Industrial network monitoring with ntopng

Martin Scheu
martin@sichere-industrie.ch
06.February 2021

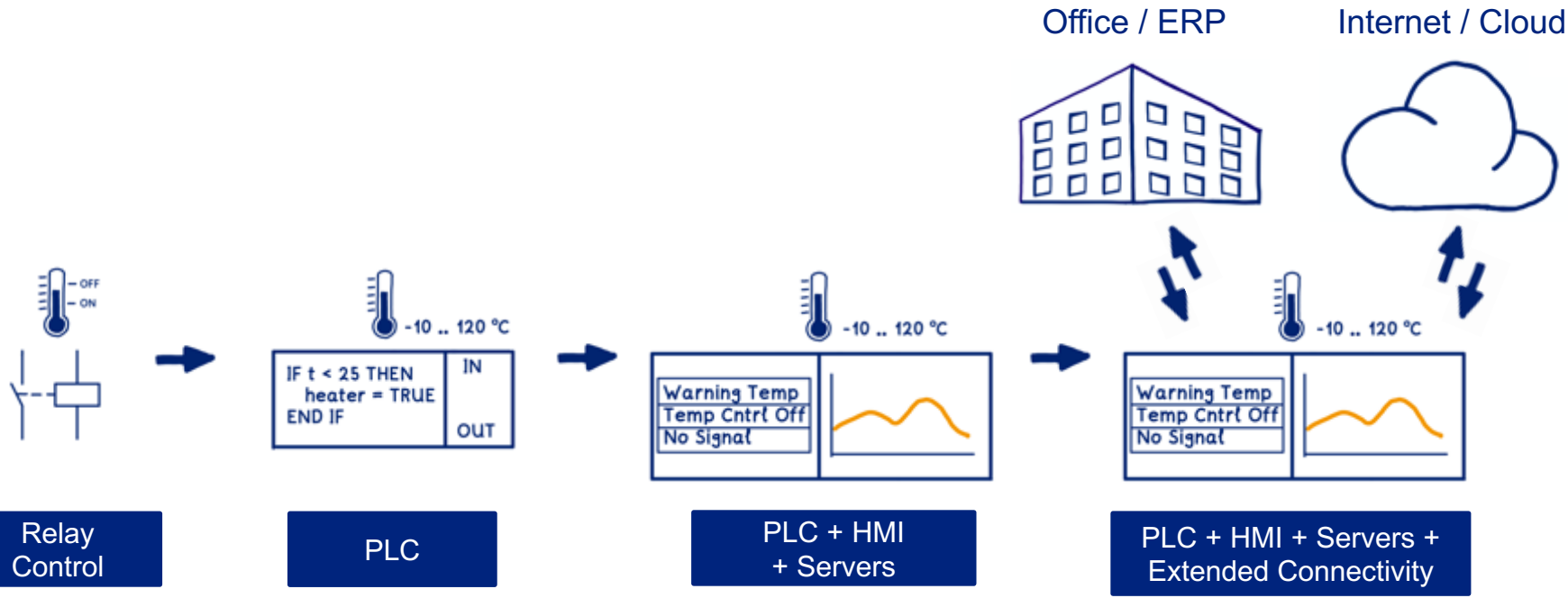
Agenda

- Industrial networks in a nutshell
- Why monitor ICS networks?
- Network and protocols
- Why use ntopng?
- Baselining
- IEC 60870-5-104
- User plugin

ICS	Industrial Control System
SCADA	Supervisory Control And Data Acquisition
OT	Operational Technology

ICS Evolution

”Industrie 4.0”



