IoT en TSN,
de volgende veiligheidsuitdaging?

Kurt van Buul
kvb@hms-networks.com

28-09-2023

E&A ELECTRONICS & APPLICATIONS '23

26 T/M 28
SEPTEMBER '23
JAARBEURS UTRECHT

HMS at a glance

+9,000,000
devices connected

+400,000
machines connected to cloud systems

Our field:
Industrial ICT
(Information and Communication Technlogy)

5G
Smart Grid
AI
IoT
Wireless

Head office in
Halmstad, Sweden

750
employees worldwide

Offices in
17 countries

Partners in over **50**

2022 sales
2,506 MSEK
(225 M EUR, 245 M USD)

2025

±0
Net positive in CO_2 emissions

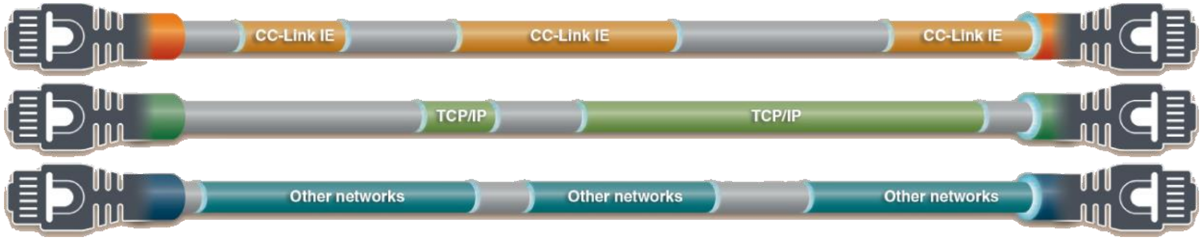
+30%
Staff NPS
Customer NPS

TSN

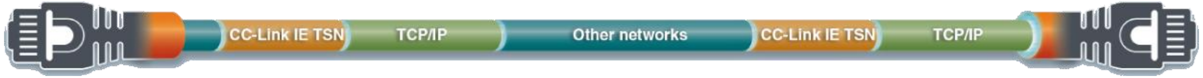
Set-up and Actual situation

Time-sensitive Networking

TSN Principle



Mixing different and real-time protocols into one

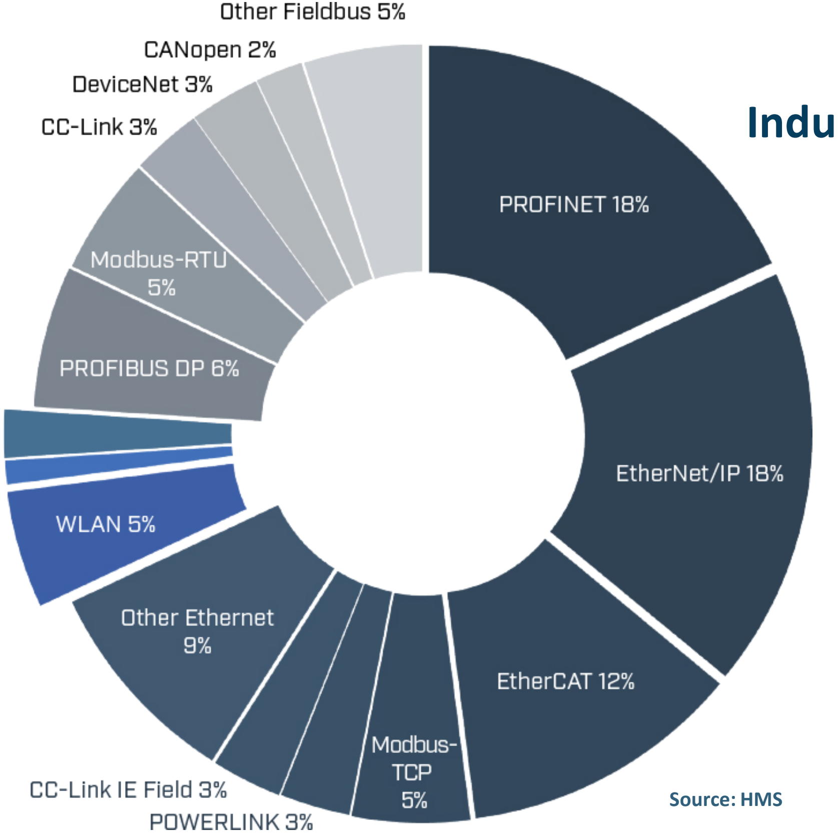


Source: Mitsubishi Electric

TSN is a set of standards to combine streams, not a new protocol!

Industrial Ethernet

Industrial network shares 2023



Industrial Ethernet 68% [66%]

Annual growth: +10%

Fieldbus 24% [27%]

Annual growth -5%

Wireless 8% [7%]

