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

txOne networks

Who are we?

A joint venture company of

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

30 years+ Cybersecurity Threat Intelligence

30 years+ OT Network Expertise

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

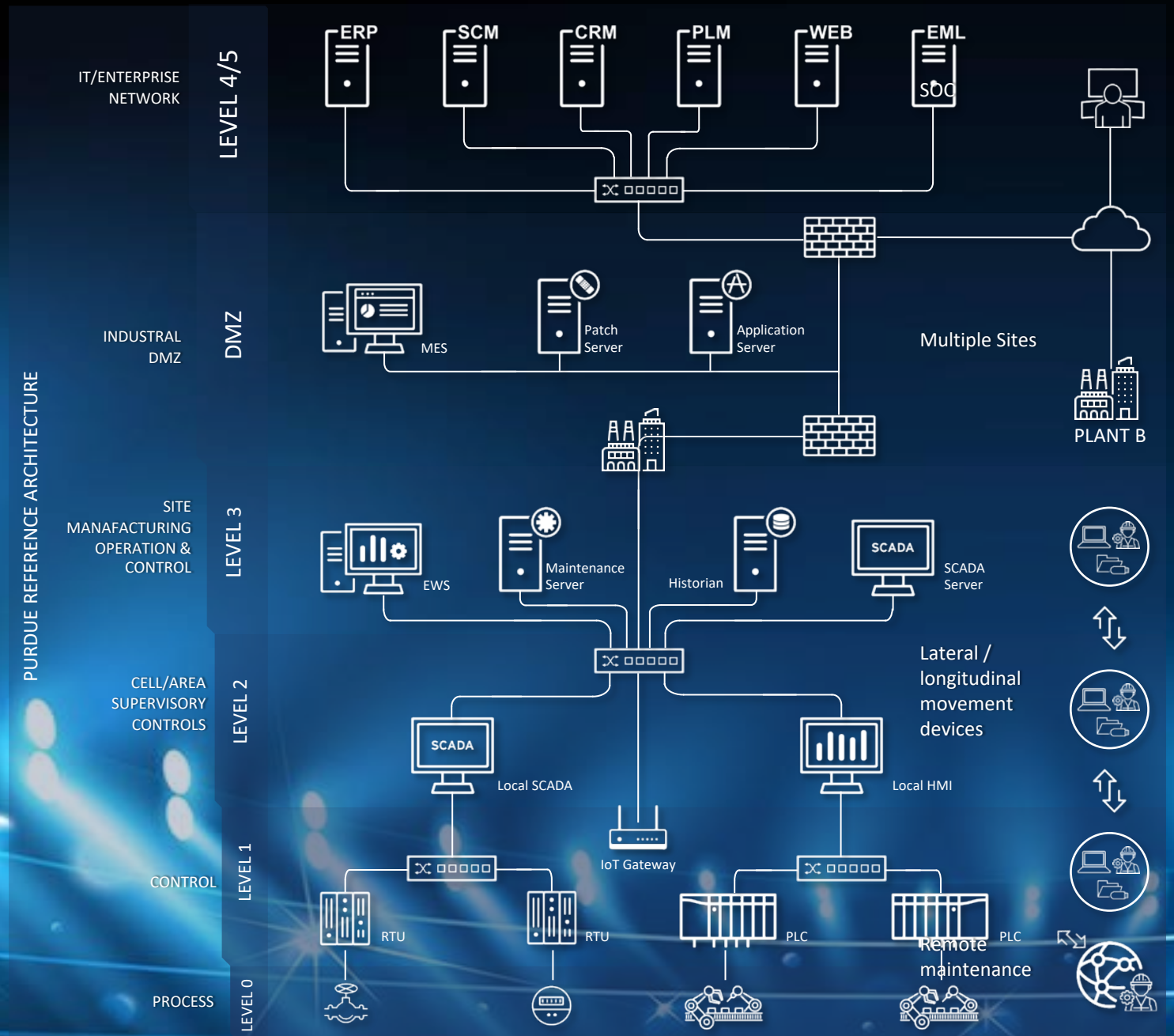
- IT/SCADA Protocol Parsing
- Linux Kernel Programming
- Honeypot Deployment & Optimization

Outline

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

txOne networks

ICS Architecture and Attack Vectors

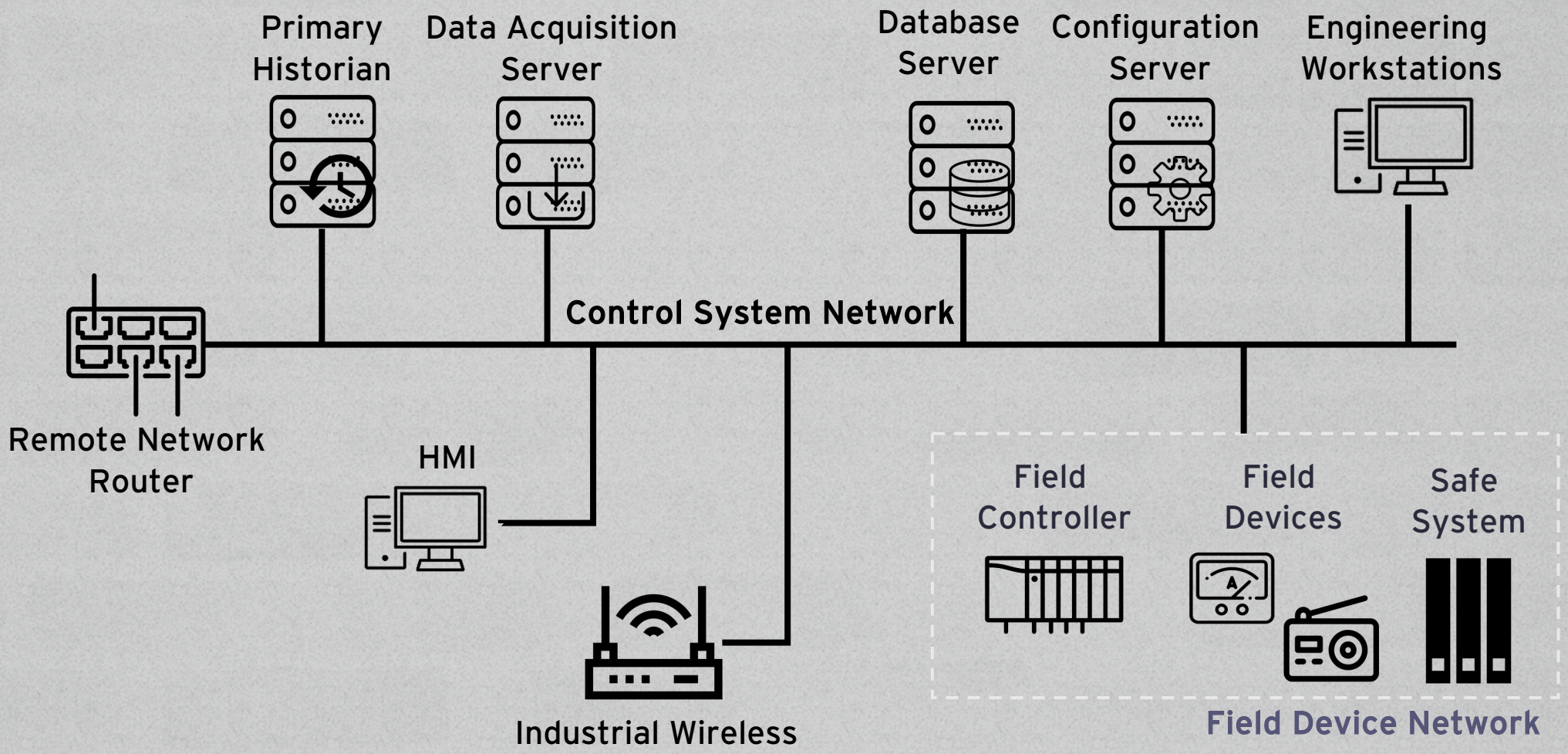


Information Technology (IT)

Operational Technology (OT)

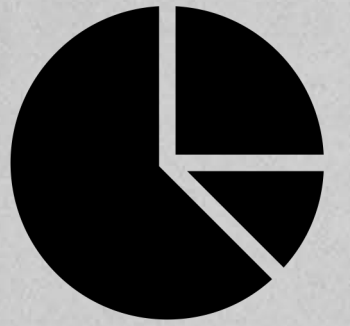
txOne networks

Common ICS Architecture

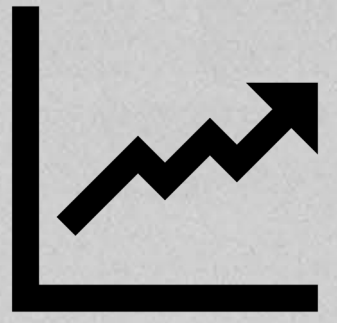


txOne networks

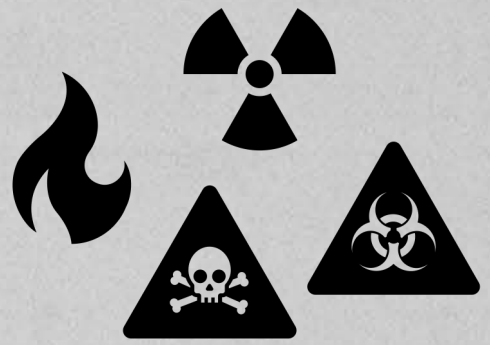
ICS/SCADA Security Threat Situation



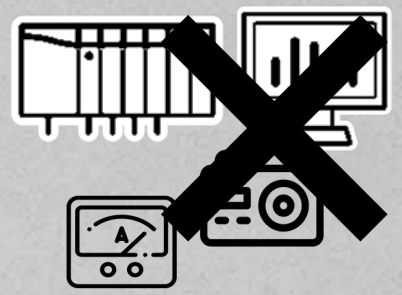
Vulnerabilities are mostly critical and high risk levels