Relay Control

PLC

PLC + HMI + Servers

PLC + HMI + Servers + Extended Connectivity

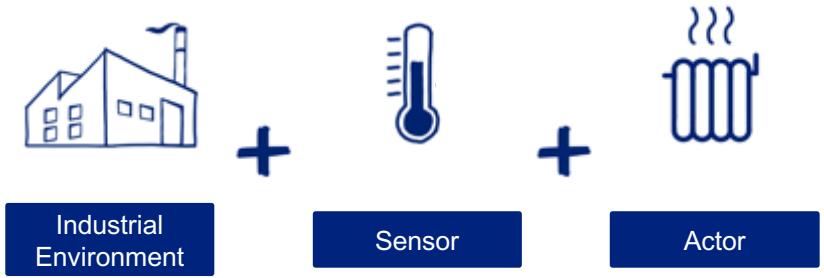
PLC =
Programmable Logic Controller

HMI =
Human Machine Interface

© 2021 Martin Scheu | 4

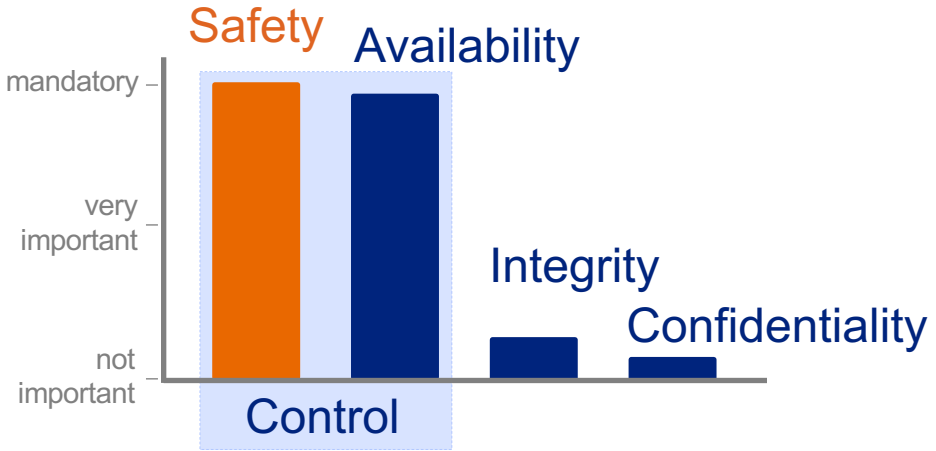