Annual growth +22%

Source: HMS

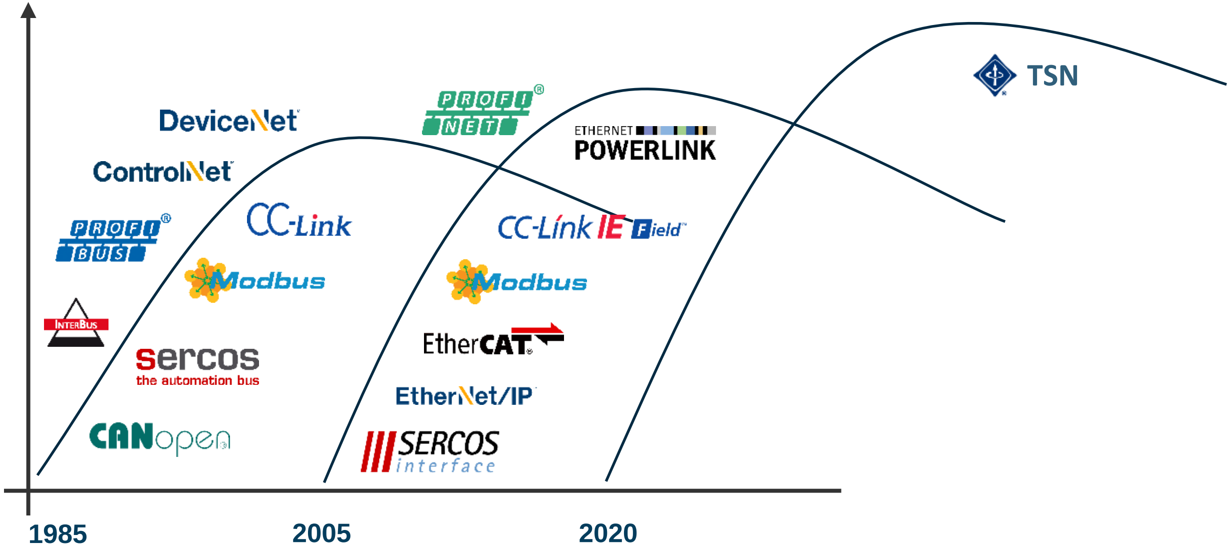
Time-sensitive Networking

The next networking wave

Gen I
Different PHY's
Different L2's
Max 1 Mbs

Gen II
Standard PHY
Different L2's
100 Mbs

Gen III
Standard PHY
Standard L2
100 / 1.000 / 10.000 Mbs



Time-sensitive Networking – Actual status

Profinet

- Standard published
- No PLC’s yet
- Multi-vendor demo’s

EtherNet/IP

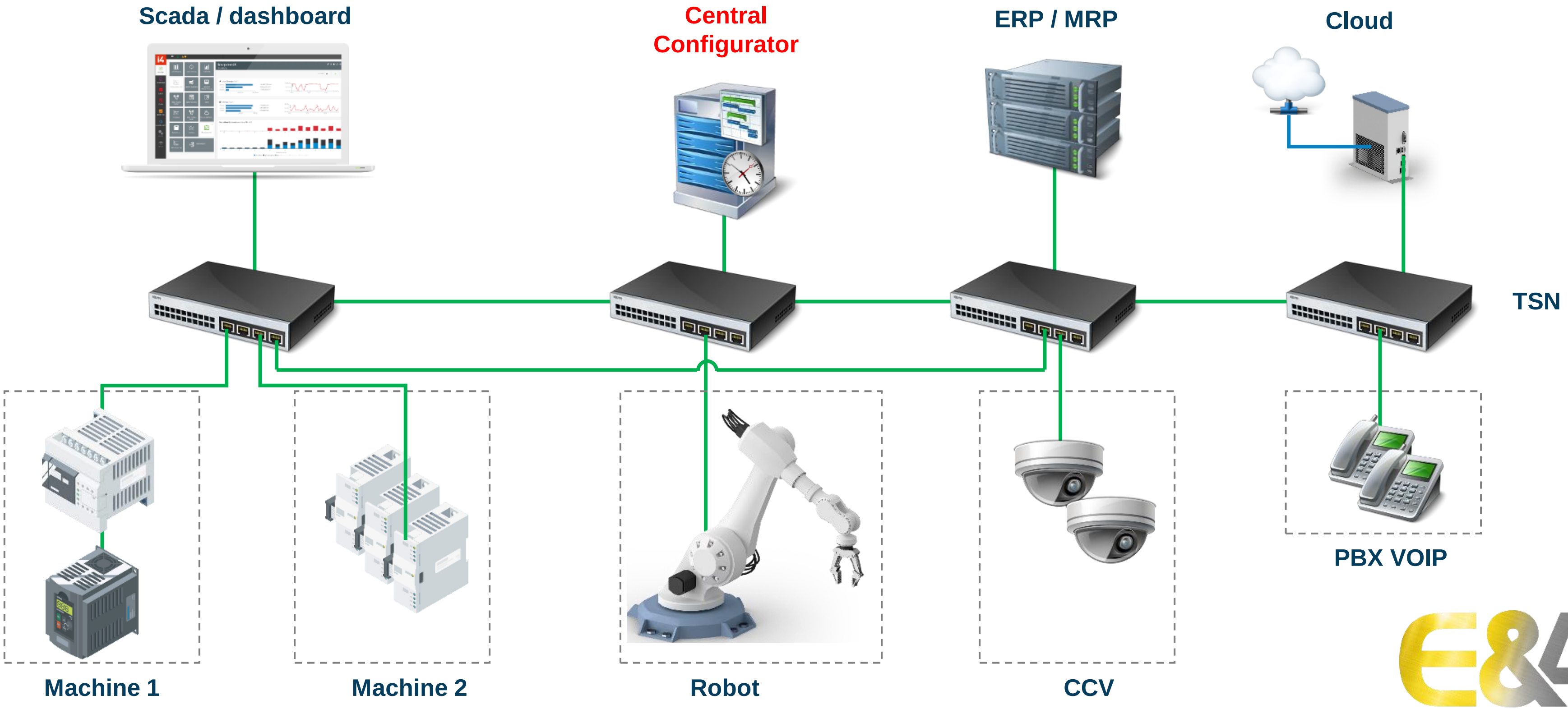
- No standard yet
- No PLC’s yet
- Unclear commitment

CC Link IE Field

- Standard published
- PLC’s on the market
- Slave node’s available

Time-sensitive Networking

Network Topology

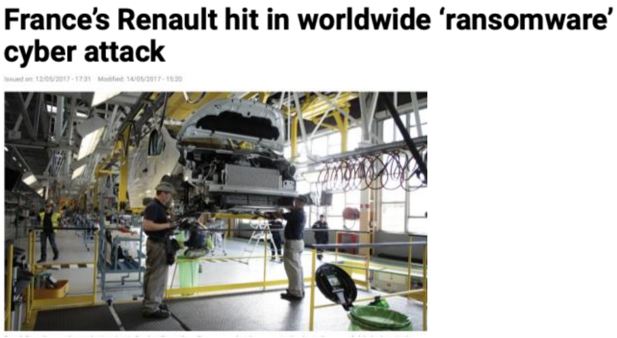


Status of CyberSecurity in Manufacturing

It’s not looking bright…

Status of Cyber Security

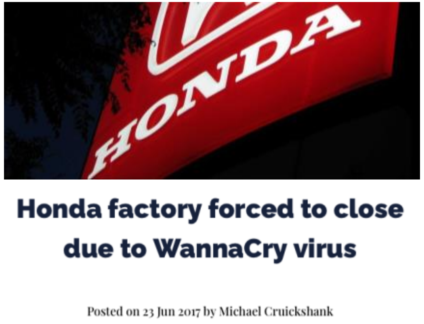
Attacks to manufactures


France’s Renault hit in worldwide ‘ransomware’ cyber attack

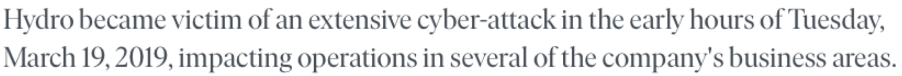
Issued on: 12/05/2017 - 17:31 Modified: 14/05/2017 - 15:20

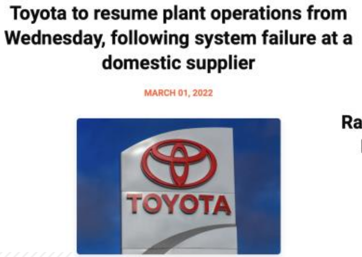
February 17th, 2023

Semiconductor industry giant says ransomware attack on supplier will cost it $250 million

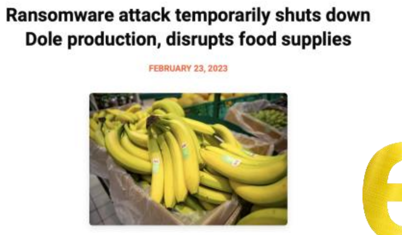

Honda factory forced to close due to WannaCry virus

Posted on 23 Jun 2017 by Michael Cruickshank

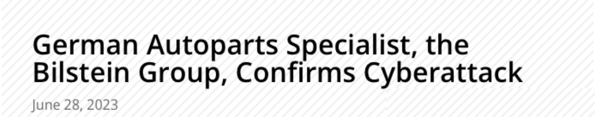

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, 2019, impacting operations in several of the company's business areas.