The number of vulnerability is rising year by year



The security incidents have a huge impact

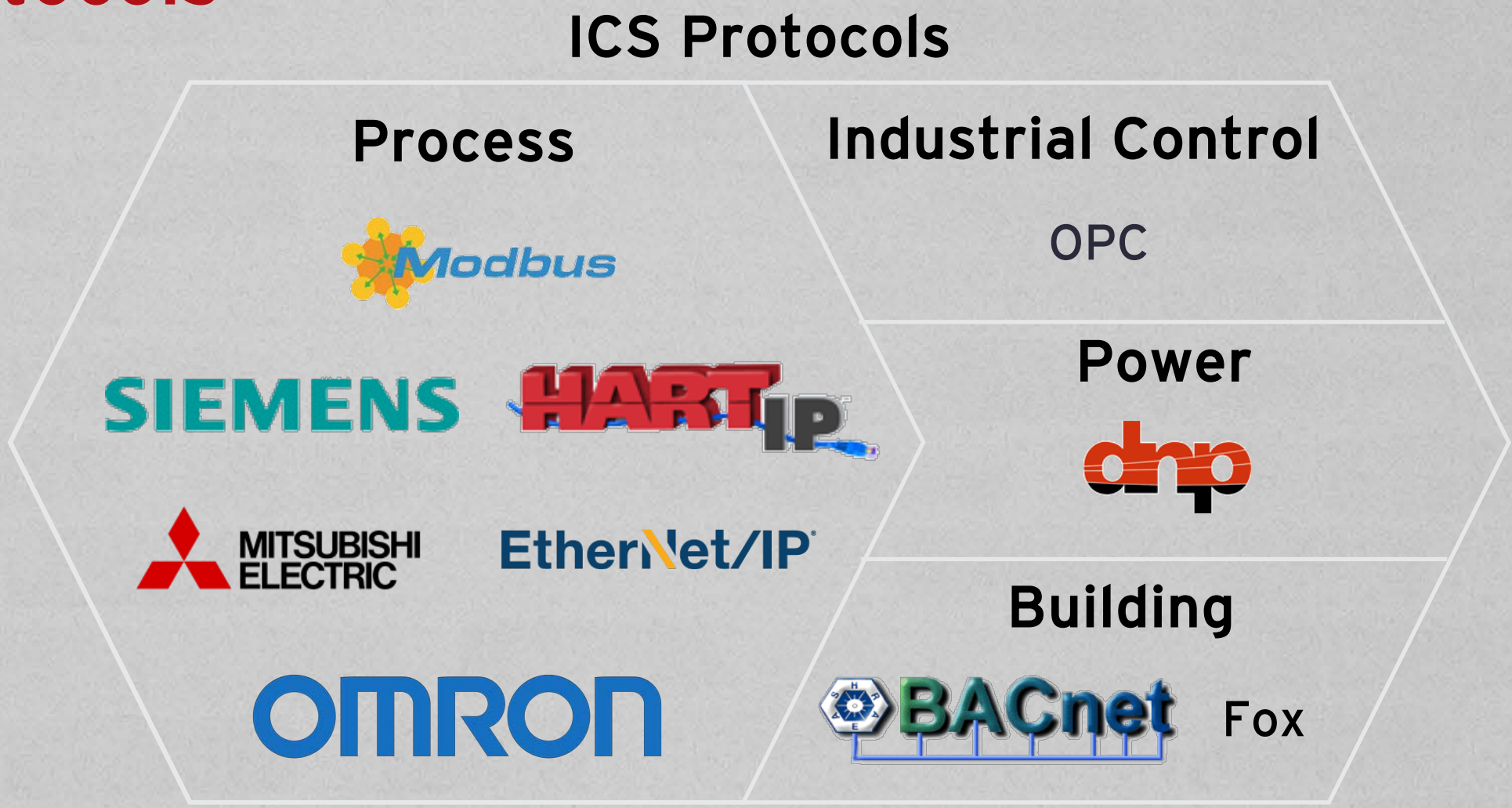


ICS/SCADA are not secure at all

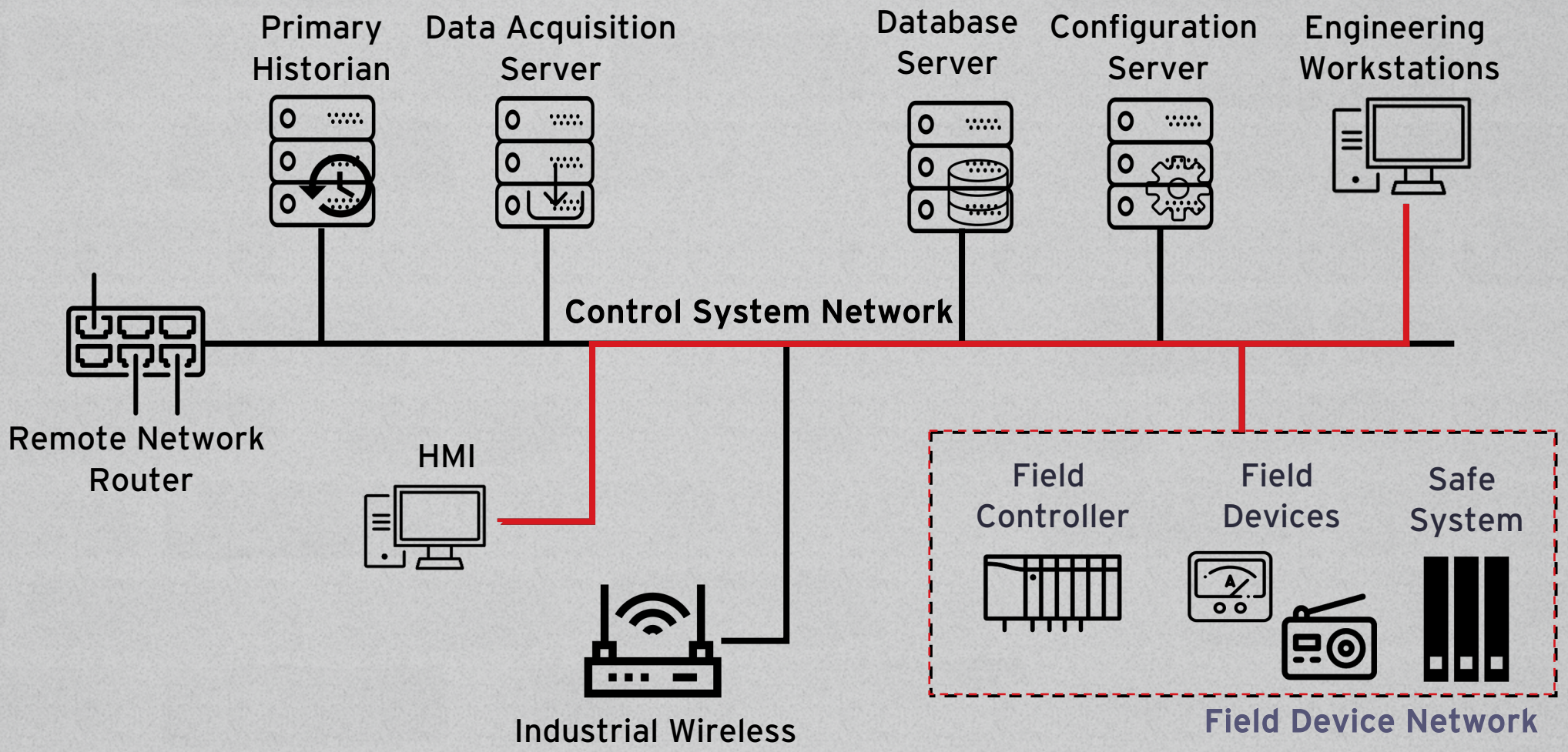
Critical

txOne networks

ICS Protocols



Common ICS Architecture



Critical Infrastructure Sectors (Taiwan)

High-Tech Park

Energy

Traffic

Communications

Government

Medical

Water

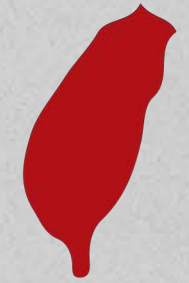
Finance

Critical Infrastructure Sectors (Taiwan)

High-Tech Park

Energy

Traffic



Communications

Government

Medical

Water

Finance

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

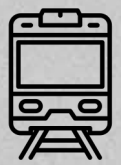
Gas

Water

Information and communication

Medical

Electric power supply



Railway

Chemical

Credit card

Government and administrative

Petroleum

Logistics

txOne networks

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

txOne networks

ICS Protocols and Critical Infrastructure Sectors (US)

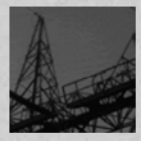
Chemical

Commercial Facilities

Communications

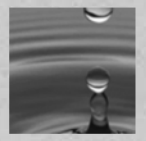
Critical Manufacturing

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

txOne networks

ICS Protocols and Critical Infrastructure Sectors (US)