Concept and Objectives

Industrial Control

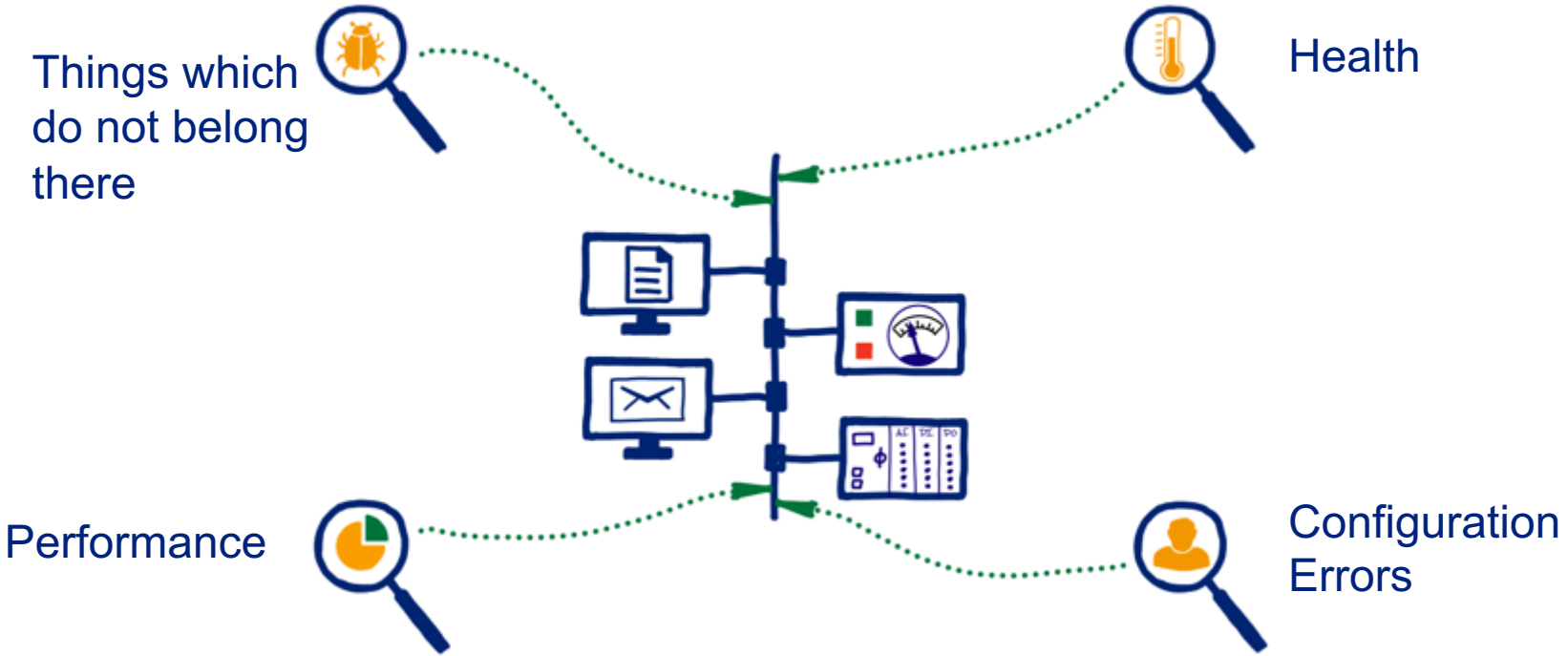


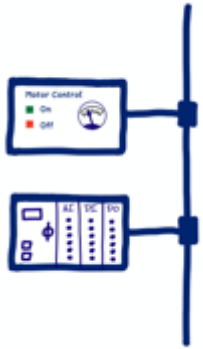
highly deterministic, predicable

Security Objectives - AIC



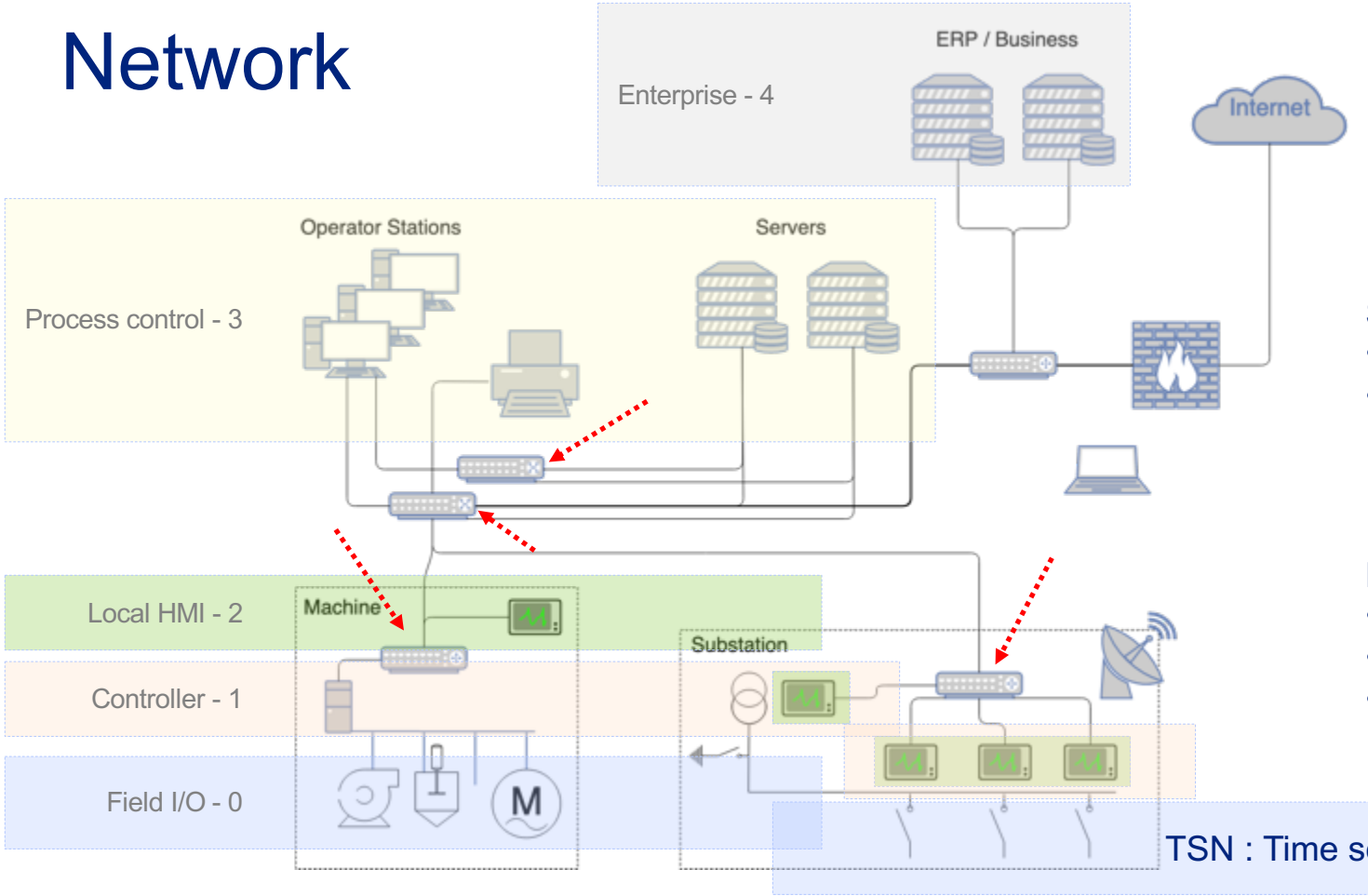
Why monitor ICS networks?





