 00 0a ...P...  
0040 00 01 14 00 00 64 00 00 a8 01 00 0a 00 .....d.....

Write data (mc\_proto.write\_data\_bin), 2 bytes

Packets: 40 · Displayed: 8 (20.0%) · Profile: Default

Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39  
Transmission Control Protocol, Src Port: 56486, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23  
3E Binary Request  
Sub Header  
Data Len: 0x000e (14)  
Timer: 0x000a (10)  
Command: 0x1401 (Batch Write Device)  
Sub-Command: 0x0000  
Request Data: 640000a801000a00  
Head device number: 0x000064 (100)  
Device code: 0xa8  
Number of device points: 0x0001 (1)  
Write data: 0a00

10s

Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39  
Transmission Control Protocol, Src Port: 56497, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23  
3E Binary Request  
Sub Header  
Data Len: 0x000e (14)  
Timer: 0x000a (10)  
Command: 0x1401 (Batch Write Device)  
Sub-Command: 0x0000  
Request Data: 640000a801000200  
Head device number: 0x000064 (100)  
Device code: 0xa8  
Number of device points: 0x0001 (1)  
Write data: 0200

2s

Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39  
Transmission Control Protocol, Src Port: 56510, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23  
3E Binary Request  
Sub Header  
Data Len: 0x000e (14)  
Timer: 0x000a (10)  
Command: 0x1401 (Batch Write Device)  
Sub-Command: 0x0000  
Request Data: 640000a801000800  
Head device number: 0x000064 (100)  
Device code: 0xa8  
Number of device points: 0x0001 (1)  
Write data: 0800

8s

Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39  
Transmission Control Protocol, Src Port: 56521, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23  
3E Binary Request  
Sub Header  
Data Len: 0x000e (14)  
Timer: 0x000a (10)  
Command: 0x1401 (Batch Write Device)  
Sub-Command: 0x0000  
Request Data: 640000a801001e00  
Head device number: 0x000064 (100)  
Device code: 0xa8  
Number of device points: 0x0001 (1)  
Write data: 1e00

