Cyber Securing your Factory Floor

SMART INDUSTRY (Fourth IR/I40 in NL) DUTCH INDUSTRY FIT FOR THE FUTURE

www.smartindustry.nl

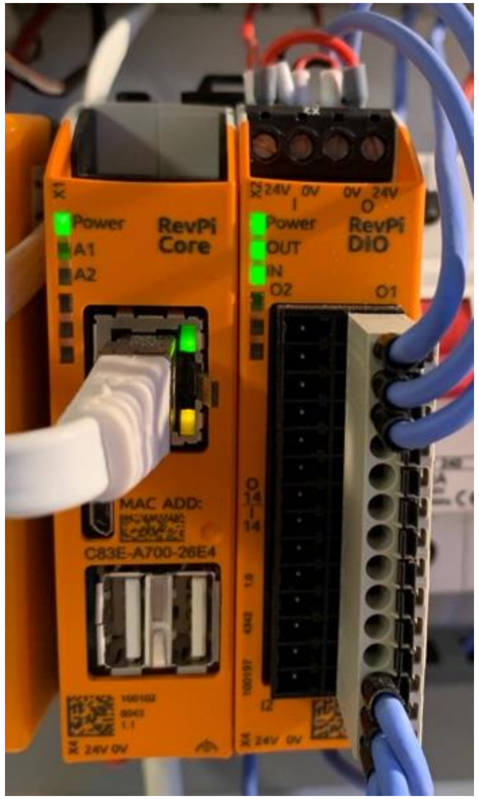
Egbert-Jan.Sol@TNO.nl

Jan 2021

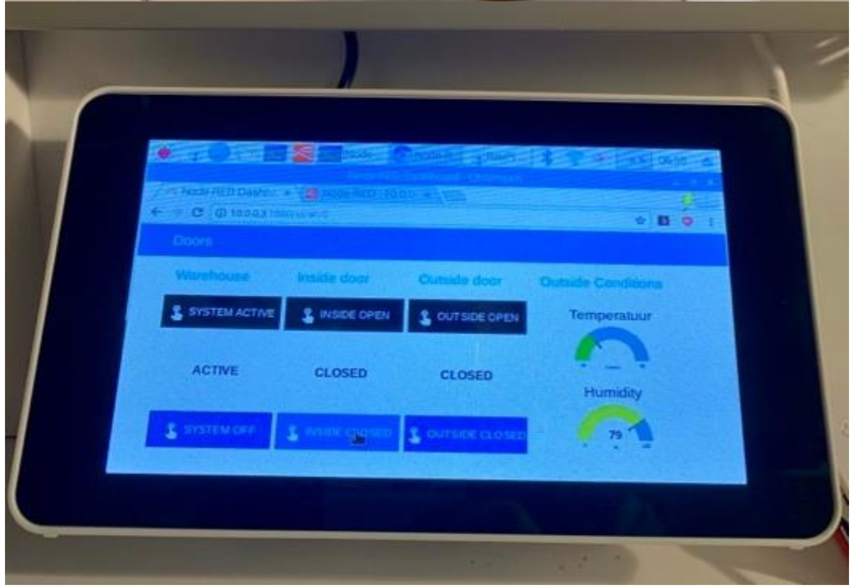
Smart Industry is the Dutch Industrie 4.0 initiative by the metal/electro branch organizations FME, MetaalUnie together with the Chamber of Commerce, TNO and the Dutch Ministry of Economic Affairs & Climate.

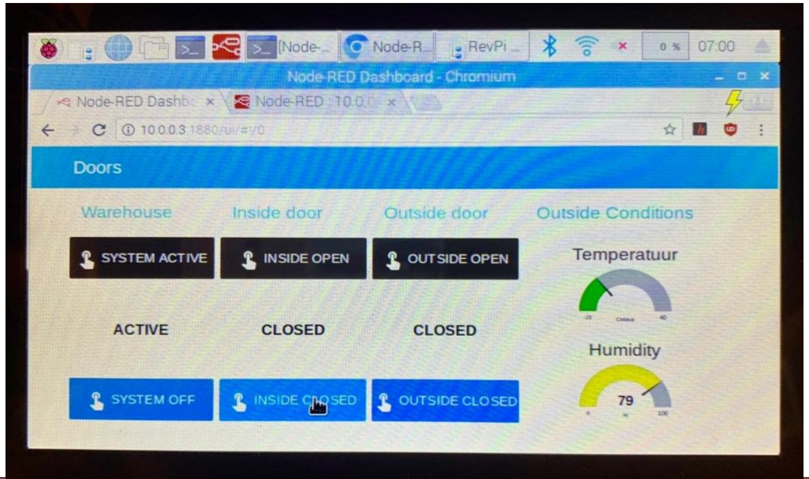
The best and most flexible digital connection production network …..