ICS Network and protocols

Network



Standards
- Perdue model
- IEC 62443
  zones and conduits

Keep in mind:
- Device CPU load
- Latency / Jitter
- East - West traffic

TSN : Time sensitive network

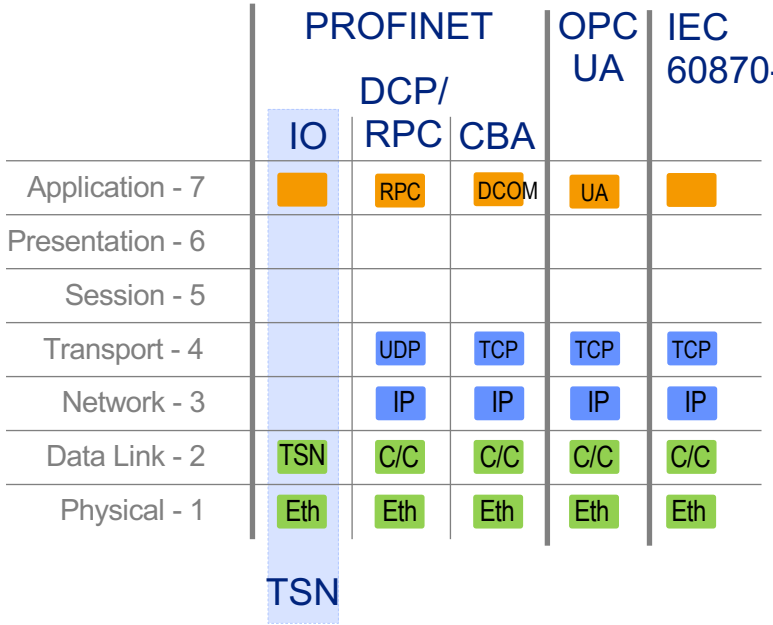
© 2021 Martin Scheu | 8

Fieldbus

2 - wire

- PROFIBUS
- IEC 60870
- Modbus
- CAN
- IO-Link
- HART

Ethernet based



Safety

- ProfiSAFE
- IO-Link Safety

Implemented as “black channel”