Toyota to resume plant operations from Wednesday, following system failure at a domestic supplier

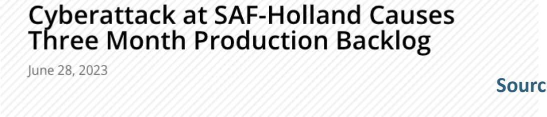
MARCH 01, 2022


Ransomware attack temporarily shuts down Dole production, disrupts food supplies

FEBRUARY 23, 2023


German Autoparts Specialist, the Bilstein Group, Confirms Cyberattack

June 28, 2023


Cyberattack at SAF-Holland Causes Three Month Production Backlog

June 28, 2023

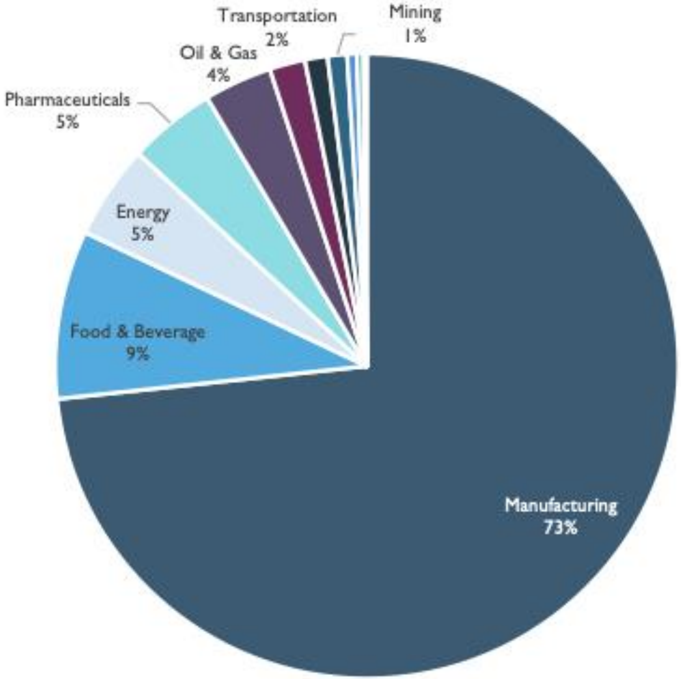
Source: NCC Group 07-2023

Status of Cyber Security

Ransomware is the biggest problem….

73% Manufacturing

Downtime costs big €€€



Source: DRAGOS

Status of Cyber Security

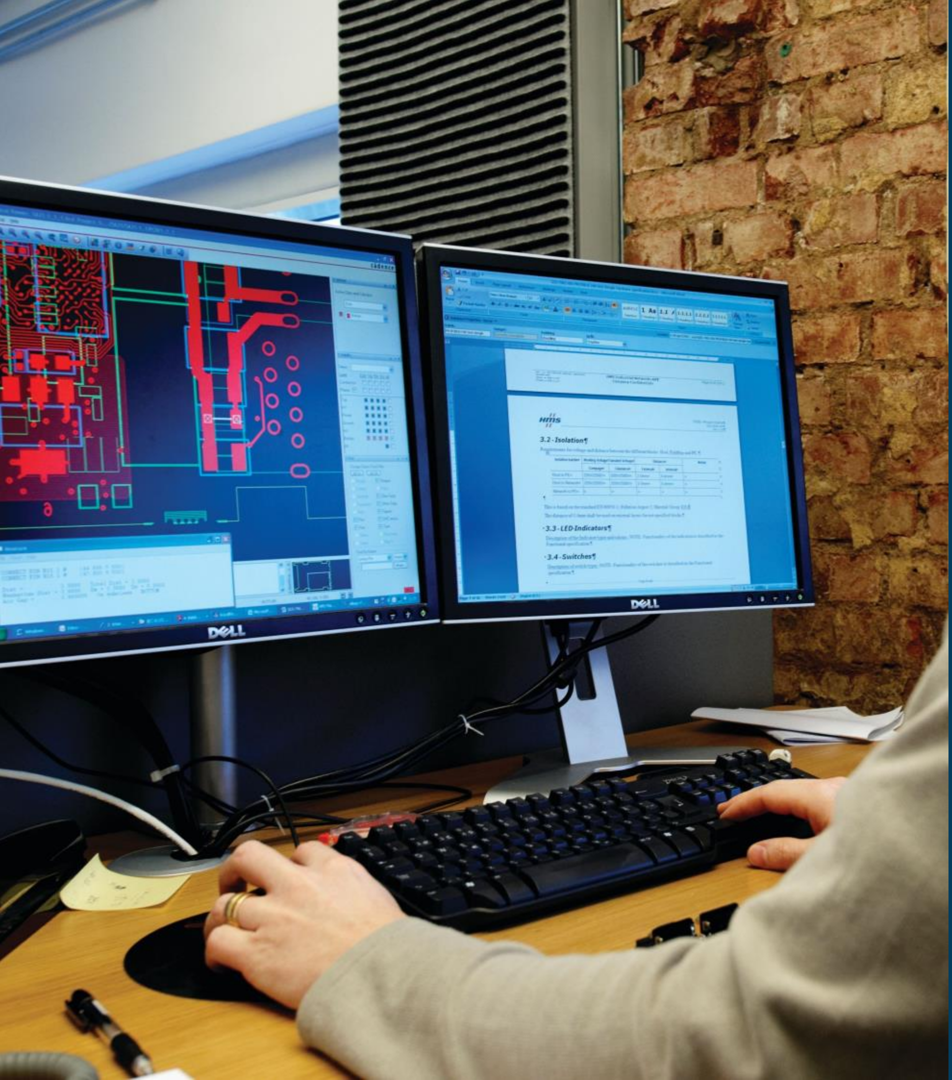
IT versus OT - Pitfalls

IT - Secure oriented

- Confidentiality / Integrity
- Credentials mandatory
- Security scanning & updates (patches)

OT - Process oriented

- Operating Running / Low down-time
- Credentials for protecting IP / User roles
- Firmware only to solve defined issues