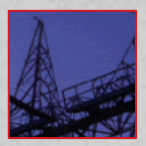
Chemical

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

txOne networks


Public and Private: ICS Network Protocols
txOne networks

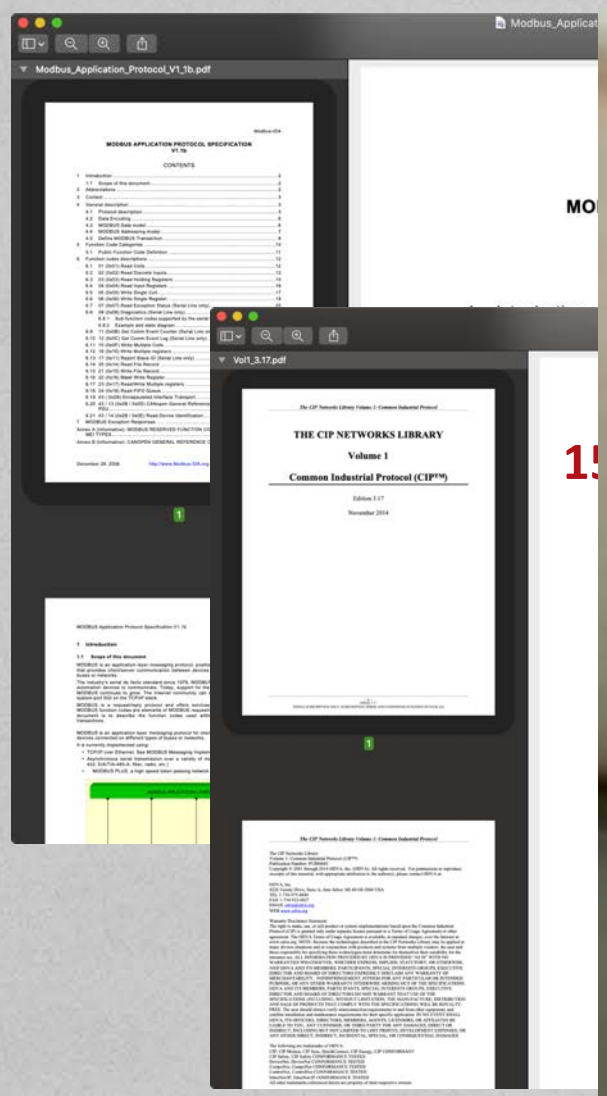
Why Public vs. Private Protocols?