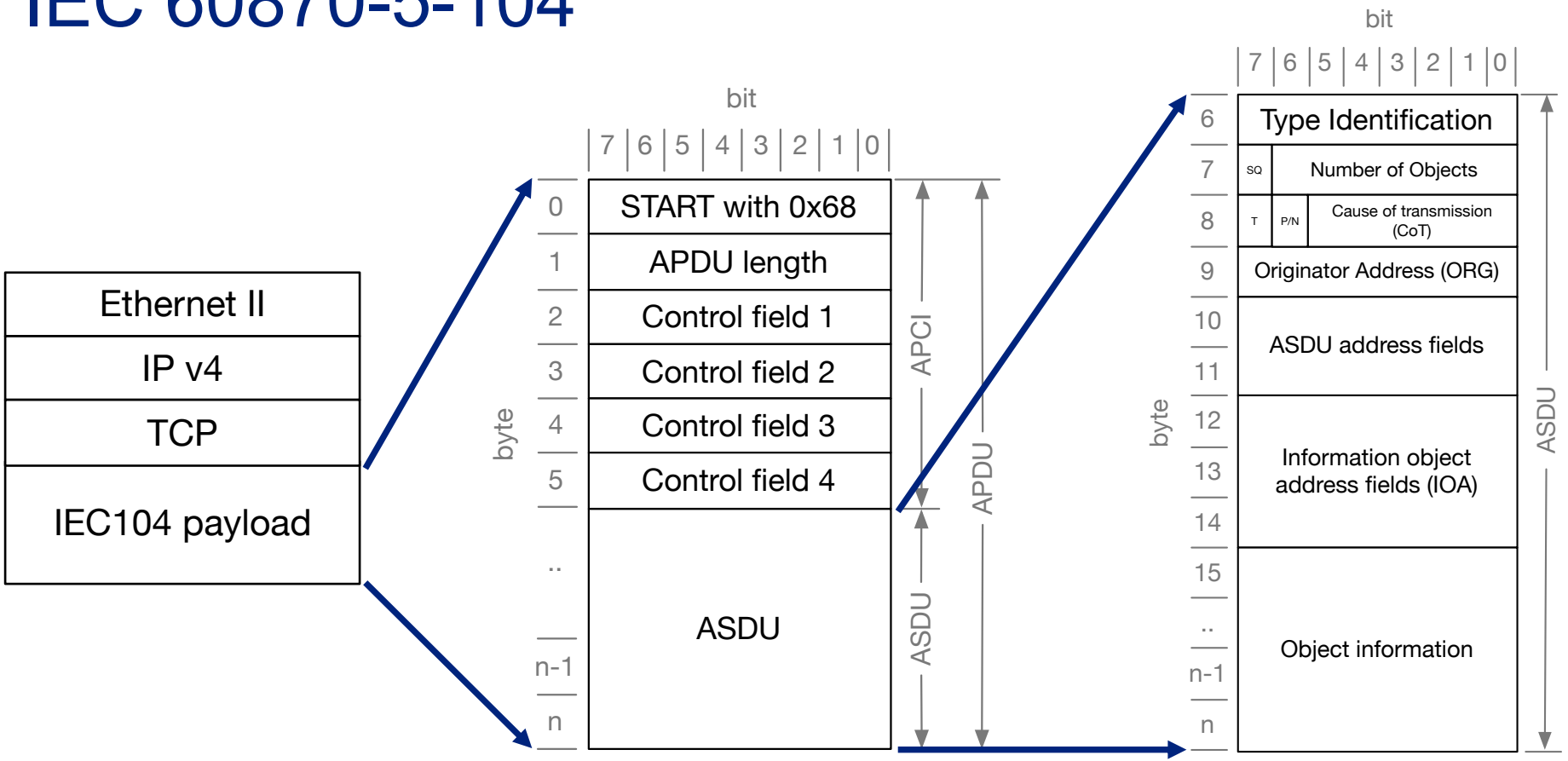
TSN: Time sensitive network

IEC 60870-5-104

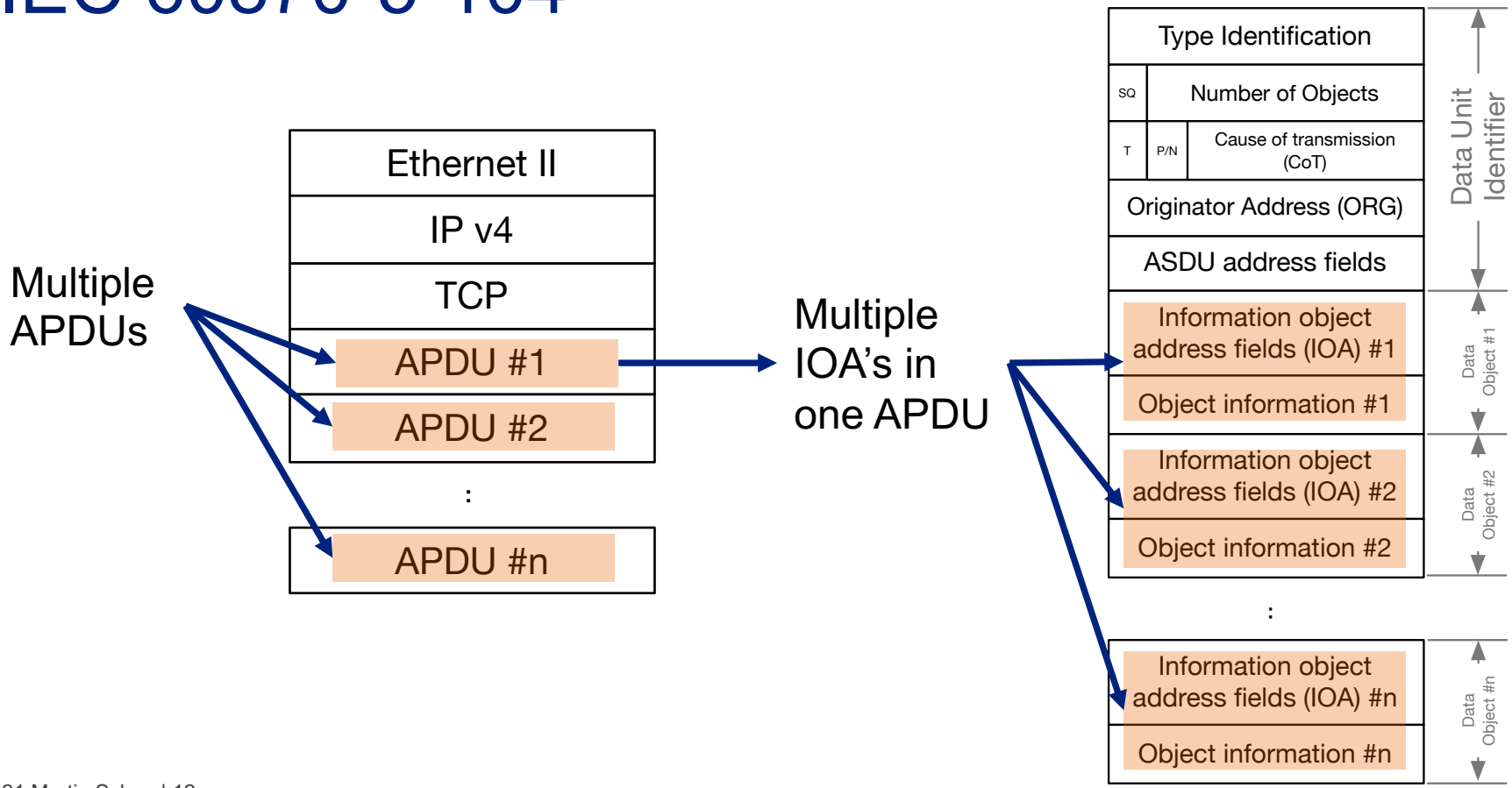
Protocol characteristics:

- Clear text, traditional controller / device protocol, published 1988
- Data exchange: long, single flows, running over days
- Connection check or keep alive communication: short, multiple flows

IEC 60870-5-104



IEC 60870-5-104



why use ntopng?

Open-source network monitoring

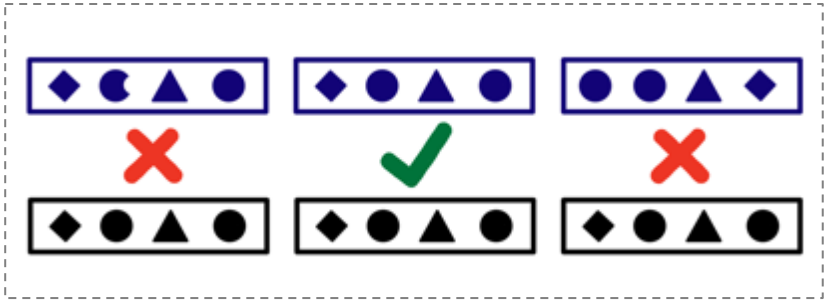
	IEC 104	Script language	Ease of use	Resource requirements	Setup and installation
Malcolm	no	zeek script	-	huge	very complicated
ntop	yes	Lua	+	minimal	easy
Suricata Open Source IDS / IPS /	no	Lua	-	minimal	complicated
SNORT	yes	snort rules	-	minimal	complicated
SOS	no	n/a	+	huge	complicated
zeek	PoC available	zeek script	-	minimal	complicated

Detection mechanism

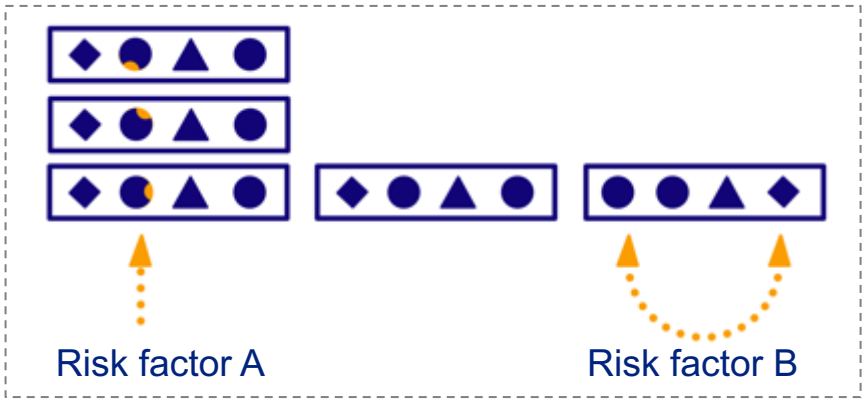
```
alert tcp any any -> any any (msg:"APT.Backdoor.MSIL.SUNBURST";
content:"T "; offset:2; depth:3; content:"Host:";
content:"freescanonline.com"; within:100; sid:77600852; rev:1;)

"detect IEC 104 traffic entering/exiting the network to
$EXTERNAL_NET"
```