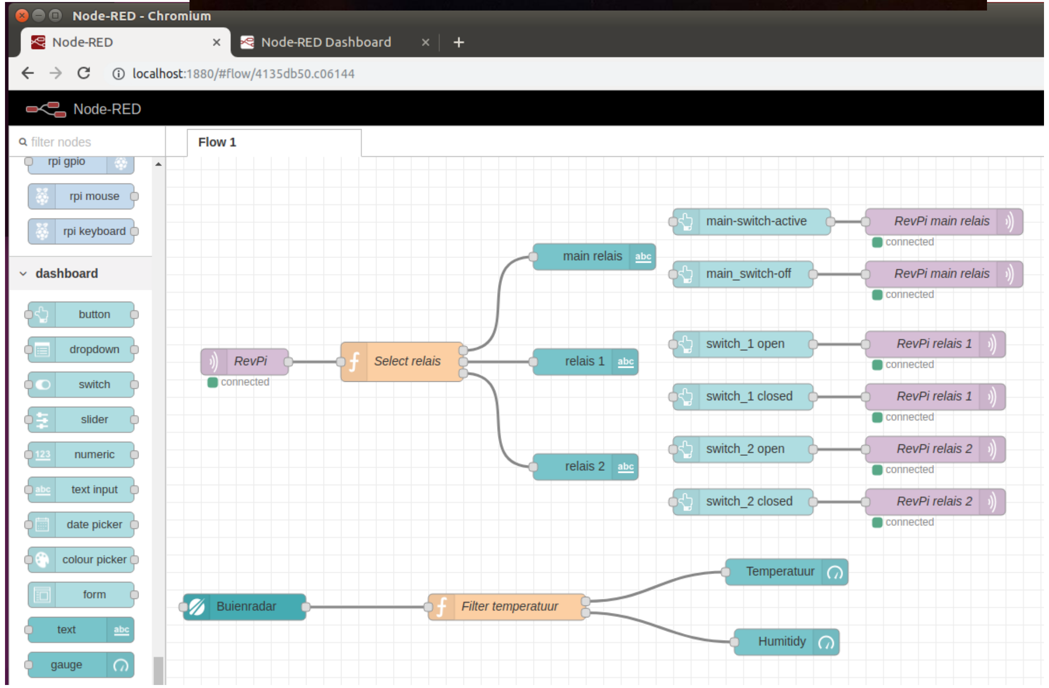
An Ethernet cable is easily plugged into production line equipment as e.g. a PLC …..