30s



# **T855-Unauthorized Command Message with OMRON FINS Protocol**



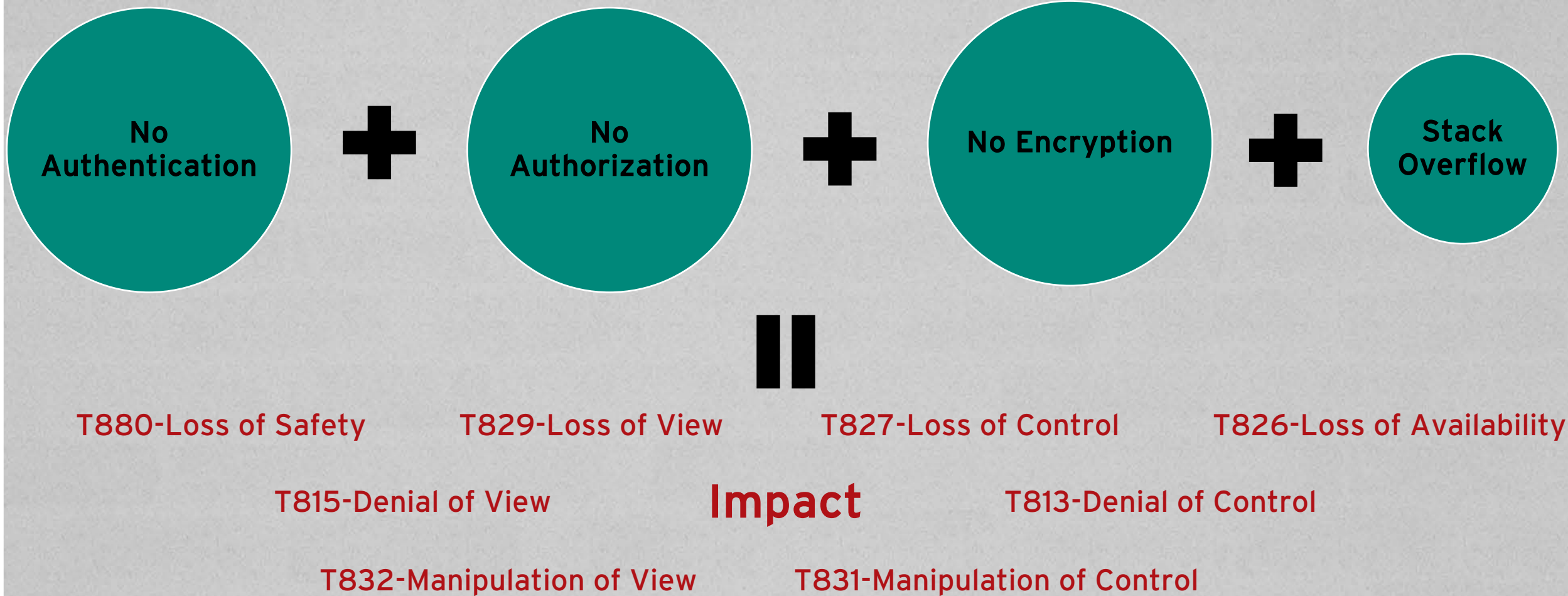


# **T856-Spoof Reporting Message with Modbus/TCP Protocol**





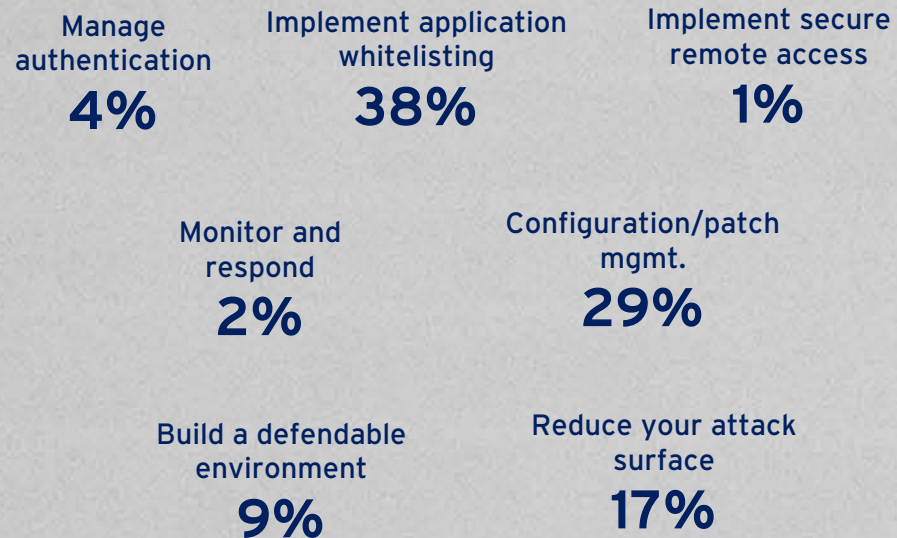
# Common Flaws in ICS Protocols



# How to Defend Against ICS Network Protocol Attacks



## Suggested Strategies from ICS CERT



*Incidents responded by ICS-CERT:* [https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf)