Signature based

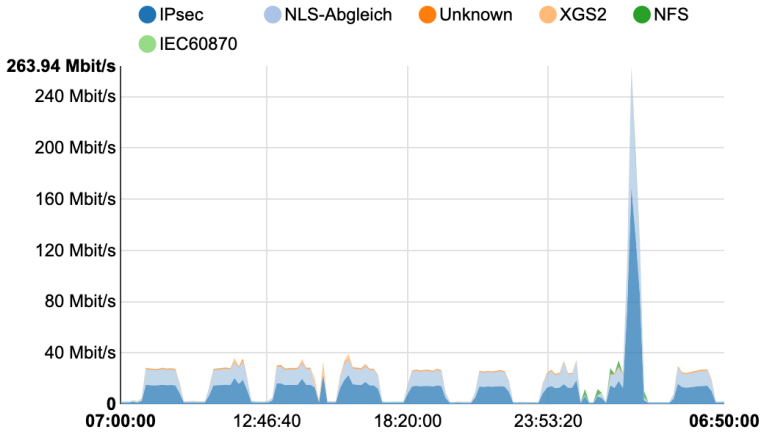


Risk based

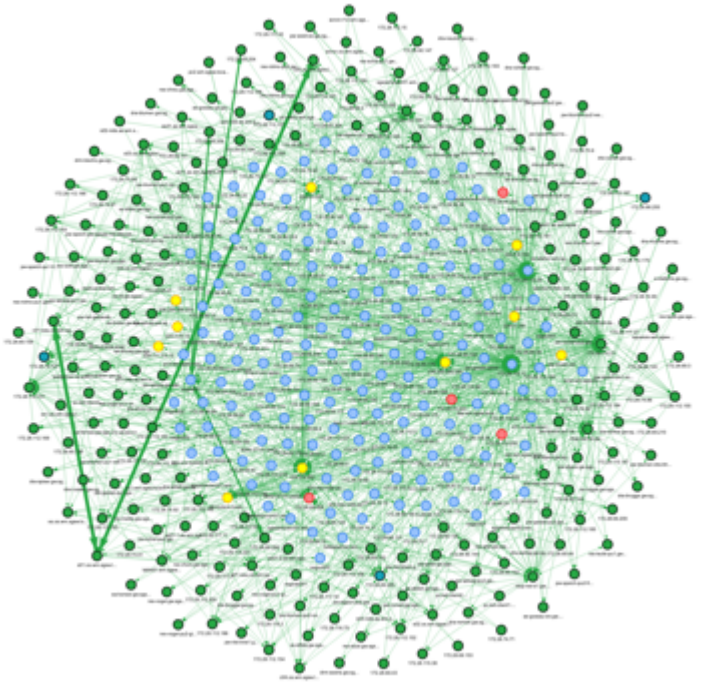


Baselining

or how does normal look like?



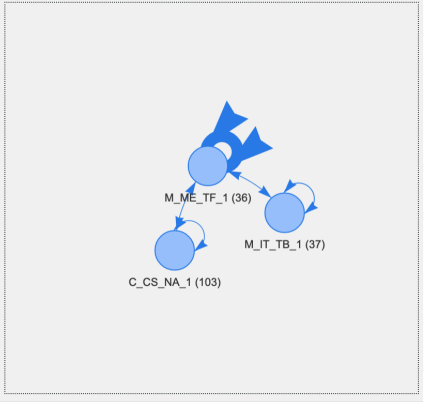
Application	Total Bytes	Percentage
HTTP	881.84 GB	48.0 %
Unknown	374.75 GB	20.4 %
SMBv23	171.28 GB	9.3 %
s7comm	158.66 GB	8.6 %
SSDP	60.94 GB	3.3 %
RDP	59.99 GB	3.3 %
ICMP	28.85 GB	1.6 %
MDNS	27.13 GB	1.5 %
NTP	14.0 GB	0.8 %
IEC60870	12.97 GB	0.7 %



IEC 60870-5-104

Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
IEC60870	TCP	21	[redacted]:2404	[redacted]:44404	14:46		Client Server	0 bps	100.48 KB	<- S, RX 21582
IEC60870	TCP	21	[redacted]:2404	[redacted]:59749	13:32		Client Server	0 bps	53.31 KB	-> I, RX 65, TX 28985
IEC60870	⚠ TCP	21	[redacted]:58463	[redacted]:2404	08:17	30	Client Server	0 bps	8.44 KB	<- S, RX 14
IEC60870	TCP	21	[redacted]:54827	[redacted]:2404	08:27		Client Server	0 bps	12.1 KB	-> U (TESTFR con)