….. to monitor and control your system and collect your data







“It is war, but no-one notice it” – unique Dutch book

Iran

Stuxnet ***Sabotage***

DigiNotar ***Certificate***

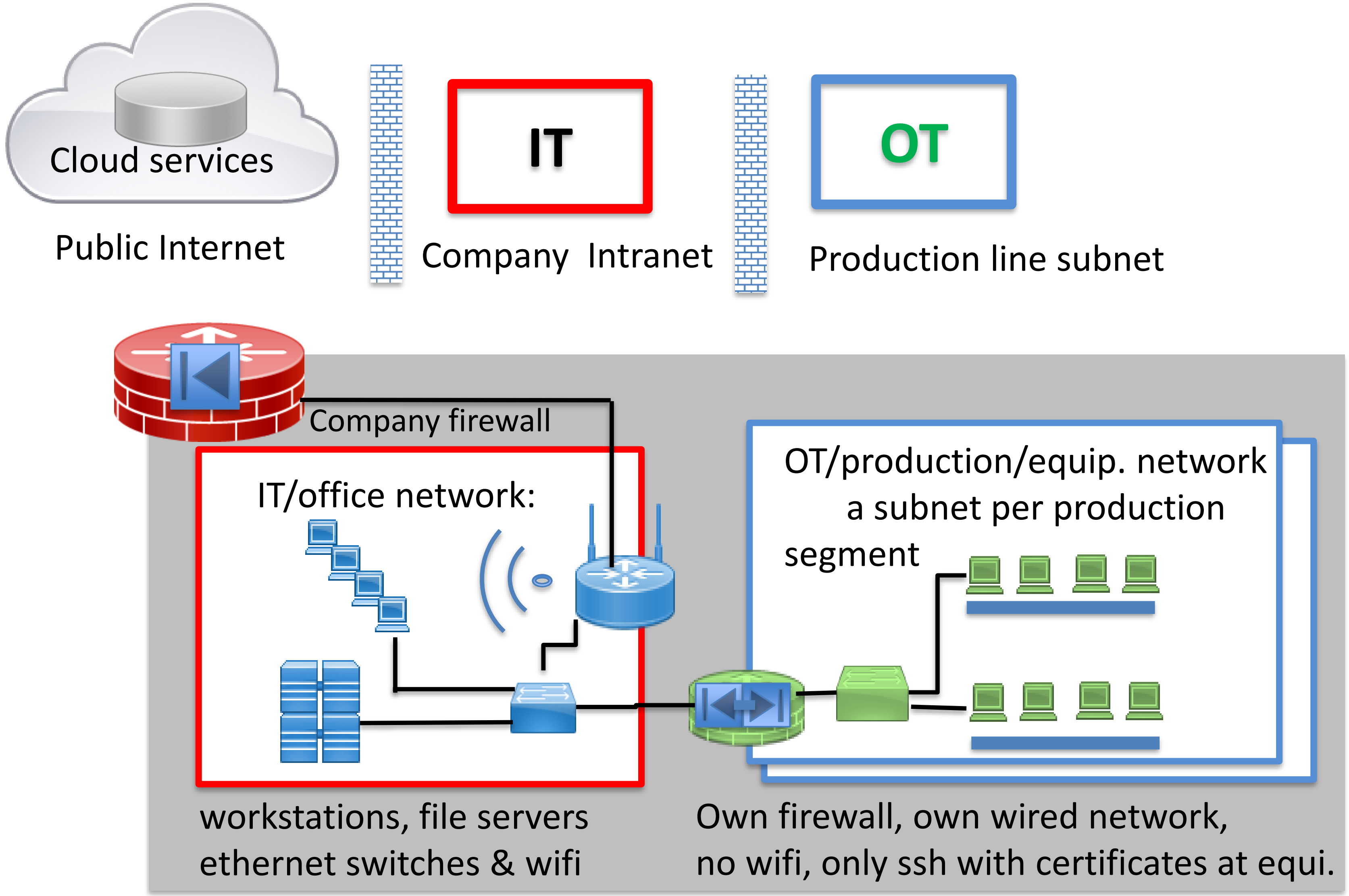
Ukraine

Maersk

Notpetya ***Ransom***

HET IS OORLOG
MAAR NIEMAND DIE HET ZIET
"Wie vroeger de wereld wilde begrijpen, las de Bijbel. Wie de wereld van nu wil begrijpen, leest dit boek."
ARJEN LUBACH
PODIUM
HUIB MODDERKOLK

IT versus OT: Office ≠ production/equipment Network



workstations, file servers
ethernet switches & wifi

Own firewall, own wired network,
no wifi, only ssh with certificates at equi.

IT cyber security paradigm:

Hardening the perimeter (firewalls)
Segmentation (subnets)
Updating of patches
Monitoring (reading log files, etc)
Usernames & passwords

OT Cyber security (IT ++):

+ internal firewall (*double locked*)
+ no USB,
+ no wifi
+ no hidden eSIM 3/4/5G

Content – data driven business and cyber security at the factory floor and value chains

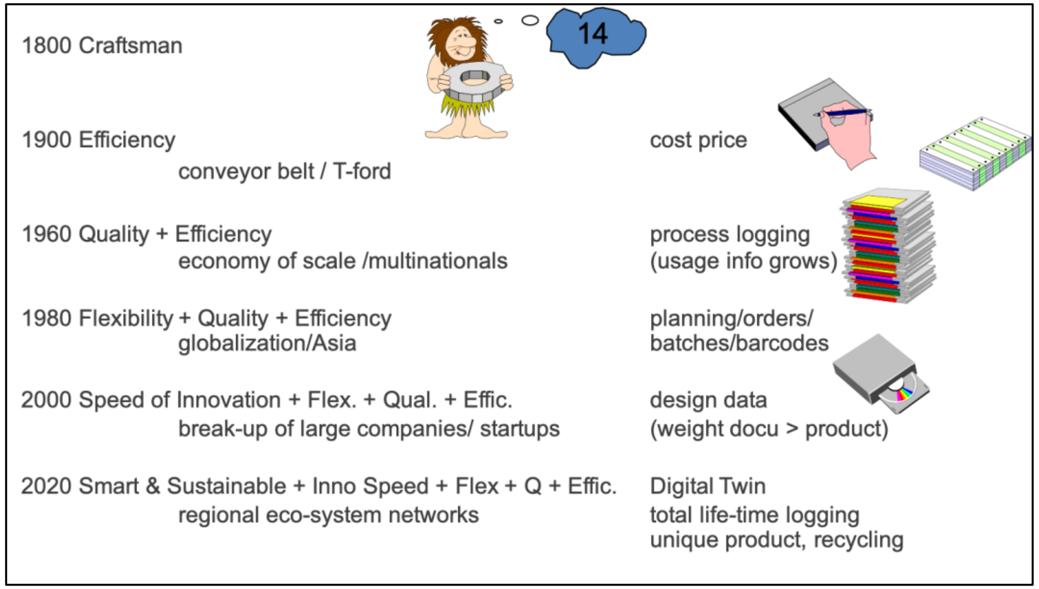
Flexible Manufacturing
Smart Products
Servitization
Digital Factory
Connected Factories
Sustainable Factory
Smart Working
Advanced Manufacturing
Manufacturing technologies
3D
Smart Industry
Network Centric
Digitization

1. Introduction
2. Vision – from digital via smart to sustainable

   more and more all data driven
3. Data – from machine data to digital twinning

   and legal issues and data eco-systems/platforms
4. OT-data - focus on cyber securing the data from the factory production line
5. Training workshop - Factory floor cyber security in a day / open source training
6. Conclusion - Life-long learning on digital skills

Smart Industry = Industrie 4.0 + Smart Services (servitisation)



1800 Craftsman

1900 Efficiency
conveyor belt / T-ford

cost price

1960 Quality + Efficiency
economy of scale /multinationals

process logging
(usage info grows)