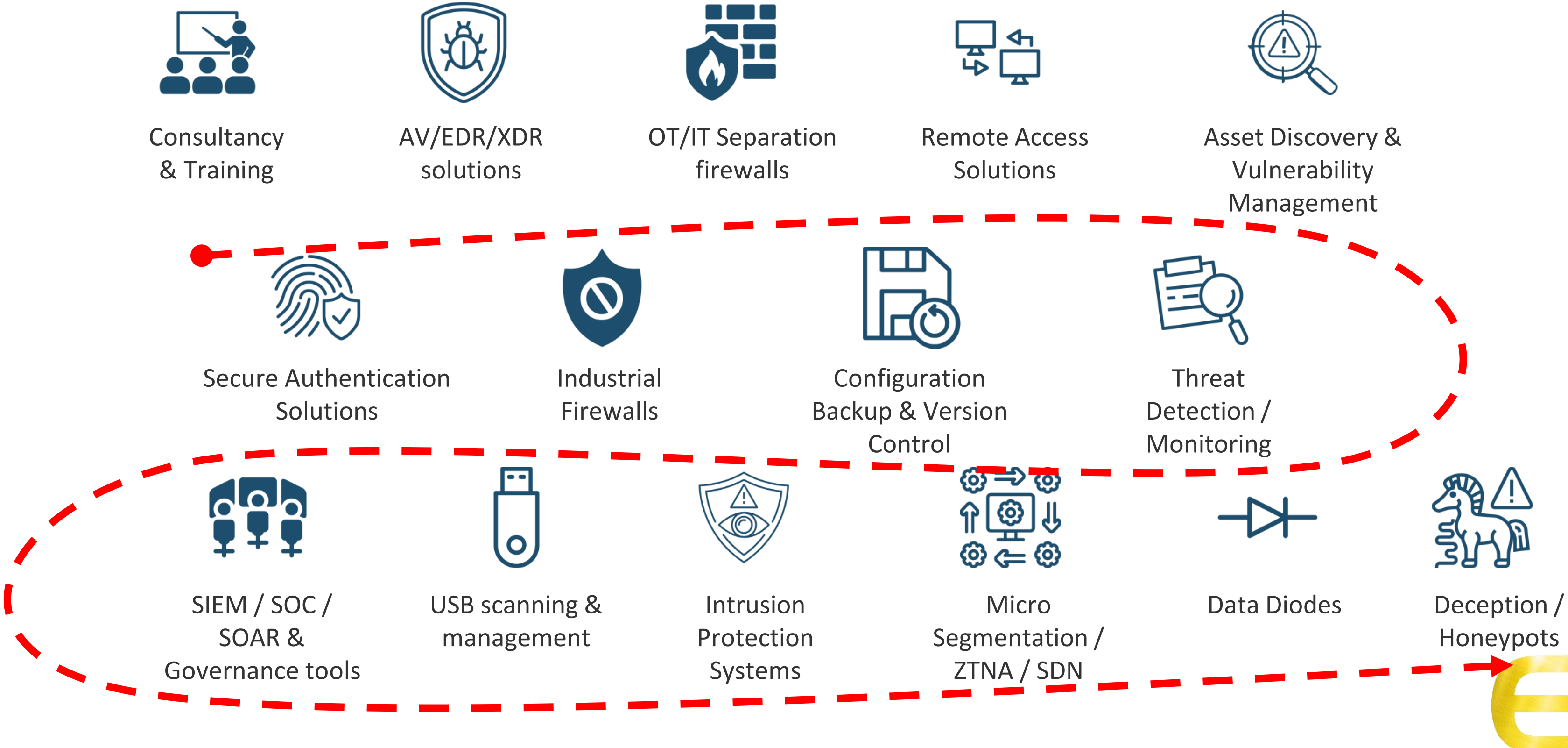


Design-in

Security in industrial embedded applications

Security design

Journey through Industrial Cybersecurity landscape



Consultancy & Training

AV/EDR/XDR solutions

OT/IT Separation firewalls

Remote Access Solutions

Asset Discovery & Vulnerability Management

Secure Authentication Solutions

Industrial Firewalls

Configuration Backup & Version Control

Threat Detection / Monitoring

SIEM / SOC / SOAR & Governance tools

USB scanning & management

Intrusion Protection Systems

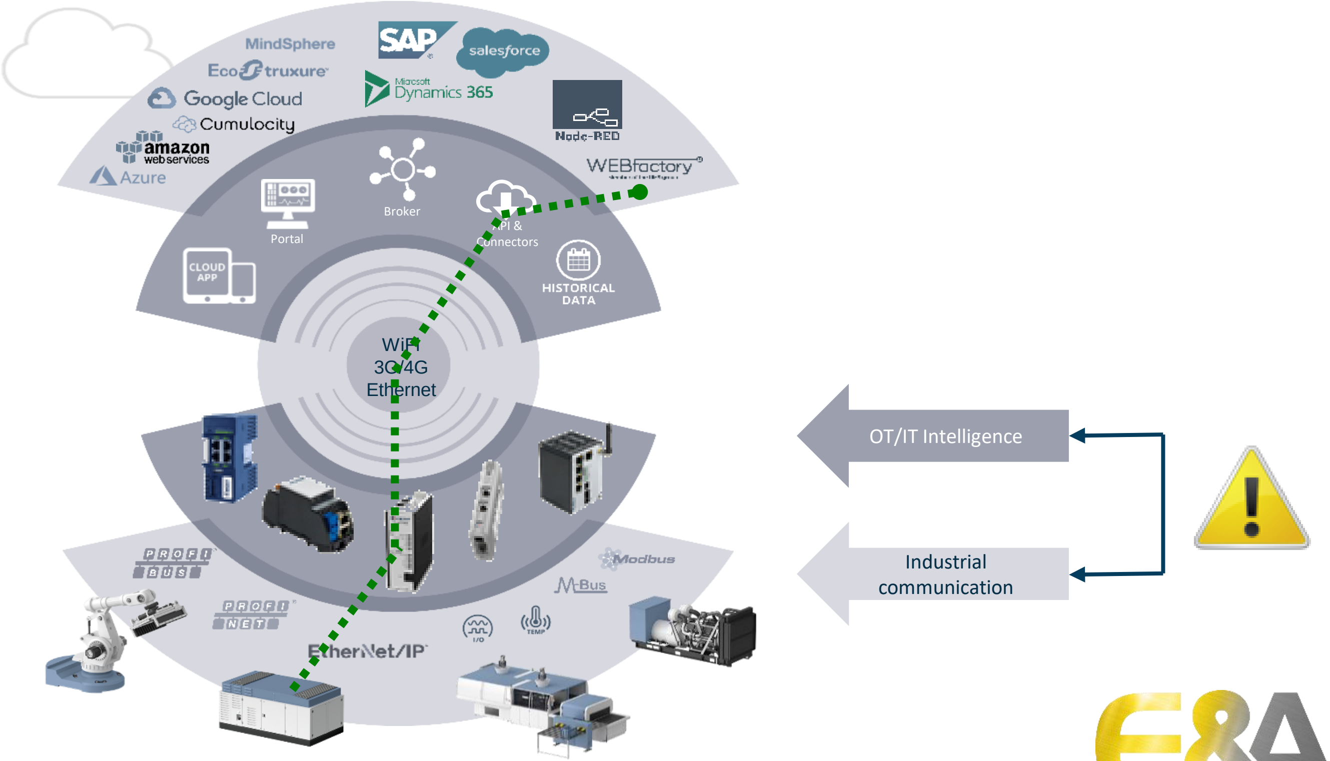
Micro Segmentation / ZTNA / SDN

Data Diodes

Deception / Honeypots

Security design

The security pitfall



Security design

Node Building blocks

Certificate Management

Trusted parties

Encryption

Secure channels

Security Chip

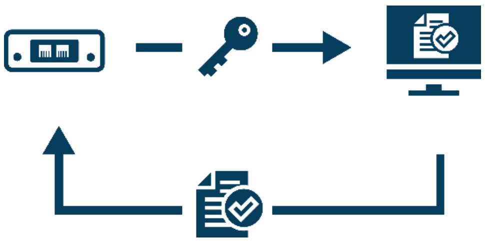
Store secret data

Secure Boot

Trusted firmware

Security design

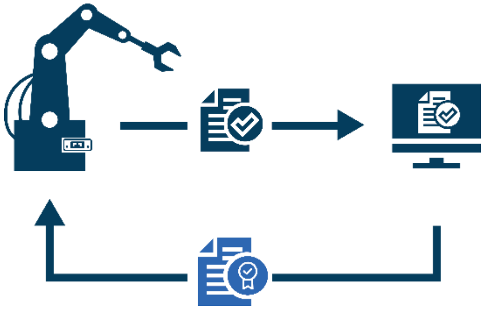
ID Certificate



Set-up custom with tool

- Factory-set public key
- Send key to local secure server
- Save certificate in security chip