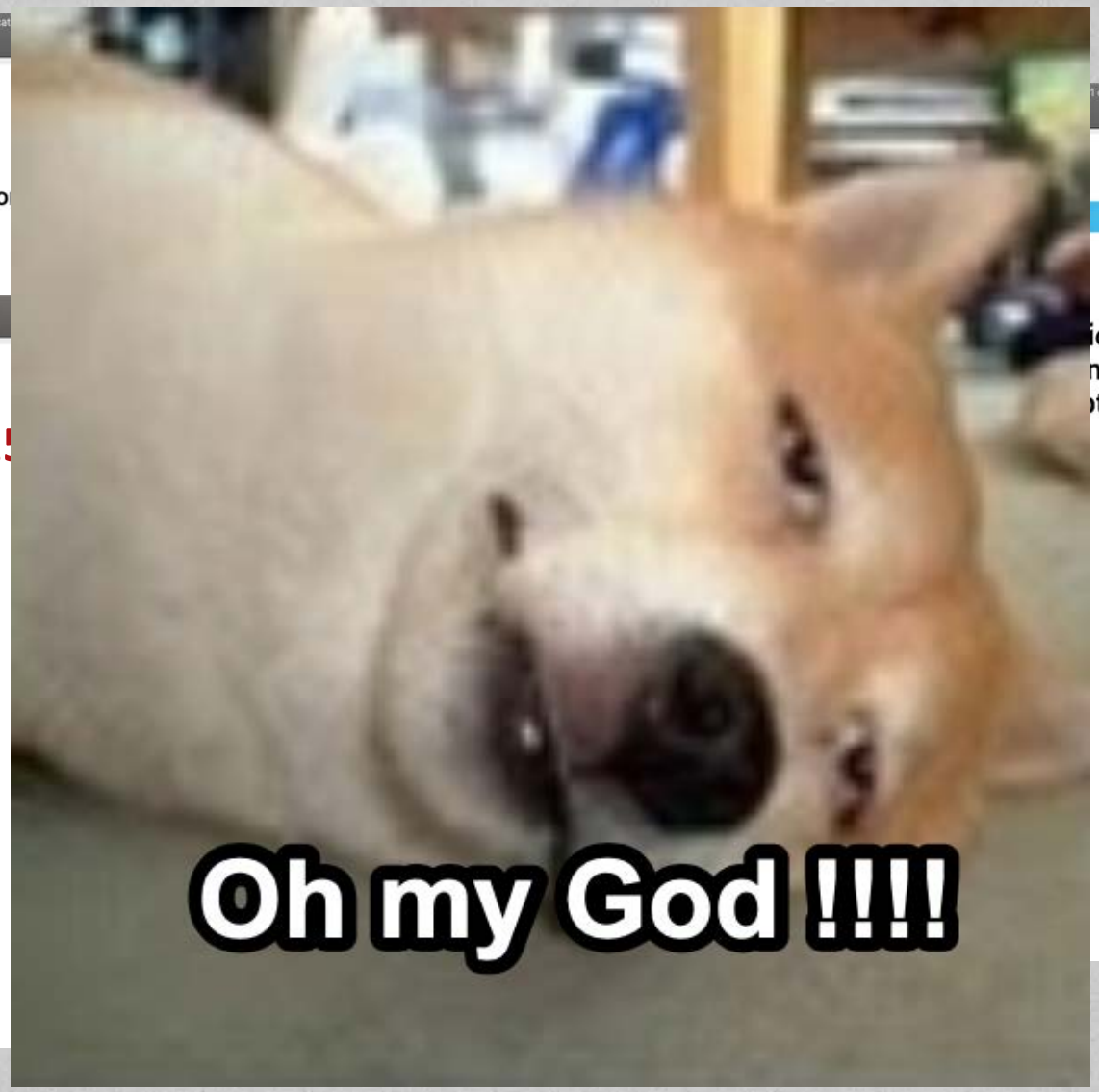
Public

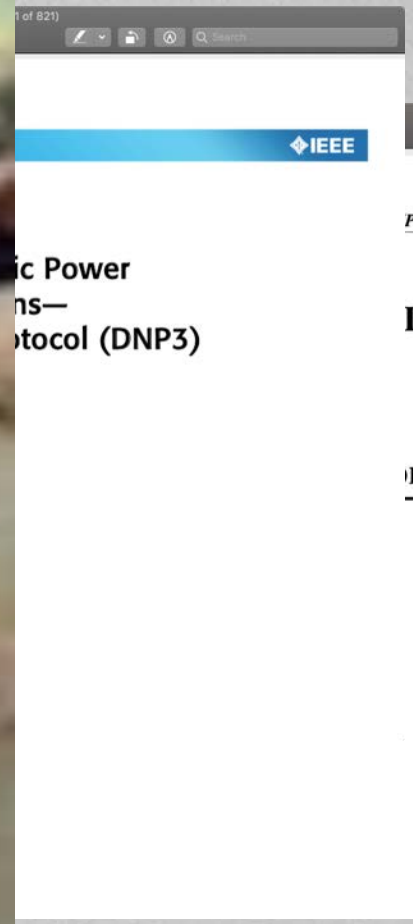
Private

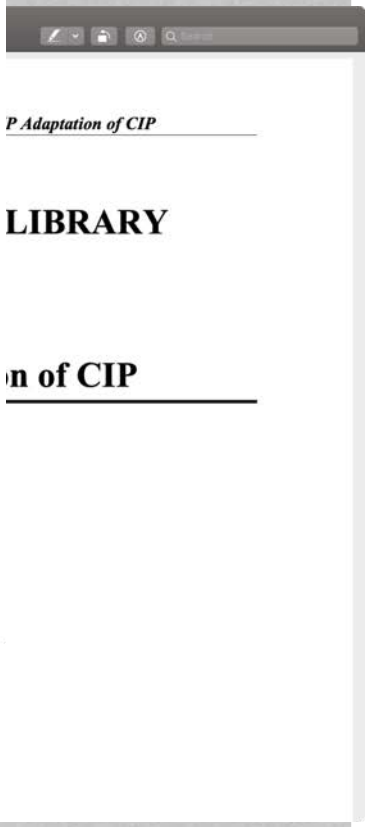
txOne networks

The Specification of Public Protocols



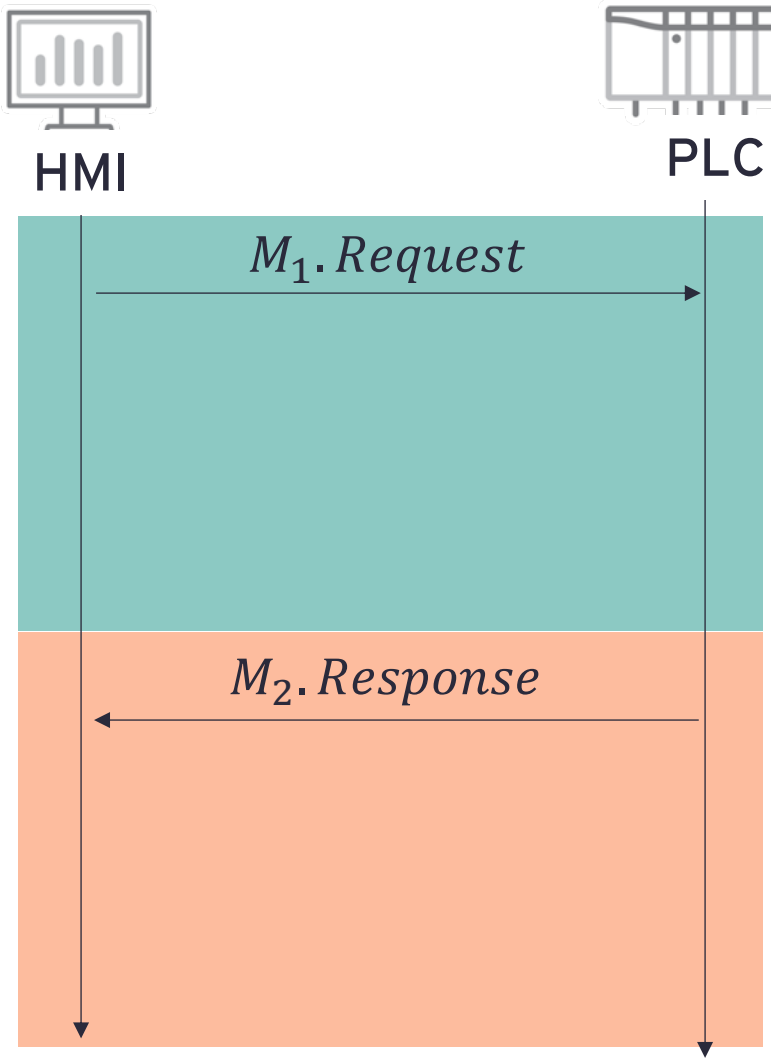




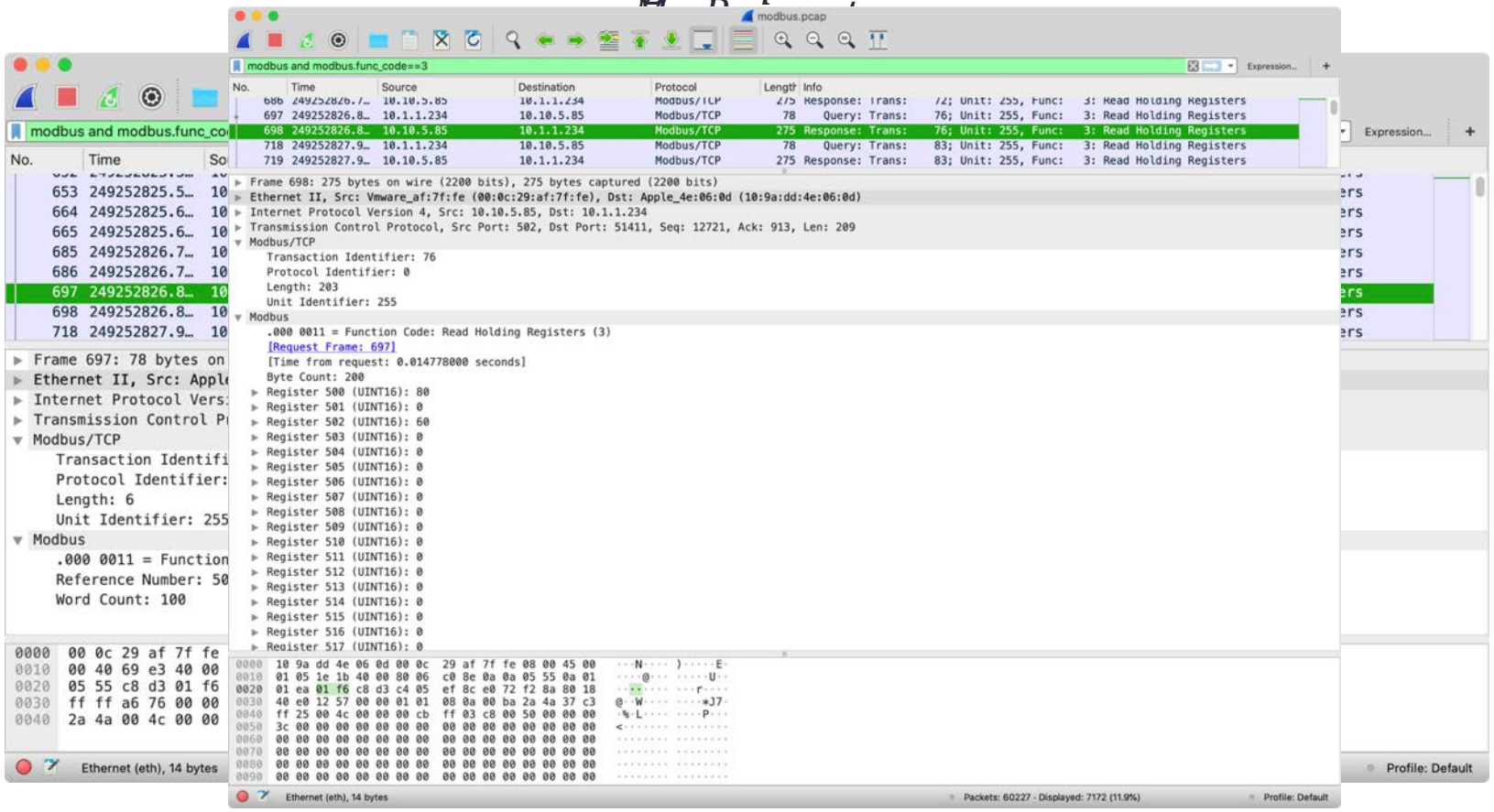


txOne networks

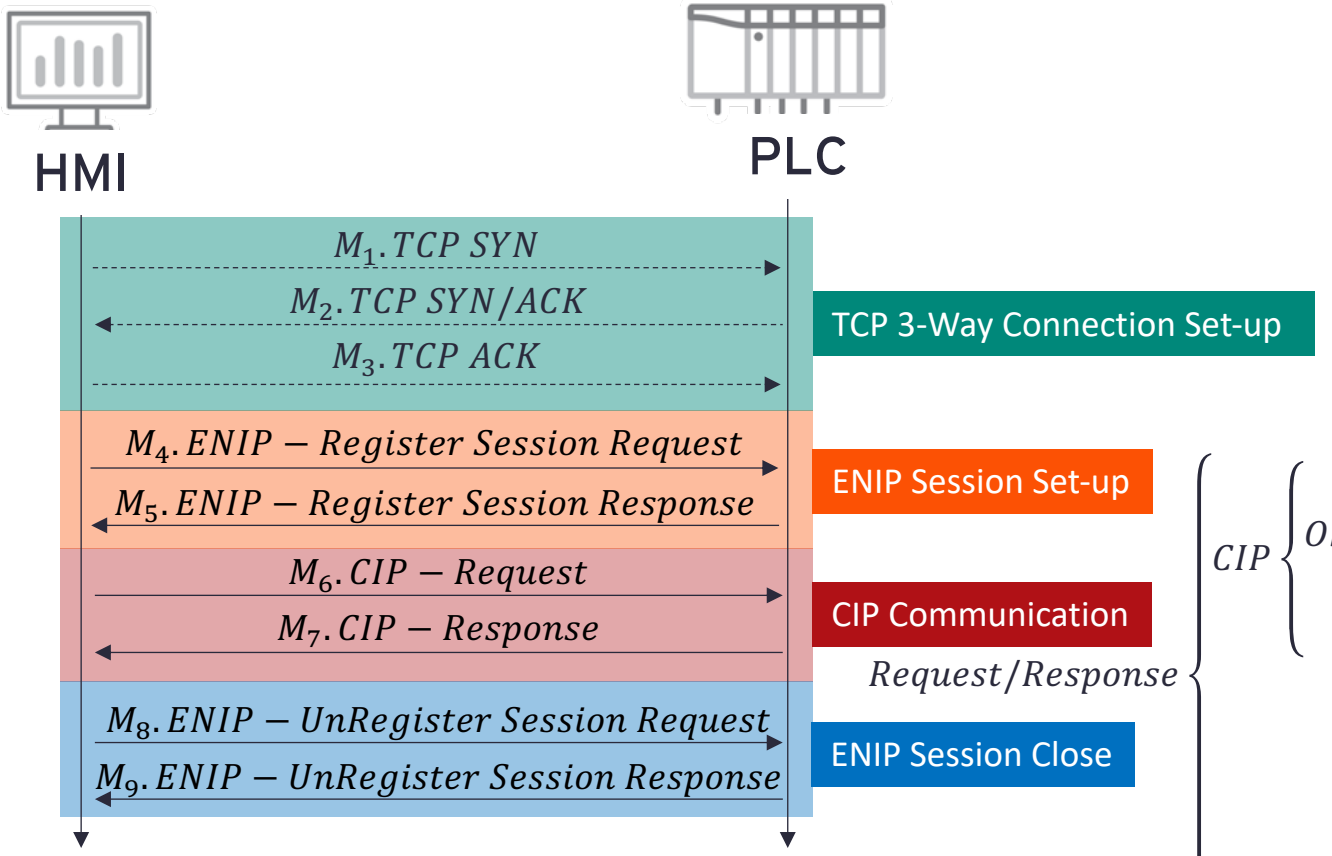
Modbus/TCP Handshake Process



$M_2.Response$



EtherNet/IP CIP Handshake Process



$$Request/Response\begin{cases} EtherNet/IP\begin{cases} Encapsulation\ Header \\ Command\ Specific\ Data \end{cases} \\ TCP/UDP \\ IP \\ Ethernet \end{cases}$$