1980 Flexibility + Quality + Efficiency
globalization/Asia

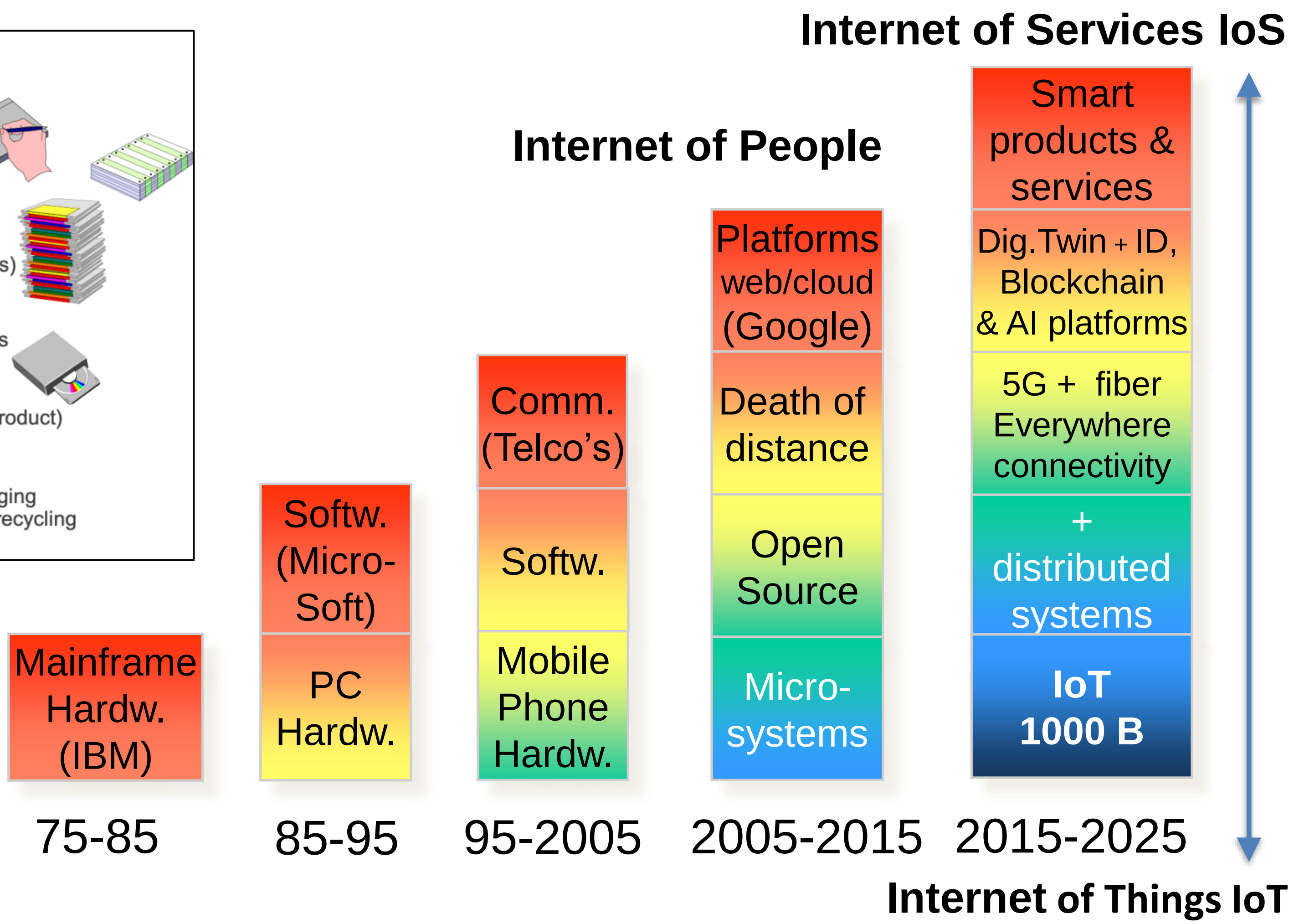
planning/orders/
batches/barcodes

2000 Speed of Innovation + Flex. + Qual. + Effic.
break-up of large companies/ startups

design data
(weight docu > product)

2020 Smart & Sustainable + Inno Speed + Flex + Q + Effic.
regional eco-system networks

Digital Twin
total life-time logging
unique product, recycling



Internet of Services IoS

Internet of People

75-85: Mainframe Hardw. (IBM)

85-95: PC Hardw.; Softw. (Micro-Soft)

95-2005: Mobile Phone Hardw.; Softw.; Comm. (Telco's)

2005-2015: Micro-systems; Open Source; Death of distance; Platforms web/cloud (Google)