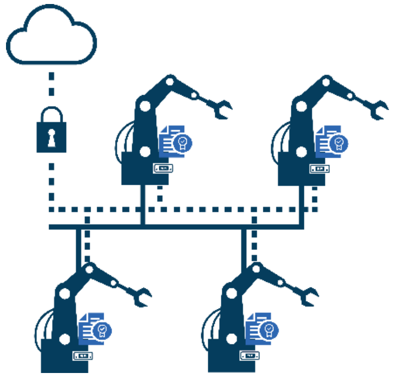
Device Certification



Identification at start-up

- Sent certificate to server
- Return certificate
- Enable data

Secure Operation

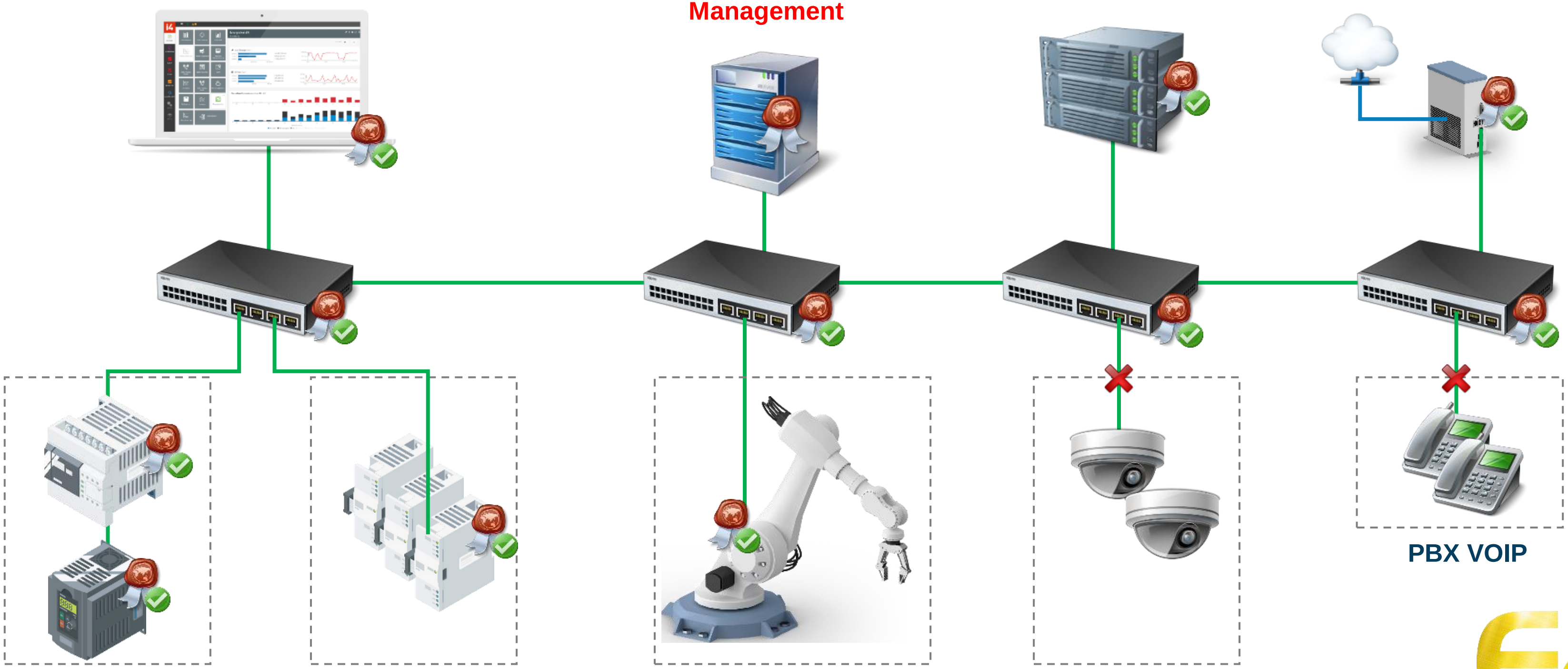


Secure and Identified

- All nodes certified
- Trusted data exchange
- All data encrypted

Security design

Factory security



Scada / dashboard

Certificate Management

ERP / MRP

Cloud

Machine 1

Machine 2

Robot

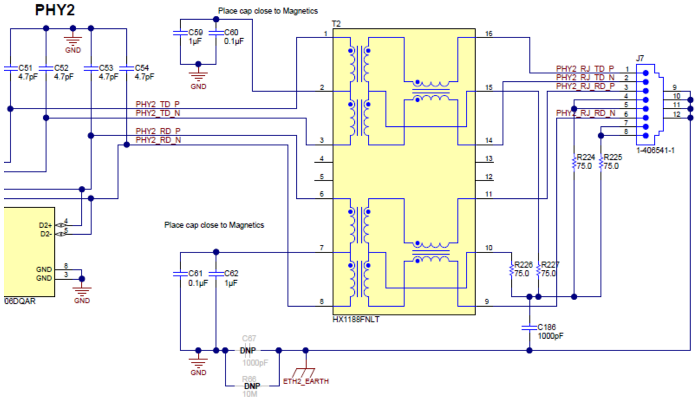
CCV

PBX VOIP

Embedded Design-in

Hardware

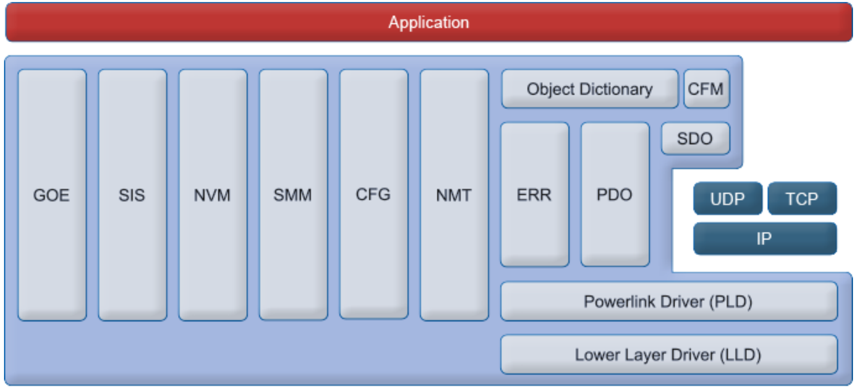