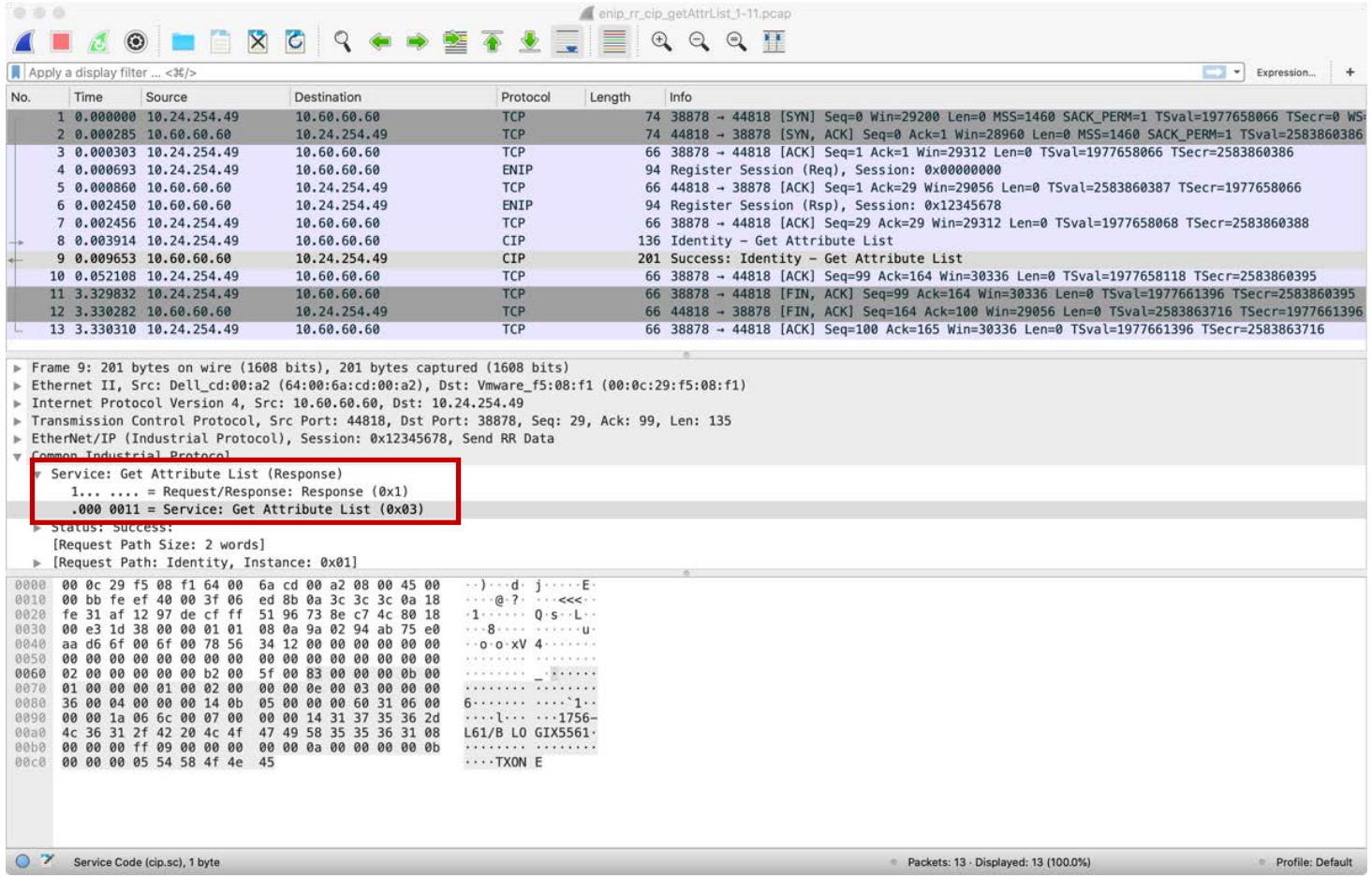
$$Request/Response\begin{cases} CIP\begin{cases} CIP\ Motion|\ Motion\ Control\ |Semiconductor\ Profiles \\ Object\ Library\ (Communication, Applications, Time\ Synchronization) \\ Data\ Management\ Services\ Explicit\ and\ I/O\ Messages \\ Connection\ Management, Routing \end{cases} \\ EtherNet/IP\begin{cases} Encapsulation\ Header \\ Command\ Specific\ Data \end{cases} \\ TCP/UDP \\ IP \\ Ethernet \end{cases}$$