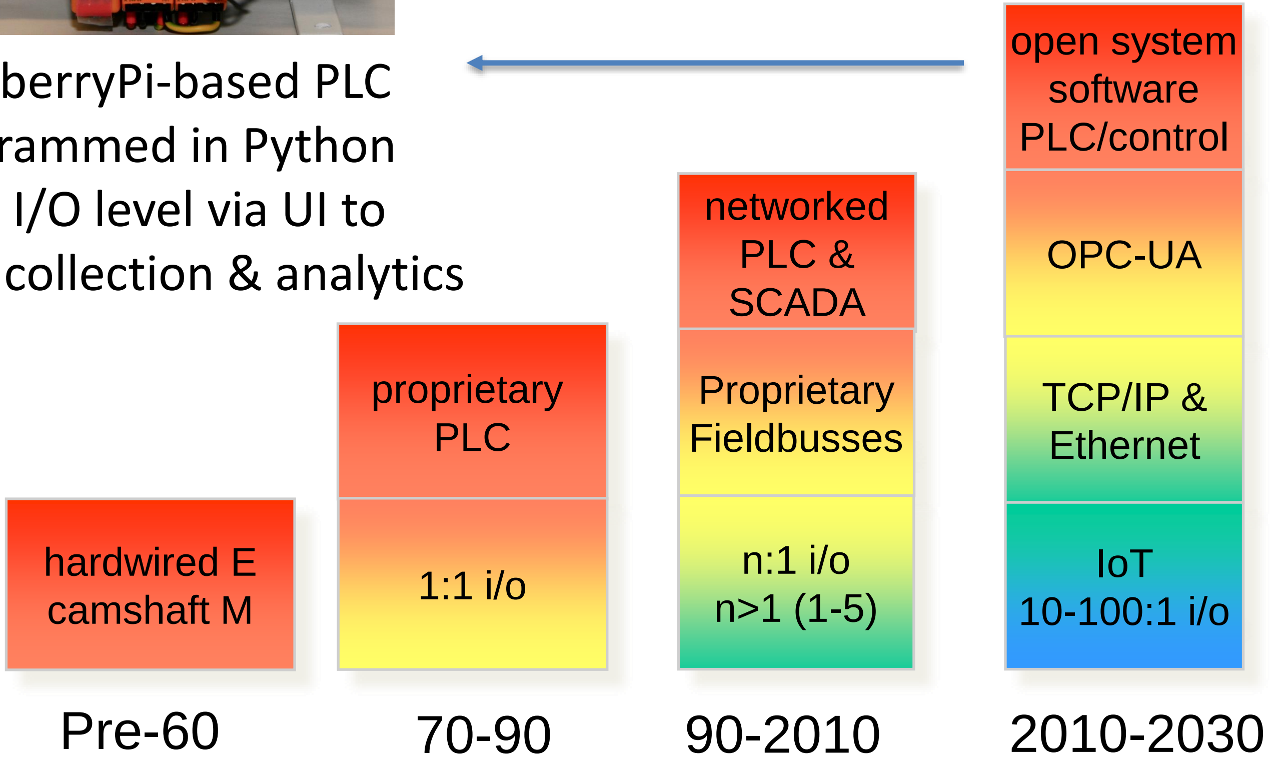
2015-2025: IoT 1000 B; + distributed systems; 5G + fiber Everywhere connectivity; Dig.Twin + ID, Blockchain & AI platforms; Smart products & services

Internet of Things IoT

Data collection from shopfloor/equipment control systems

1 Industrial IoT (IIoT) or edge computer
as number of I/O increases to 10+/1
for production control, data logging, etc.

2 RaspberryPi-based PLC
programmed in Python
from I/O level via UI to
data collection & analytics



hardwired E camshaft M

Pre-60

proprietary PLC

1:1 i/o

70-90

networked PLC & SCADA

Proprietary Fieldbusses

n:1 i/o
n>1 (1-5)

90-2010

open system software PLC/control

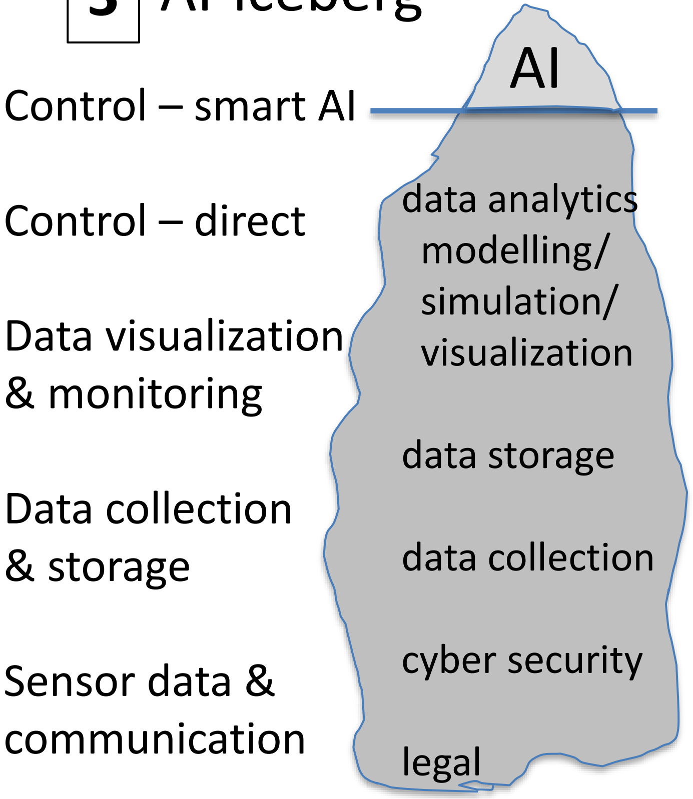
OPC-UA

TCP/IP & Ethernet

IoT
10-100:1 i/o

2010-2030

3 AI-iceberg



Control – smart AI

Control – direct

Data visualization & monitoring

Data collection & storage

Sensor data & communication

ROADMAP FACTORIES

Zero paper:
100% of stations/workcells are digitalized

Zero defect: e.g.
100% automated Q-control at each step

Zero programming:
Robots, cobots, AGV with sensing
& Digital Twin

Zero tooling:
3D printing/additive manufacturing

Zero delay:
just-in-time, lot size n=1,

Zero surprise:
predictive maintenance and servitisation

Zero waste:
recycling and sustainable energy

Zero drop-out: lifelong learning for everyone

Digital Factory
Robotics, Cobots, AGV,
Industrial Internet of Things,
Digital Twinning, AR/VR,
Automated workcells,
(**zero** ambitions)