Understanding the architectures



- Beside RJ45 everything is different
- TSN synchronization / Non-TSN
- Security

Software

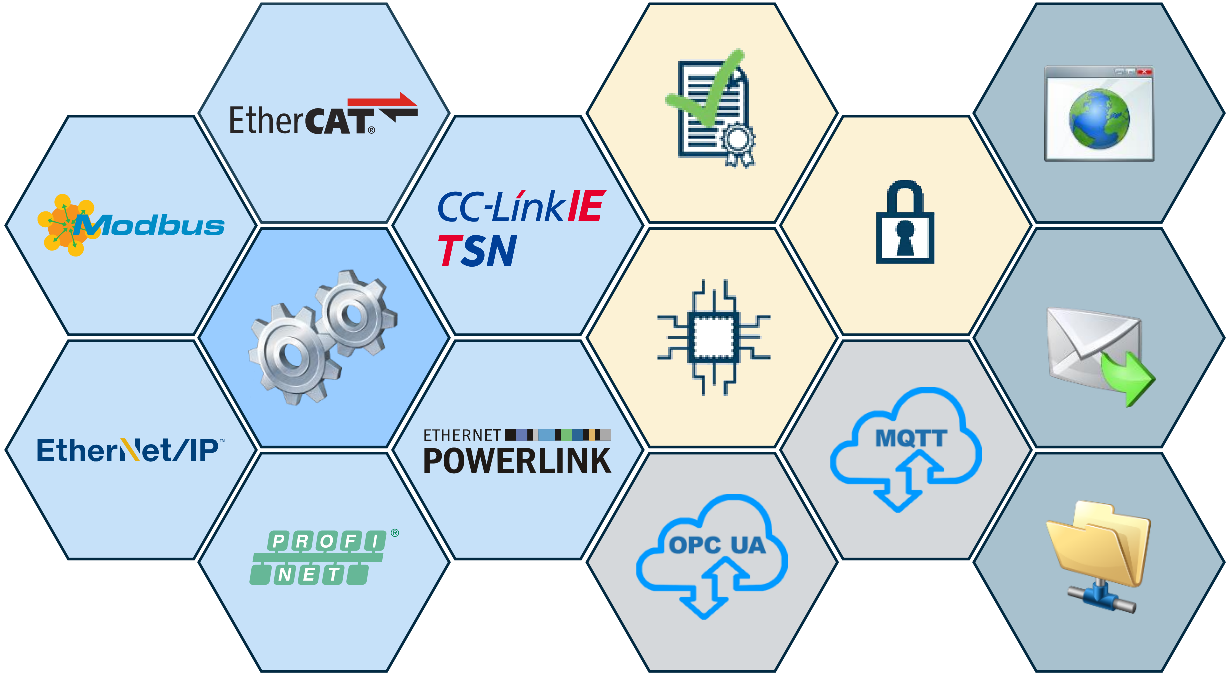
Understanding the protocols



- Stacks requires in-depth knowledge
- Secure boot & integrity
- Requiring certification

Embedded Design-in

Multiple-protocol - Software stacks



Software is not standardized

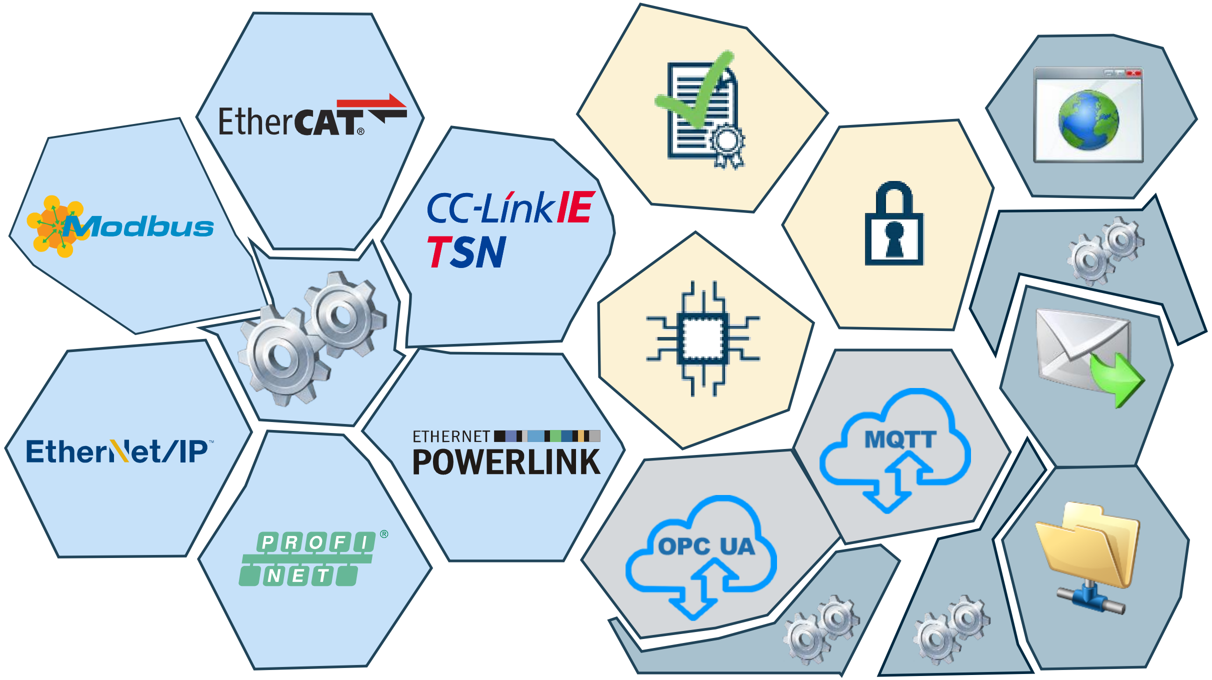
- Different vendors
- Different structures
- Different interfaces
- Different drivers
- Different releases