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

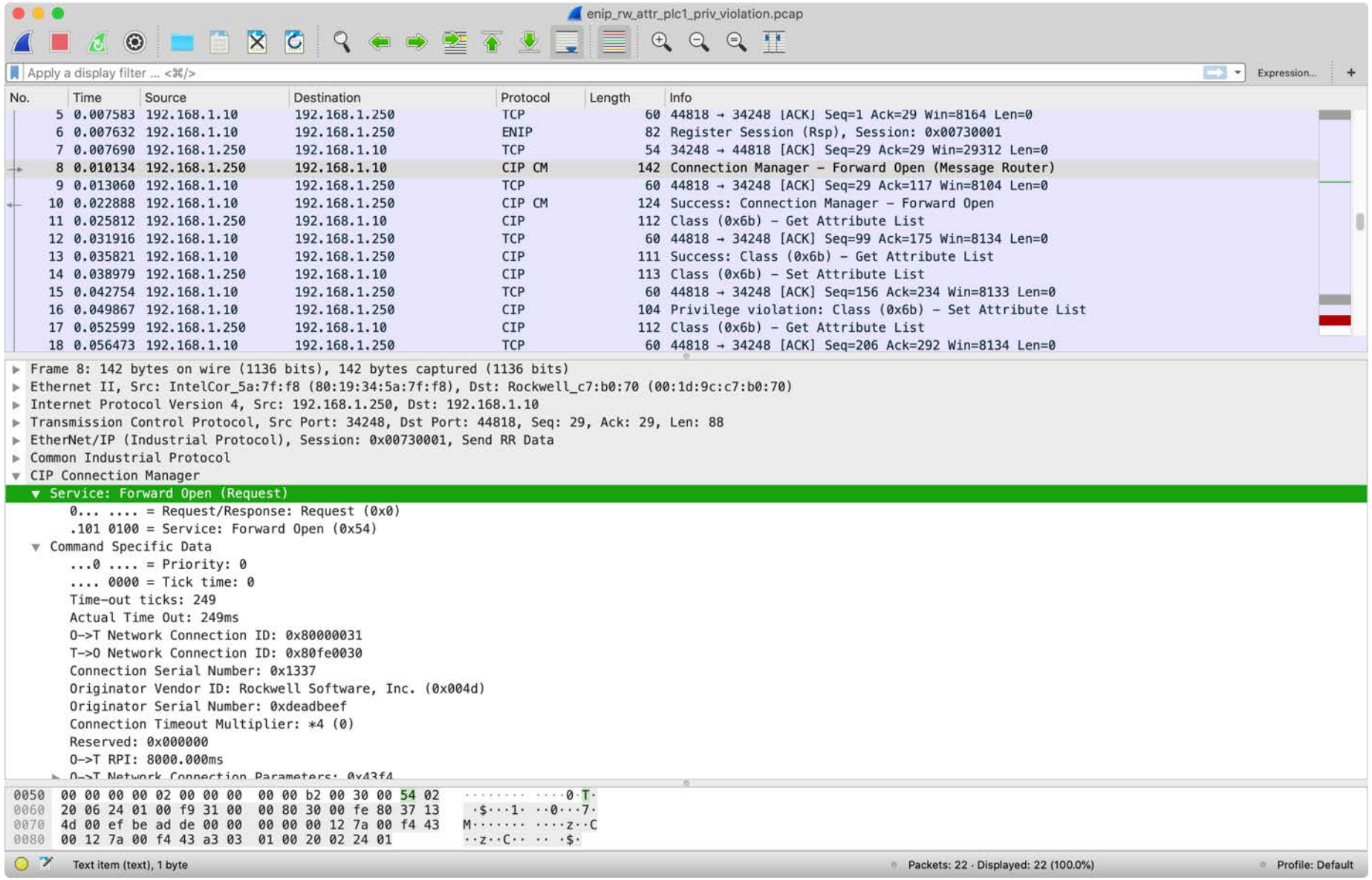
txOne networks

Function Code

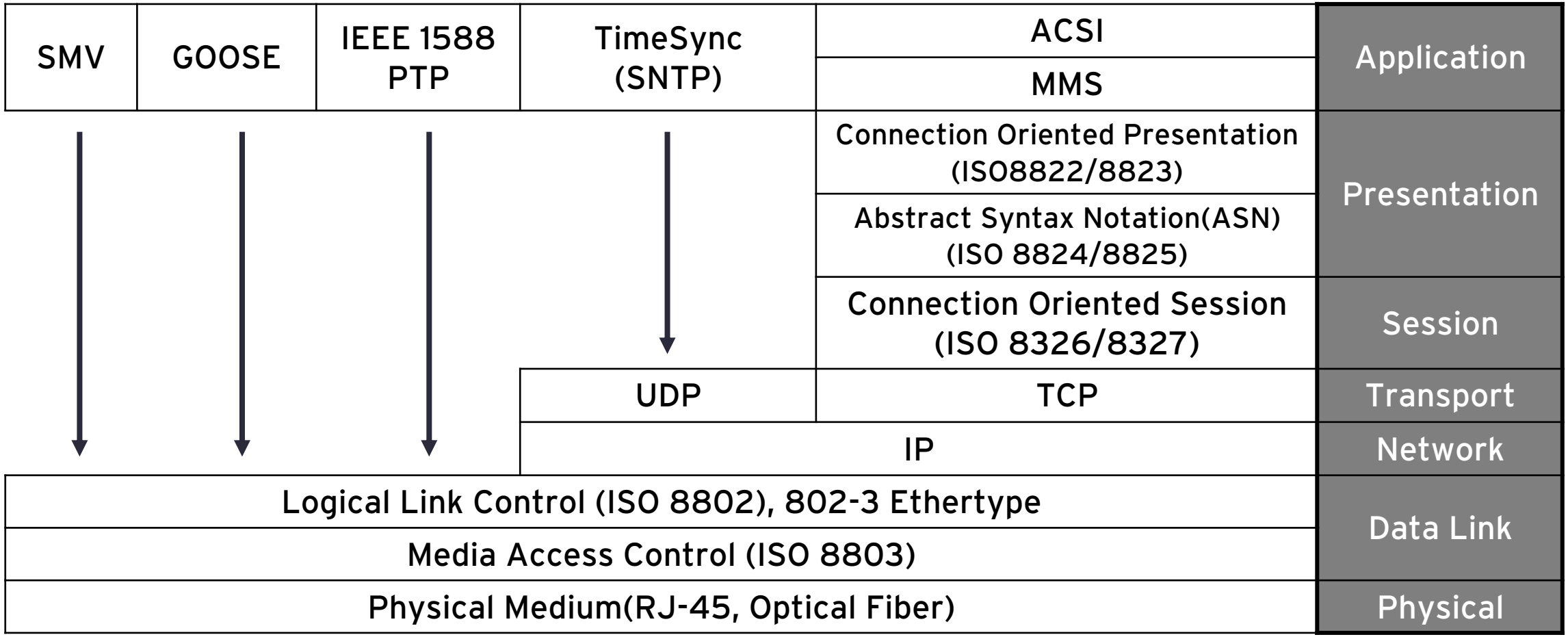
- Get Attributes All 0x01
- Set Attributes All 0x02
- Get Attribute List 0x03
- Set Attribute List 0x04
- Start 0x06
- Stop 0x07



EtherNet/IP Traffic



IEC 61850



IEC 61850 Manufacturing Message Spec (MMS)