1: known series of products

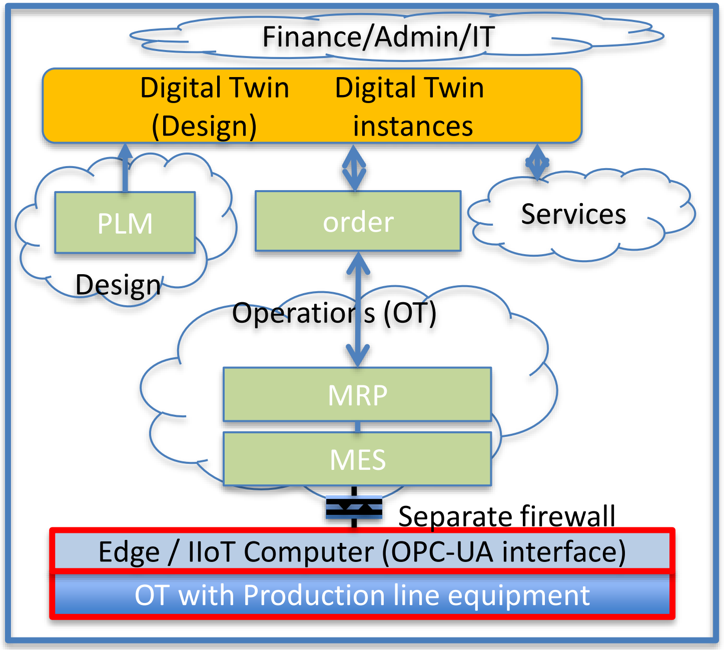
Smart Factory
Flexible, Robust, resiliency
downloadable design for 3D
printing, lot-size-1

2: new products & variants

Sustainable Factory - Extreme
Flexible (Re-) Manufacturing
Autonomous systems, handling
'never seen' products

**3: unknown products
based on recycled materials and products**

ROADMAP VALUE CHAINS



1

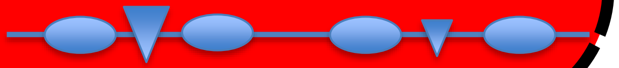
Digital Chain (digital customer portals)

Digital exchange of orders to factory and inside factory all process steps digitalized/paperless (from workorder, programs, status, etc.) from all robotic & operator stations to **customer portal** with realtime info. Manufacturing Data (sharing) Platforms

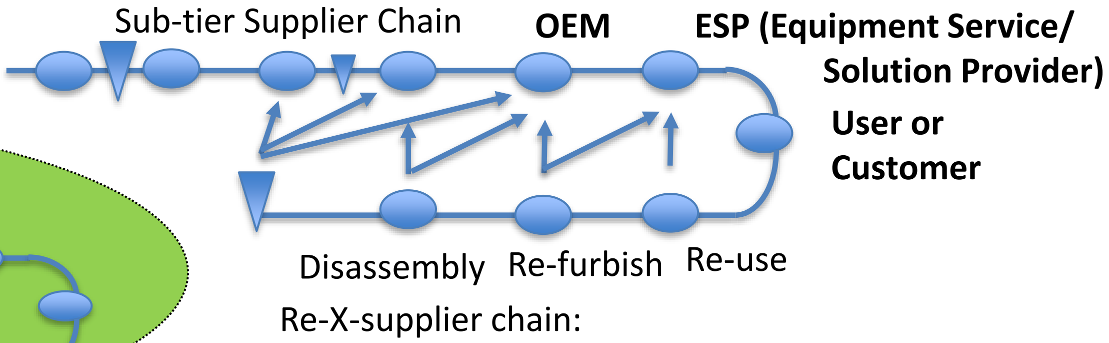
2

Smart Chain

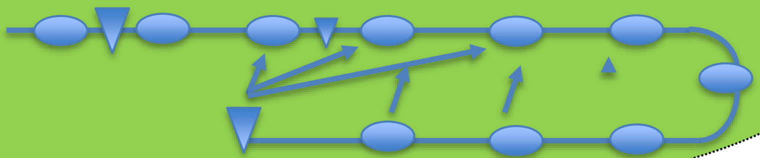
Real-time deep chain planning & control, paperless product changes, full traceability,