Special attention

- Non-TCP/IP protocols
- Real-time priority
- Software interference

Embedded Design-in

Multiple-protocol - Software stacks



Software is not standardized

- Different vendors
- Different structures
- Different interfaces
- Different drivers
- Different releases

Special attention

- Non-TCP/IP protocols
- Real-time priority
- Software interference

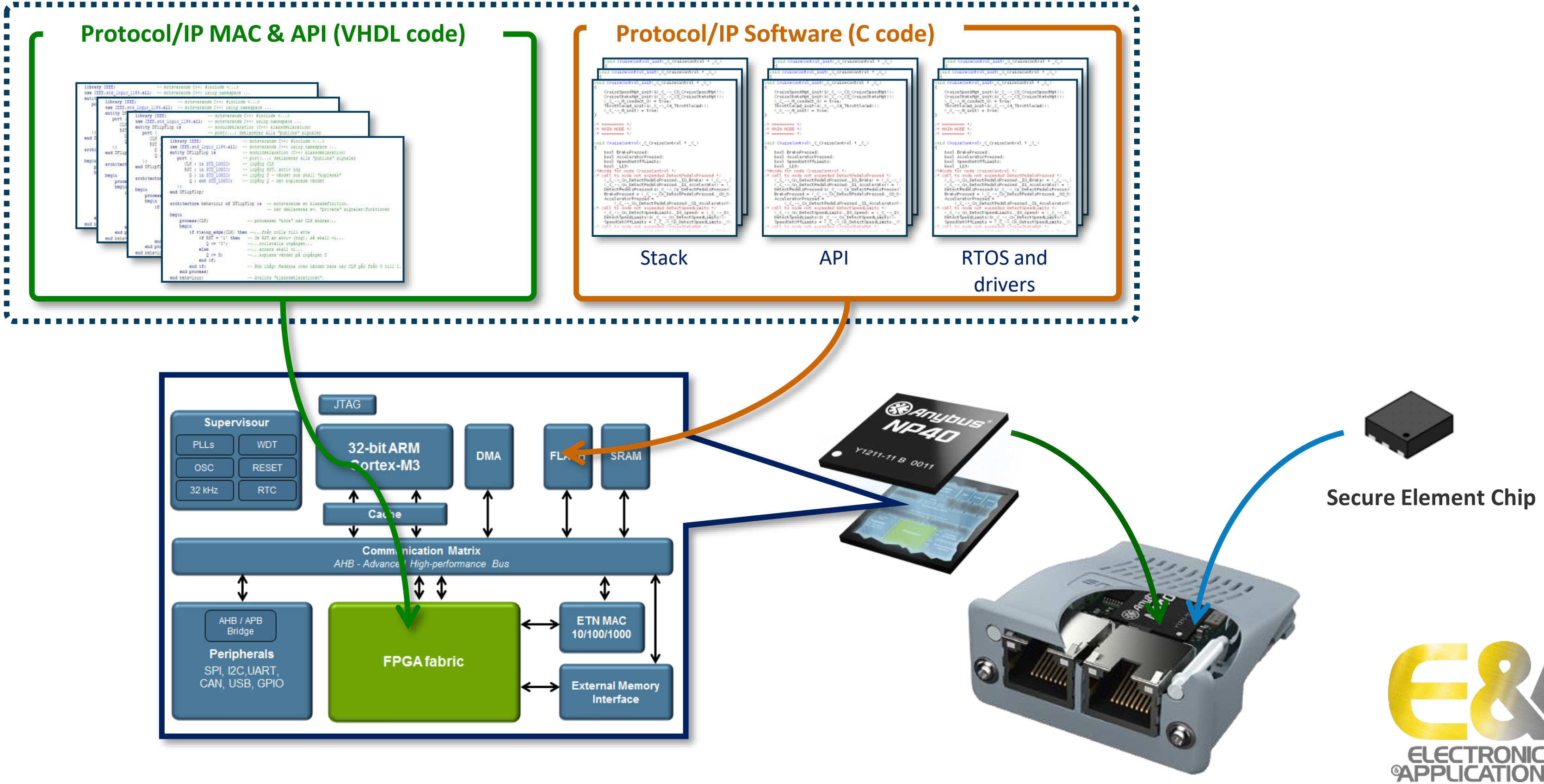
Multi-protocol software-development is a complex task!

Embedded Communication Module

Smart and reliable

Embedded Communication

Programmable hard- & software



Protocol/IP MAC & API (VHDL code)

```
library IEEE;                 -- motsvarande C++: #include <...>
use IEEE.std_logic_1164.all;  -- motsvarande C++: using namespace ...
entity DFlipFlop is           -- moduldeklaration (C++: klassdeklaration)
   port (                     -- port(...) deklarerar alla "publika" signaler
      CLK : in STD_LOGIC;     -- ingång CLK
      RST : in STD_LOGIC;     -- ingång RST, aktiv hög
        D : in STD_LOGIC;     -- ingång D - värdet som skall "kopieras"
        Q : out STD_LOGIC;    -- utgång Q - det kopierade värdet
   );
end DFlipFlop;

architecture behaviour of DFlipFlop is  -- motsvarande en klassdefinition.
                                        -- här deklareras ev. "privata" signaler/funktioner
begin
    process(CLK)              -- processen "körs" när CLK ändras...
    begin
        if rising_edge(CLK) then --...från nolla till etta
            if RST = '1' then    -- Om RST är aktiv (hög), så skall vi...
               Q <= '0';         --...nollställa utgången...
            else                 --...annars skall vi...
               Q <= D;           --...kopiera värdet på ingången D
            end if;
        end if;                  -- Kom ihåg: Raderna ovan händer bara när CLK går från 0 till 1.
    end process;
end behaviour;                   -- Avsluta "klassdeklarationen".
```

Protocol/IP Software (C code)

```
void CruiseControl_init(_C_CruiseControl * _C_)
{
    CruiseSpeedMgt_init(&(_C_->_C0_CruiseSpeedMgt));
    CruiseStateMgt_init(&(_C_->_C5_CruiseStateMgt));
    (_C_->_M_condact_0) = true;
    ThrottleCmd_init(&(_C_->_C4_ThrottleCmd));
    (_C_->_M_init) = true;
}

/* ========= */
/* MAIN NODE */
/* ========= */

void CruiseControl(_C_CruiseControl * _C_)
{
    bool BrakePressed;
    bool AcceleratorPressed;
    bool SpeedOutOffLimits;
    bool _L19;
/*#code for node CruiseControl */
/* call to node not expanded DetectPedalsPressed */
    (_C_->_Cn_DetectPedalsPressed._I0_Brake) = (_C_->_I
    (_C_->_Cn_DetectPedalsPressed._I1_Accelerator) = (_
    DetectPedalsPressed(&(_C_->_Cn_DetectPedalsPressed)
    BrakePressed = (_C_->_Cn_DetectPedalsPressed._O0_Br
    AcceleratorPressed =
        (_C_->_Cn_DetectPedalsPressed._O1_AcceleratorPr
/* call to node not expanded DetectSpeedLimits */
    (_C_->_Cn_DetectSpeedLimits._I0_speed) = (_C_->_I0_
    DetectSpeedLimits(&(_C_->_Cn_DetectSpeedLimits));
    SpeedOutOffLimits = (_C_->_Cn_DetectSpeedLimits._O0_
/* call to node not expanded CruiseStateMgt */
    (_C_->_C5_CruiseStateMgt._I0_BrakePressed) = BrakeP
```