Type ID Transitions

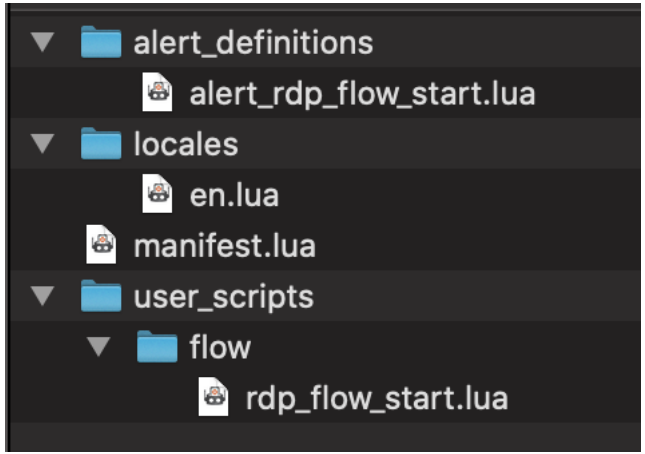


M_ME_TF_1 (36) ⇄ M_ME_TF_1 (36)	98.651 %
M_IT_TB_1 (37) ⇄ M_IT_TB_1 (37)	1.000 %
M_ME_TF_1 (36) → M_IT_TB_1 (37)	0.116 %
M_IT_TB_1 (37) → M_ME_TF_1 (36)	0.116 %
C_CS_NA_1 (103) → M_ME_TF_1 (36)	0.047 %
M_ME_TF_1 (36) → C_CS_NA_1 (103)	0.047 %
C_CS_NA_1 (103) ⇄ C_CS_NA_1 (103)	0.023 %

Alarm Typ	Score	Applikation	Beschreibung	Actions
! Invalid IEC Transition	50	IEC60870	Invalid transition detected [M_ME_NB_1 (11) -> C_CS_NA_1 (103)] [Flow: [redacted] Lokaler Host :2404 ⇄ [redacted] Lokaler Host :22525] [TCP] [Applikation: IEC60870] [Info: IEC60870]	

Type I-S Ack Latency (Average / Std Dev)	0.160 ms (0.474 msec)
Messages Breakdown	83.9% / 16.1%
Messages Lost / Retransmissions	← 0, → 18 / 1 Retransmitted

User plugin




```
function script.hooks.protocolDetected(now)

   local appProtoID = flow.getnDPIAppProtoId()

   --RDP      ID 88

   if appProtoID == 88 then

    local line5tuple = shortFlowLabel(flow.getInfo())

    local line =  line5tupletime .. " -RDP flow started"

    print(line)
    log:write(line)
    flow.setCustomInfo("Flow logged")

    local cli_score, srv_score, flow_score = 0, 0, 0
    local alert =alert_consts.alert_types.alert_rdp_flow_s
        "Flow A Info",
        "Flow B Info"
     )

     alert:set_severity(alert_severities.warning)
     alert:trigger_status(cli_score, srv_score, flow_score
```

General use cases

- Unusual or exceptional activities in a network
- Connection of a new device, disconnection of a device
- Rogue DHCP, DNS, SMTP or NTP server
- Data packets from an unknown device
- Data transmission between devices that have not previously communicated
- Data transmission via a protocol / port that has not been used before
- Data transmission via an unusual protocol or one not intended for the purpose at hand
- Events that occur at unusual times
- Use of unexpected addresses (public IP addresses, etc.)
- Generally noteworthy events such as address or port scans
- Changes in network quality, including high broadband usage, increased round-trip times and smaller TCP window sizes

© 2021 Martin Scheu

Source [3]: allianz-fuer-cybersicherheit.de

Use cases ICS protocol specific

- ❑ Unusual error messages
- ❑ Unsupported function calls
- ❑ Function calls that have not been used before
- ❑ Flawed data packets
- ❑ Unknown function codes
- ❑ Abnormal protocol behaviour
- ❑ Unexpected transition from one protocol to another

requires DPI and ICS protocol understanding

- ❑ Values outside of defined ranges
- ❑ Changes in frequency / periodicity
- ❑ Changes in cycle times
- ❑ Changing variance within certain periods of time

ICS or network monitoring?

© 2021 Martin Scheu | 20

Source [1]: allianz-fuer-cybersicherheit.de

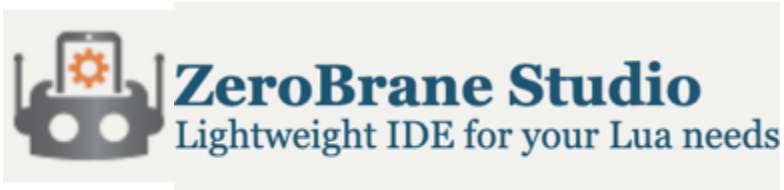
Give it a try!

Tooling

ntopng

https://packages.ntop.org/

https://www.wireshark.org/



https://studio.zerobrane.com/

Sources

Picture / Information	Link
[1]	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_134.html?nn=6656412
IEC 60870-5-104	https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard/
IEC 60870-5-104	https://www.uni-muenster.de/imperia/md/content/informatik/agremke/comparison_of_scada_protocols_and_implementation_of_iec_104_and_mqtt_in_mosaik.pdf
IEC 60870-5-104	https://infosys.beckhoff.com/english.php?content=../content/1033/tcplclibiec870_5_104/html/tcplclibiec870_5_104_telegrammstructure.htm&id=