3



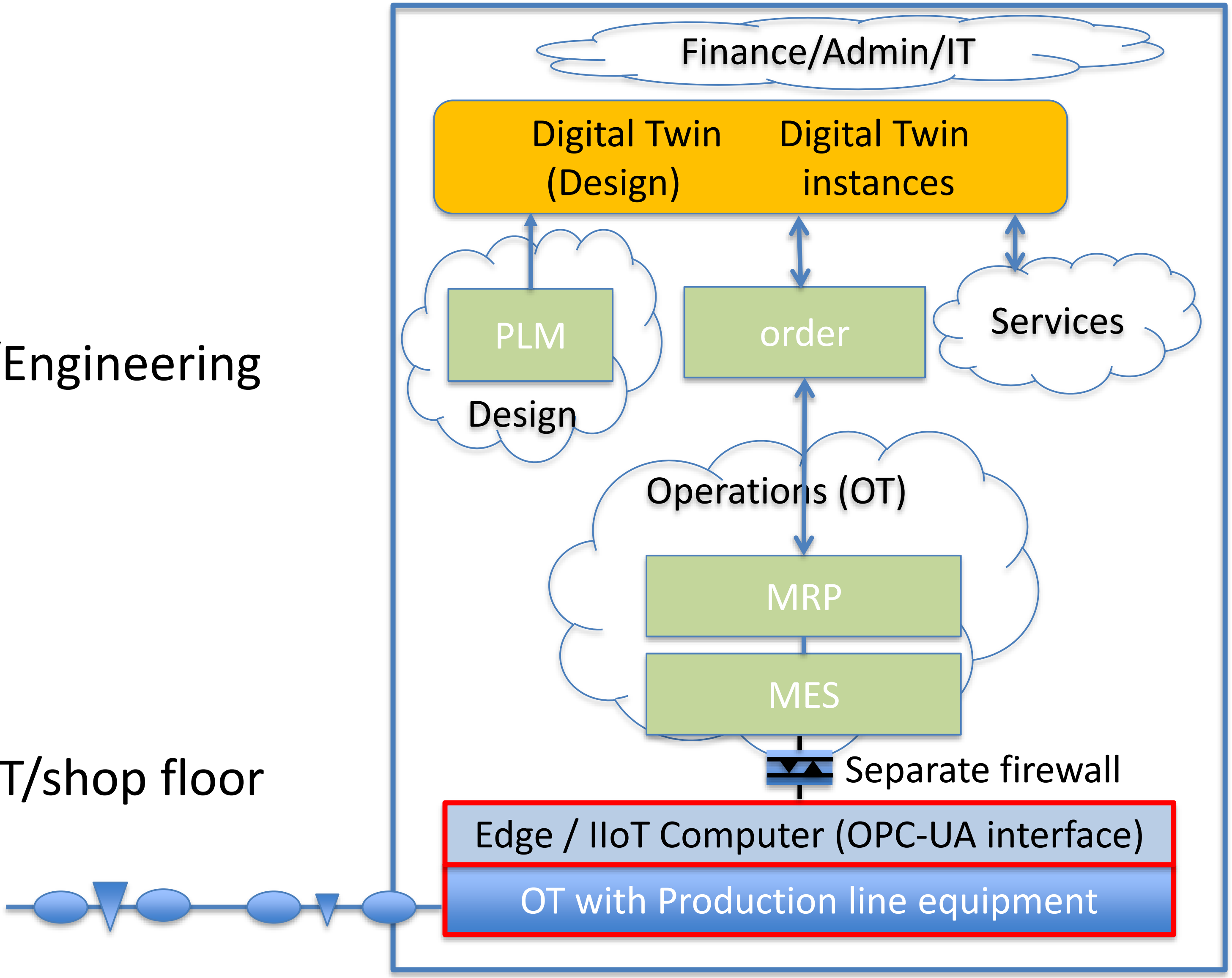
Sustainable Chain/eco-systems



Data Collection from production using edge/IIoT computers

IT/Engineering

OT/shop floor



Ost G information upload by hand

1nd G automation of some workcells

2rd G digitalisation of all workcells and realtime upload with factory ERP/MRP and a few customer portals

3th G realtime updating and structured storage in Digital Twin of your factory ERP and customer portal

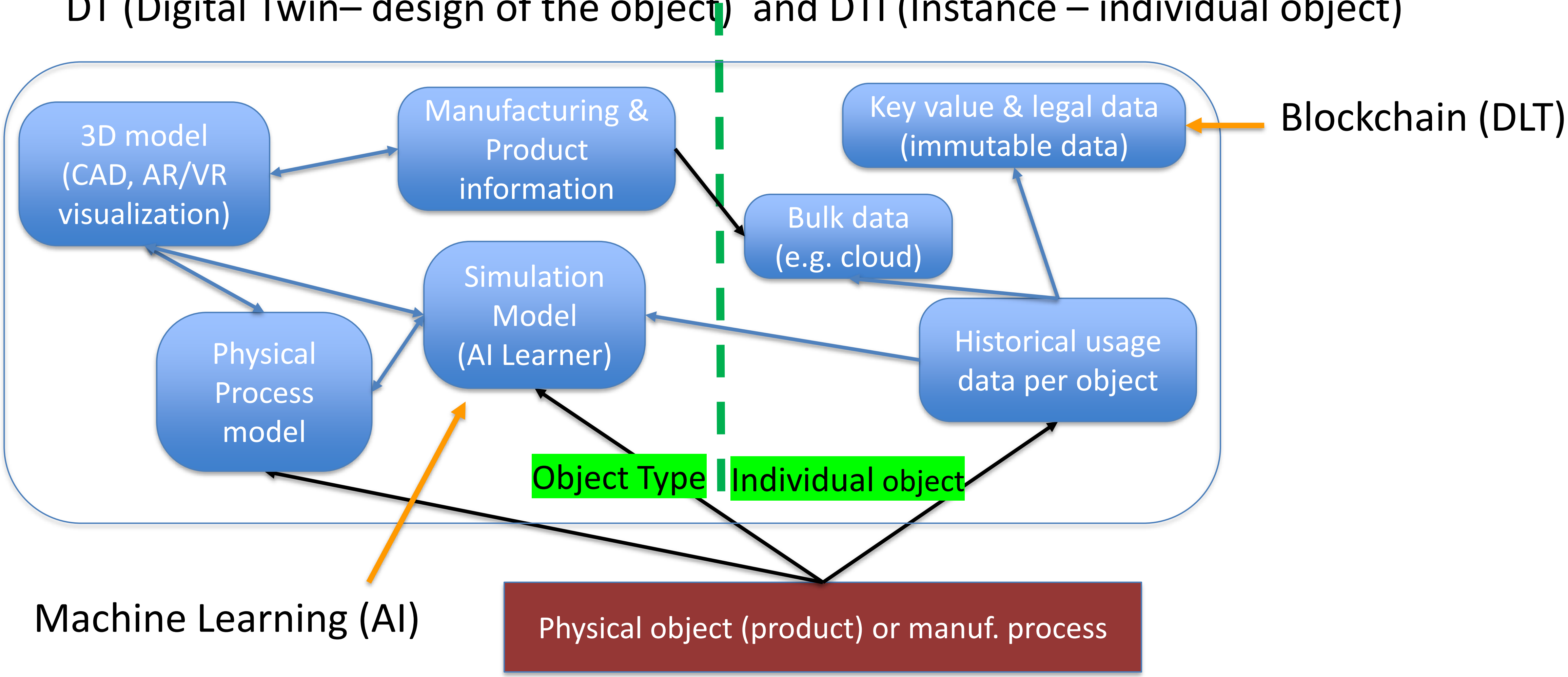
4th G data exchange in value chain with 1st tiers and some subs.