HMI

PLC

$M_1.TCP\ SYN$

$M_2.TCP\ SYN/ACK$

$M_3.TCP\ ACK$

TCP 3-Way Co

$M_4.CR\ Connect\ Request$

$M_5.CC\ Coneect\ Confirm$

COTP Connect

$M_6.OSI\ Connect\ Request$

$M_7.OSI\ Accept\ Response$

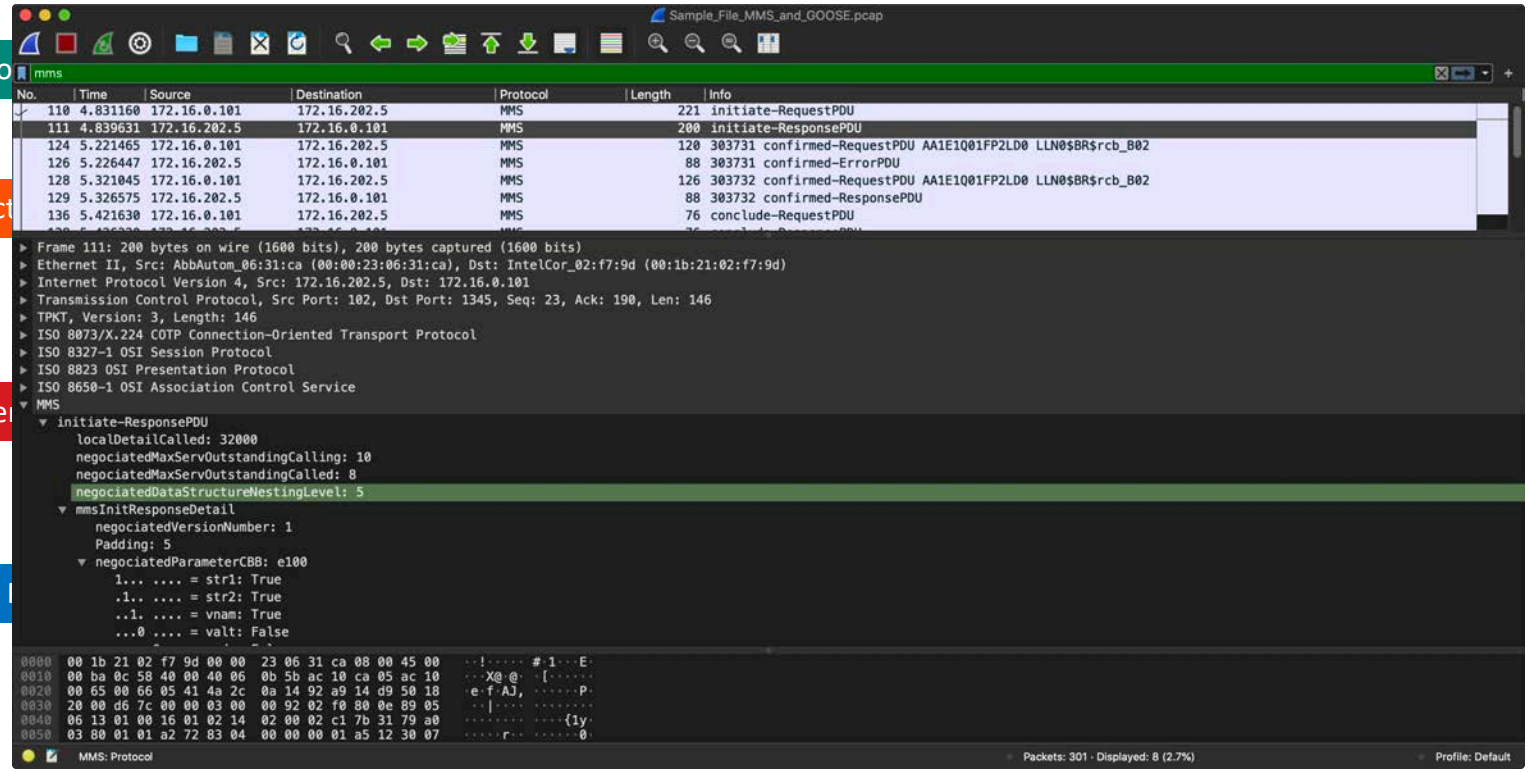
OSI conn-orie

$M_8.MMS\ Request$

$M_9.MMS\ Response$

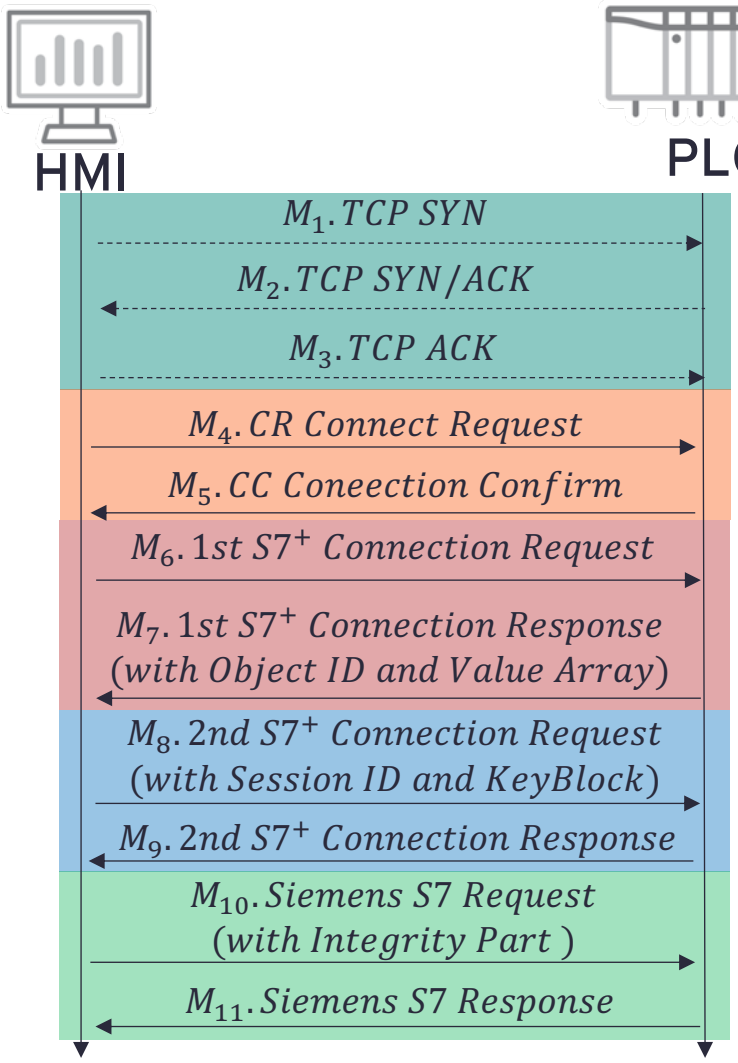
MMS Initiate

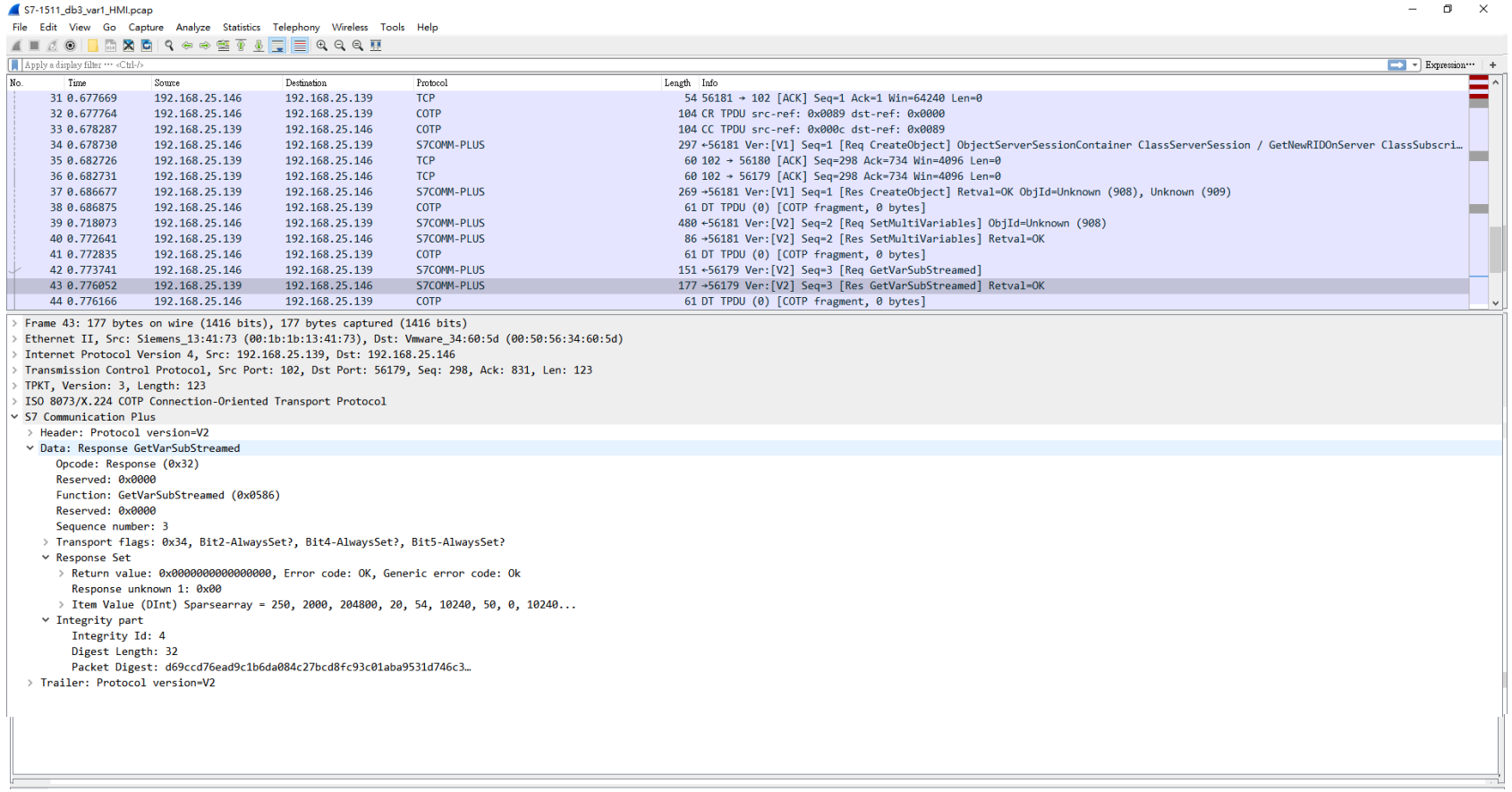
$M_8.MMS\ Response$



txOne networks

Siemens S7 Plus Handshake Process





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: SiemensN_08:e7:db (00:1c:06:
> 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
```

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
S7 Communication Plus
> 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 Integrity part
      Integrity Id: 10
      Digest Length: 32
      Packet Digest: c6bf255aaec1f182c3ee8fe37ca48ac577a008ae3a520112…
> Trailer: Protocol version=V2
```