Implementing **FIVE** Tactics to prevent 98% incidents

# Best Practices for ICS Cyber Threat Resistance



Keep the Operation Running



# Network Segmentation Benefits



Risk Mitigation



Prevent Lateral  
Movement



Outbreak  
Prevention



Deal with Massive  
IoT Adoption

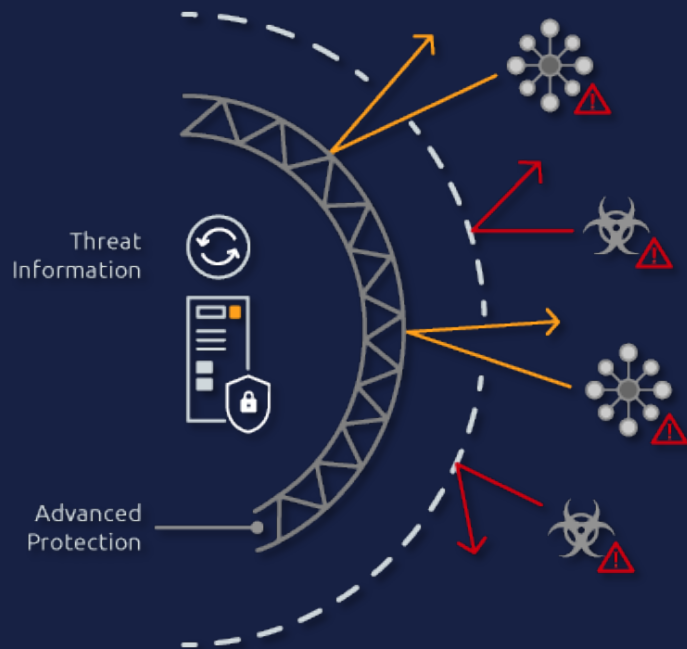


Future Private 5G  
Connection



Zero Trust  
Network

# Bridge the ICS Vulnerability Gap: Virtual Patching



Shield vulnerable  
assets



Zero-Day Attack  
Prevention



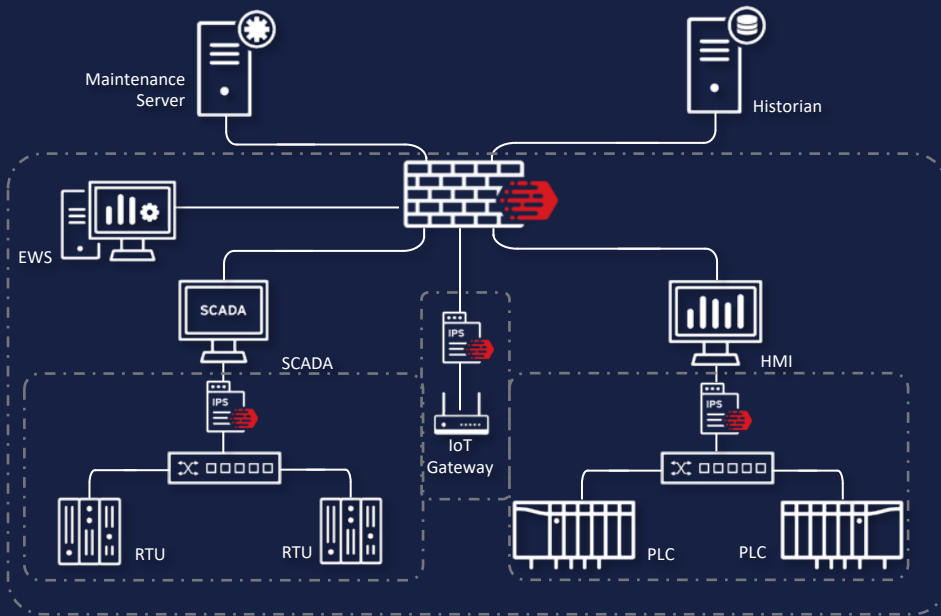
Maintain  
Productivity



Patching Process  
Enhancement

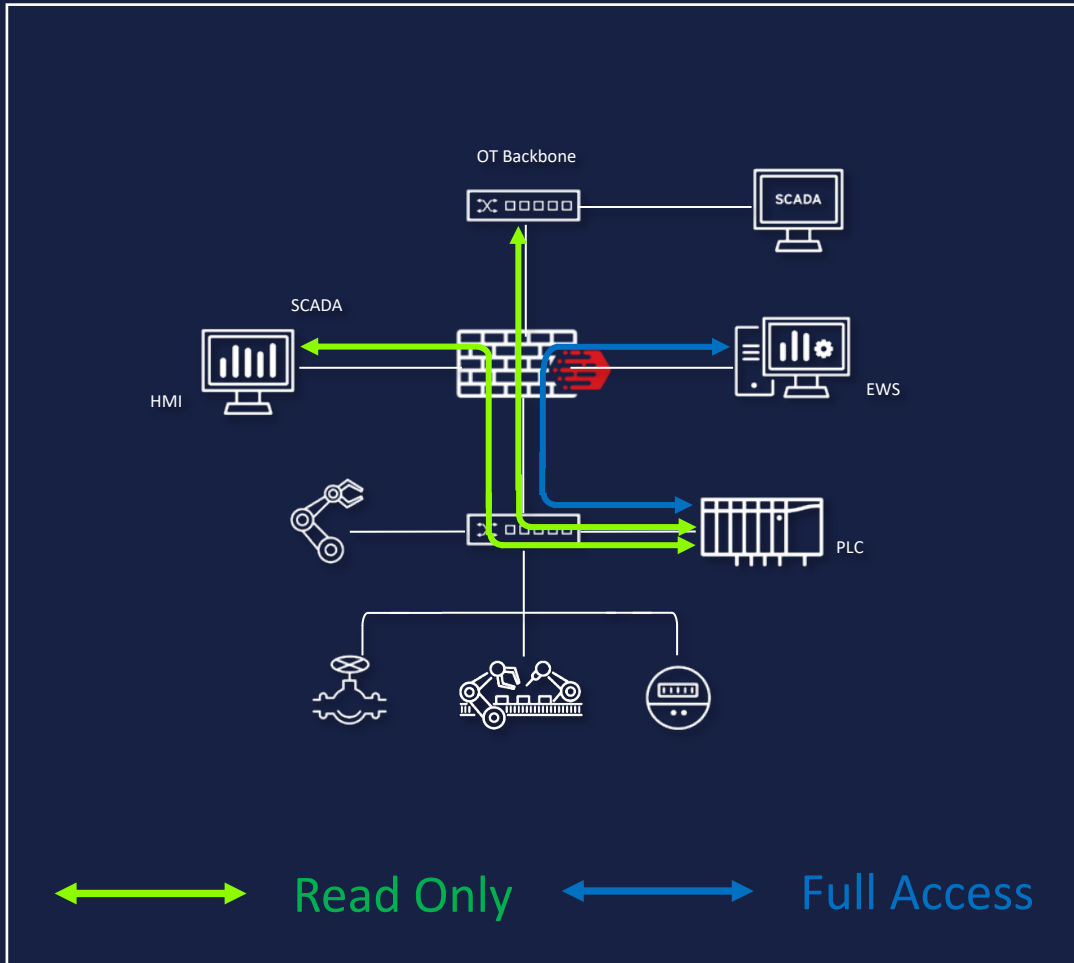


# Effective Internal/Micro Segmentation and Shielding with Virtual Patch



- Divide a big flat L2 network into secured segments
- Virtual Patch (IPS)
  - Containment of malware and worms
  - Shield device vulnerabilities
  - Deeply inspect IT protocols: SMB, RDP, ...
- Industrial-Grade Hardware

# Trust List



- Asset and protocol visibility
- Fine-grained access control at different levels
  - Devices
  - Protocols (HL7, DICOM, Modbus, Melsec/SLMP, CC-Link IE, Ethernet/IP, Profinet, S7COMM, HSMS/SECS-II, ...)
  - Control Commands (read, configure, shutdown, ...)
- Greatly lower the possibility of Denial-of-Service by OT trojans



# Thanks for Listening

Mars Cheng (@marscheng\_)

Selmon Yang