Stack

API

RTOS and drivers

JTAG

Supervisour

PLLs

WDT

OSC

RESET

32 kHz

RTC

32-bit ARM Cortex-M3

DMA

FLASH

SRAM

Cache

Communication Matrix

AHB - Advanced High-performance Bus

AHB / APB Bridge

Peripherals

SPI, I2C,UART, CAN, USB, GPIO

FPGA fabric

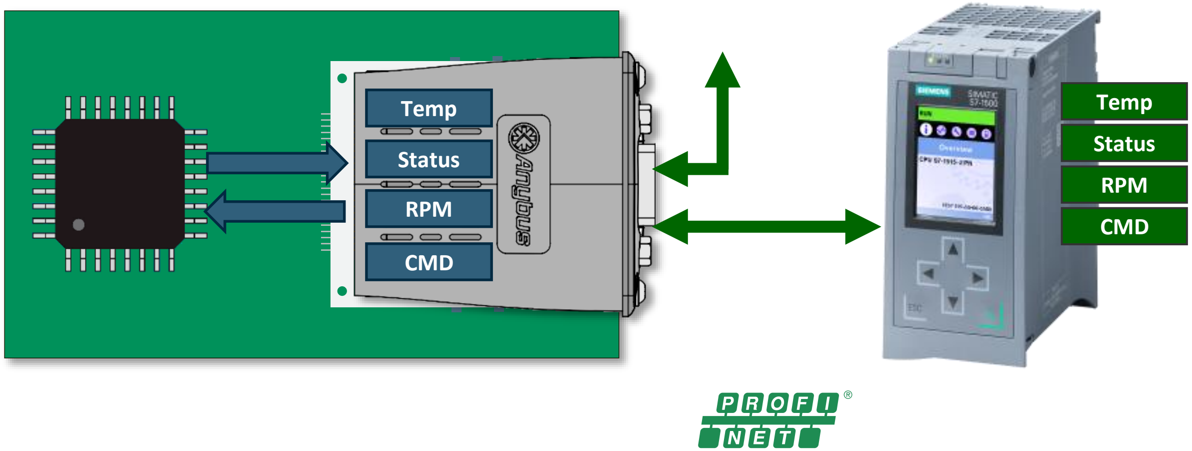
ETN MAC 10/100/1000

External Memory Interface

Secure Element Chip

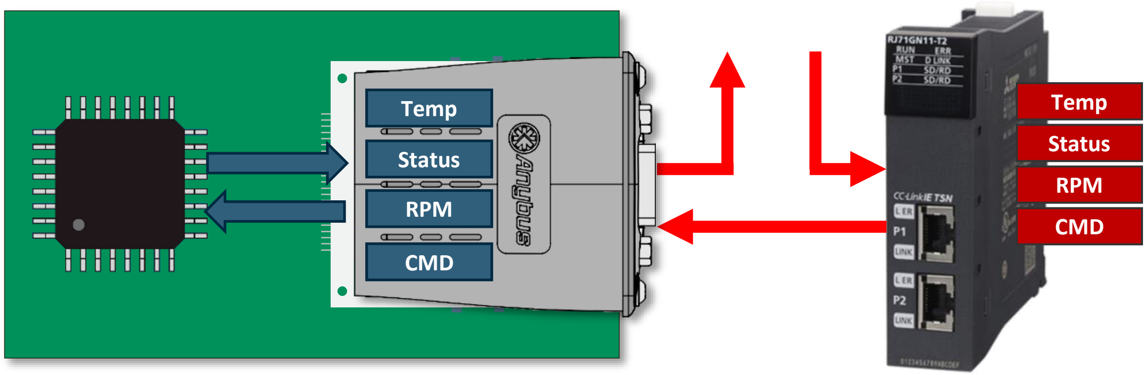
Embedded Communication

Host & Master principle: PROFINET & EtherCAT



Embedded Communication

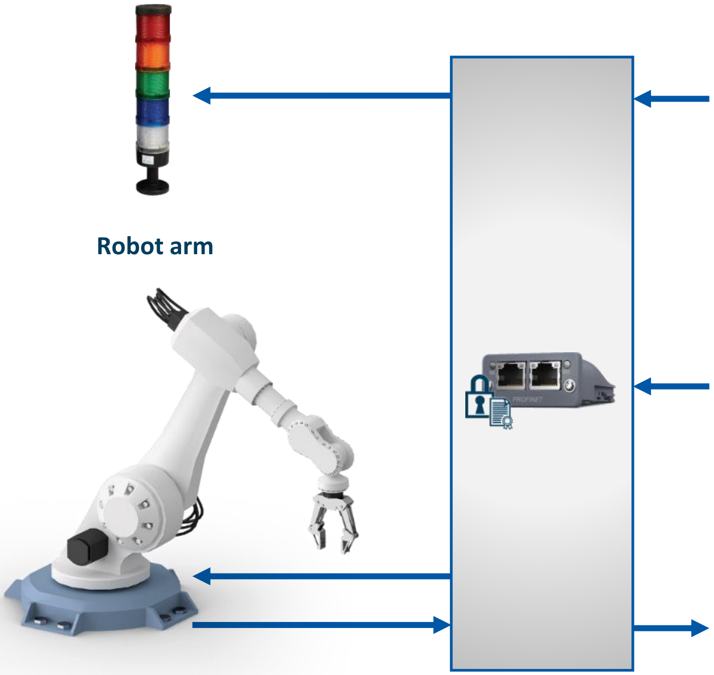
Host & Master principle: PROFINET & EtherCAT



CC-Link IE TSN

Anybus CompactCom 40

Practice



Tower Light with 5 colors

Robot arm

ADI #100
Name: TowerLights
Array of 5 Boolean
Read

ADI #200
Name: PositionCtrl
Array of 3 Dword
Read

ADI #201
Name: DeviceStatus
Integer
Write

Availability

Secure

PROFINET®

EtherNet/IP

OPC UA

MQTT.ORG

Time Sensitive

CC-Link IE TSN

Stay Connected at www.hms-networks.com

HMS

Anybus® BY HMS NETWORKS Ewon® BY HMS NETWORKS Intesis® BY HMS NETWORKS Ixxat® BY HMS NETWORKS

You are invited to our booth 7E011

E&A ELECTRONICS & APPLICATIONS '23

26 T/M 28 SEPTEMBER '23 JAARBEURS UTRECHT

Hardware Meets Softwareft′

Stay Connected!

www.hms-networks.com