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
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
```

Common Flaws in ICS Network Protocols

txOne networks

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	✓ (EWS <-> PLC)	✓(HMAC-SHA256)

txOne networks

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	?	✓	?	✓	✓

txOne networks

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

EtherNet/IP CIP(PCCC)

Keyence HMI
10.24.104.11

EtherNet/IP CIP(PCCC)

Allen-Bradley MicroLogix 1400
10.24.104.10

EtherNet/IP CIP

AB Device-NU EP1
10.24.104.12

Infrared length detector

Barometer

Unknown

FATEK HMI
10.24.101.11

Unknown

FATEK FBS-10MCR2-A
10.24.101.10

Modbus/TCP

MOXA E1240
10.24.101.12

Unknown

MOXA MPC-2120 HMI
10.24.101.13

Modbus/TCP

MOXA UC-2100
10.24.101.17

Unknown

MOXA UC-2100
10.24.101.14-16

OMRON FINS/TCP

OMRON HMI
10.24.102.11

OMRON FINS/UDP

OMRON NX102 PLC
10.24.102.10

EtherCAT

Motor ASDA-A2-E
10.24.101.12

Melsec /TCP

Keyence HMI
192.168.3.200

Melsec /UDP

192.168.3.39

Melsec /UDP

Pneumatic valve
M4G/MN4G-T8
192.168.3.250

CC-Link IE Field

Siemens S7

Simatic TP1200-12 HMI
10.24.103.11

Siemens S7+

Simatic S7-1200 PLC
10.24.103.10

Profinet

Temperature module
SRZ COM-ML-4
10.24.103.14

OPC/UA

Keyence HMI
10.24.103.13

Modbus/TCP

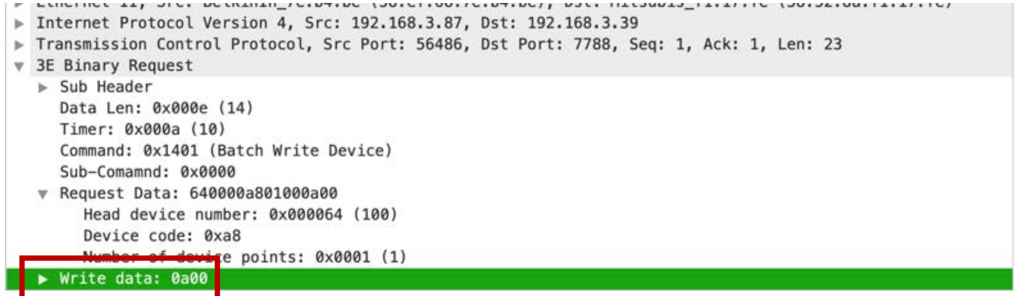
Schneider TM251 PLC
10.24.103.12
10.24.104.20

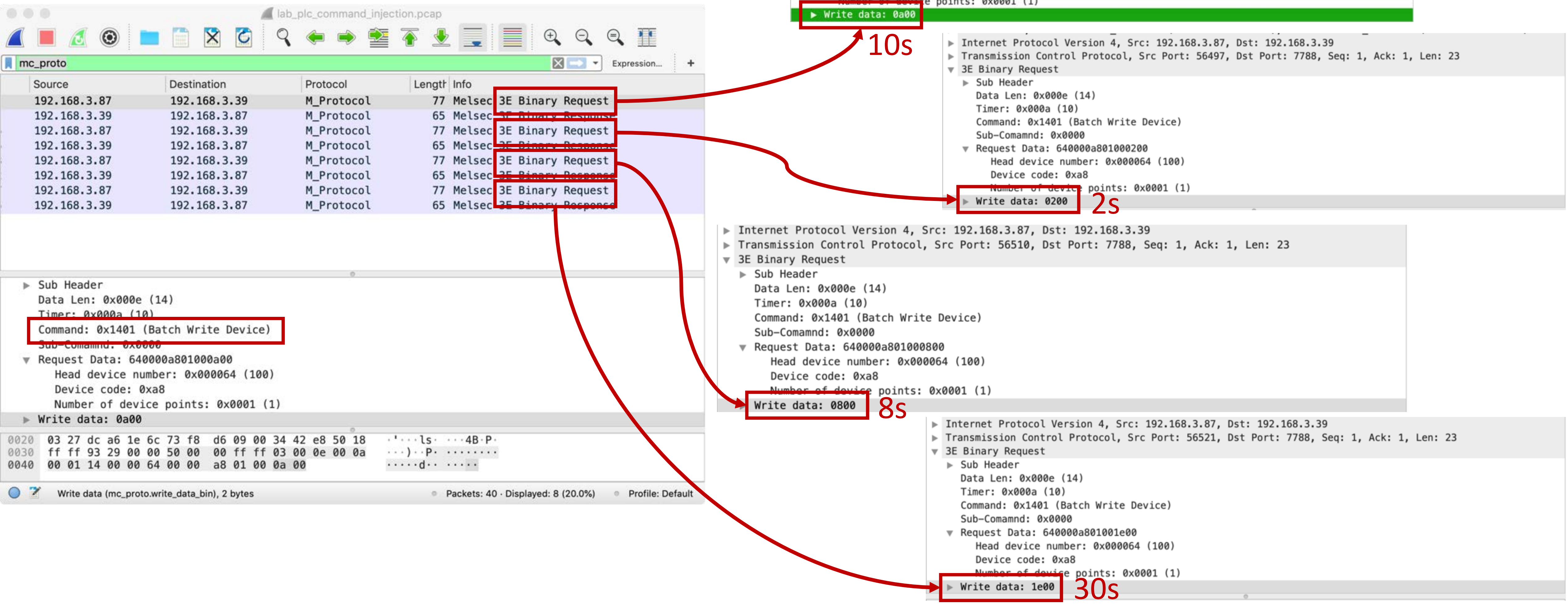
EtherNet/IP CIP

Water flow meter
10.24.104.21

T836-Modify Parameter with Mitsubishi Melsec Protocol

T836-Modify Parameter

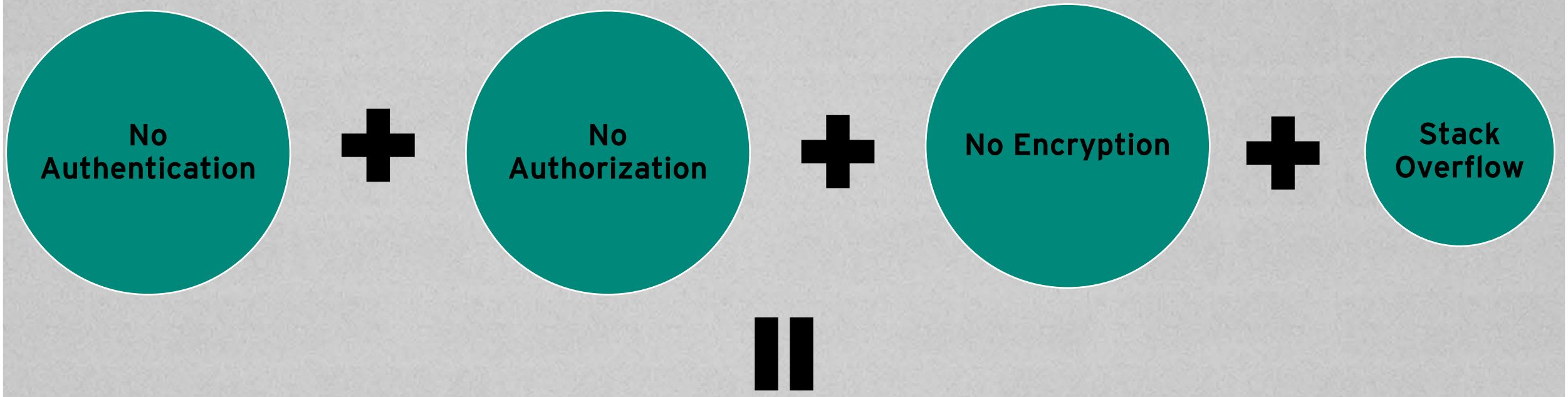




T855-Unauthorized Command Message with OMRON FINS Protocol

T856-Spoof Reporting Message with Modbus/TCP Protocol

Common Flaws in ICS Protocols



T880-Loss of Safety T829-Loss of View T827-Loss of Control T826-Loss of Availability

T815-Denial of View **Impact** T813-Denial of Control

T832-Manipulation of View T831-Manipulation of Control


How to Defend Against ICS Network Protocol Attacks
txOne networks

Suggested Strategies from ICS CERT

Manage authentication
4%

Implement application whitelisting
38%

Implement secure remote access
1%

Monitor and respond
2%

Configuration/patch mgmt.
29%

Build a defendable environment
9%

Reduce your attack surface
17%

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

Implementing FIVE Tactics to prevent 98% incidents

Best Practices for ICS Cyber Threat Resistance

Keep the Operation Running

txOne networks

Network Segmentation Benefits

Risk Mitigation

Prevent Lateral Movement

Outbreak Prevention

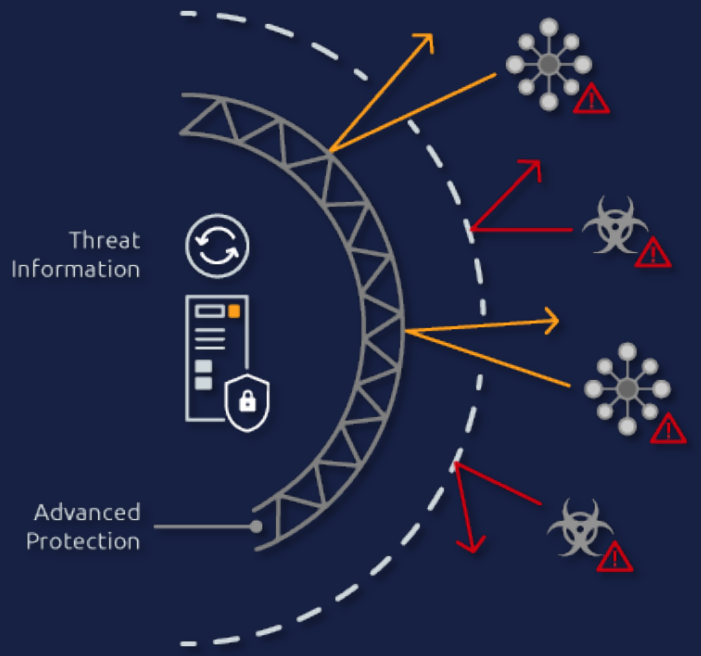
Deal with Massive IoT Adoption

Future Private 5G Connection

Zero Trust Network

txOne networks

Bridge the ICS Vulnerability Gap: Virtual Patching



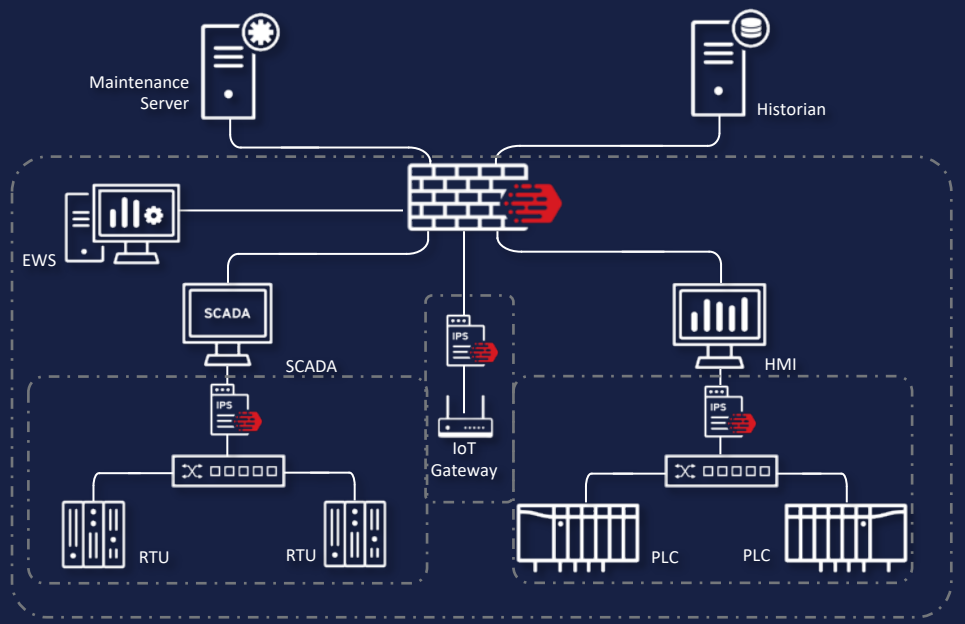
Shield vulnerable assets

Zero-Day Attack Prevention

Maintain Productivity

Patching Process Enhancement

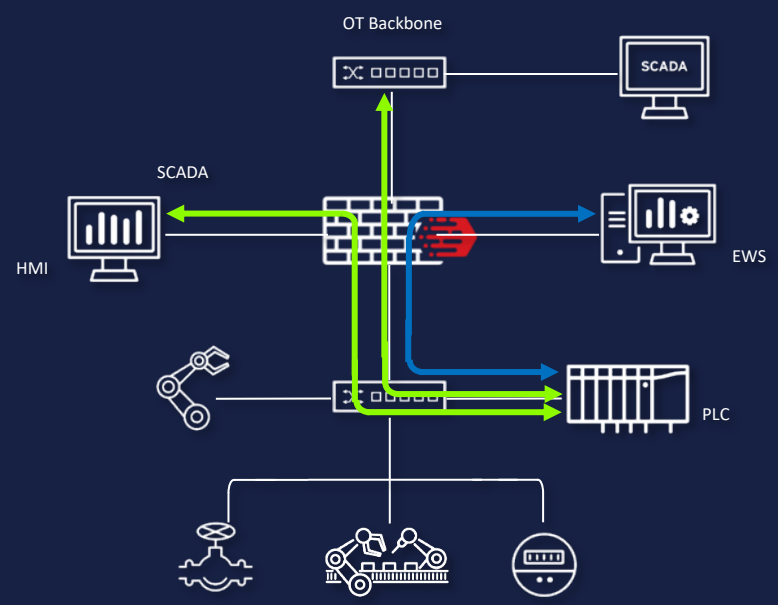
Effective Internal/Micro Segmentation and Shielding with Virtual Patch



- 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

txOne networks

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

txOne networks

Thanks for Listening

Mars Cheng (@marscheng_)
Selmon Yang