5th G common manufacturing data ecosystem with deep chain realtime planning, control (+AI)

Digital Twinning in design (type) & production & use phase (indiv.)

Digital Twin is a “living” digital representation of the physical object

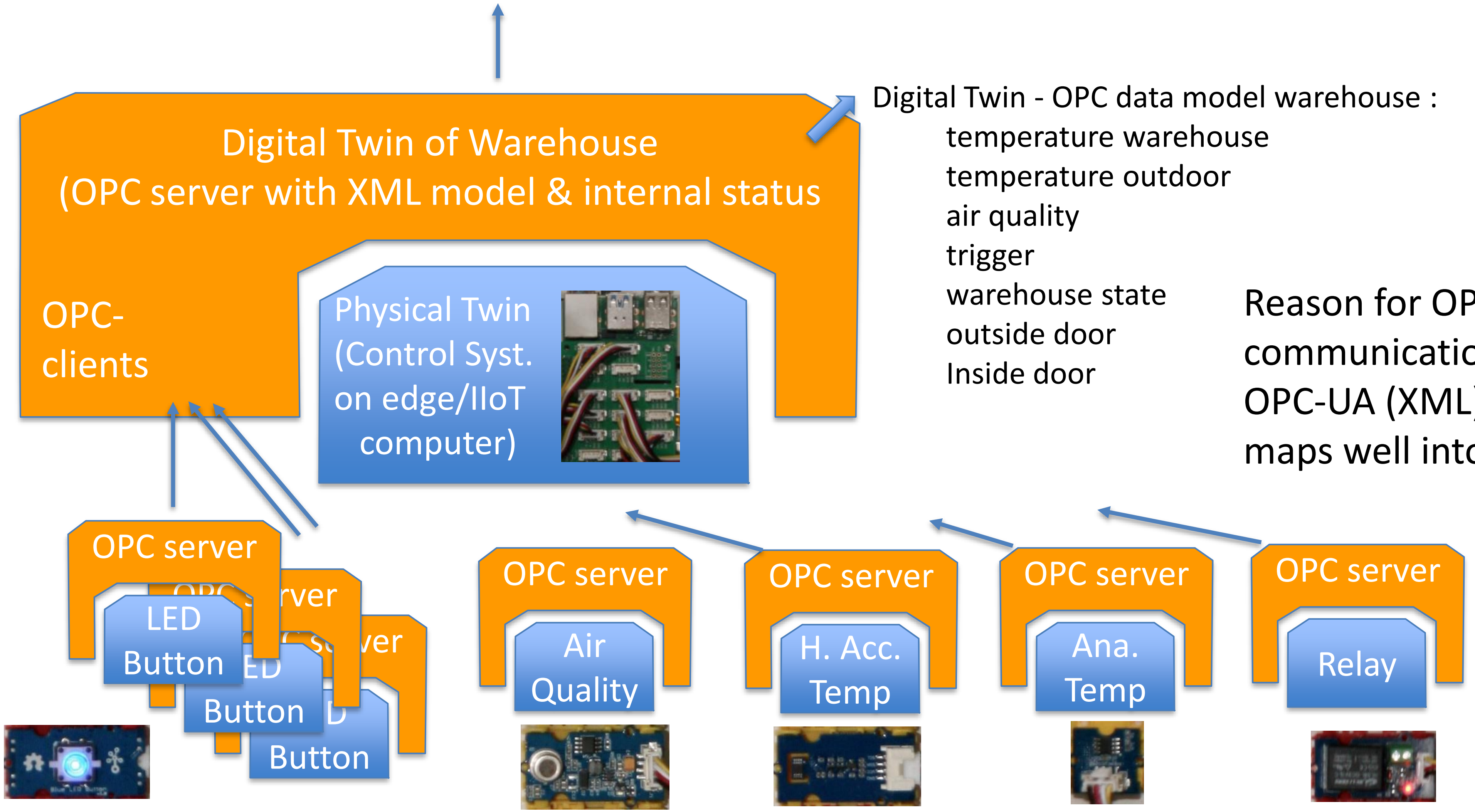
DT (Digital Twin– design of the object) and DTI (Instance – individual object)



3D model (CAD, AR/VR visualization)
Manufacturing & Product information
Key value & legal data (immutable data)
Blockchain (DLT)
Bulk data (e.g. cloud)
Simulation Model (AI Learner)
Physical Process model
Historical usage data per object
Object Type
Individual object
Machine Learning (AI)
Physical object (product) or manuf. process

Warehouse Digital twin in OPC-UA XML namespace

ERP/(real-time) planning & control + traceability info at higher level systems & product digital twins



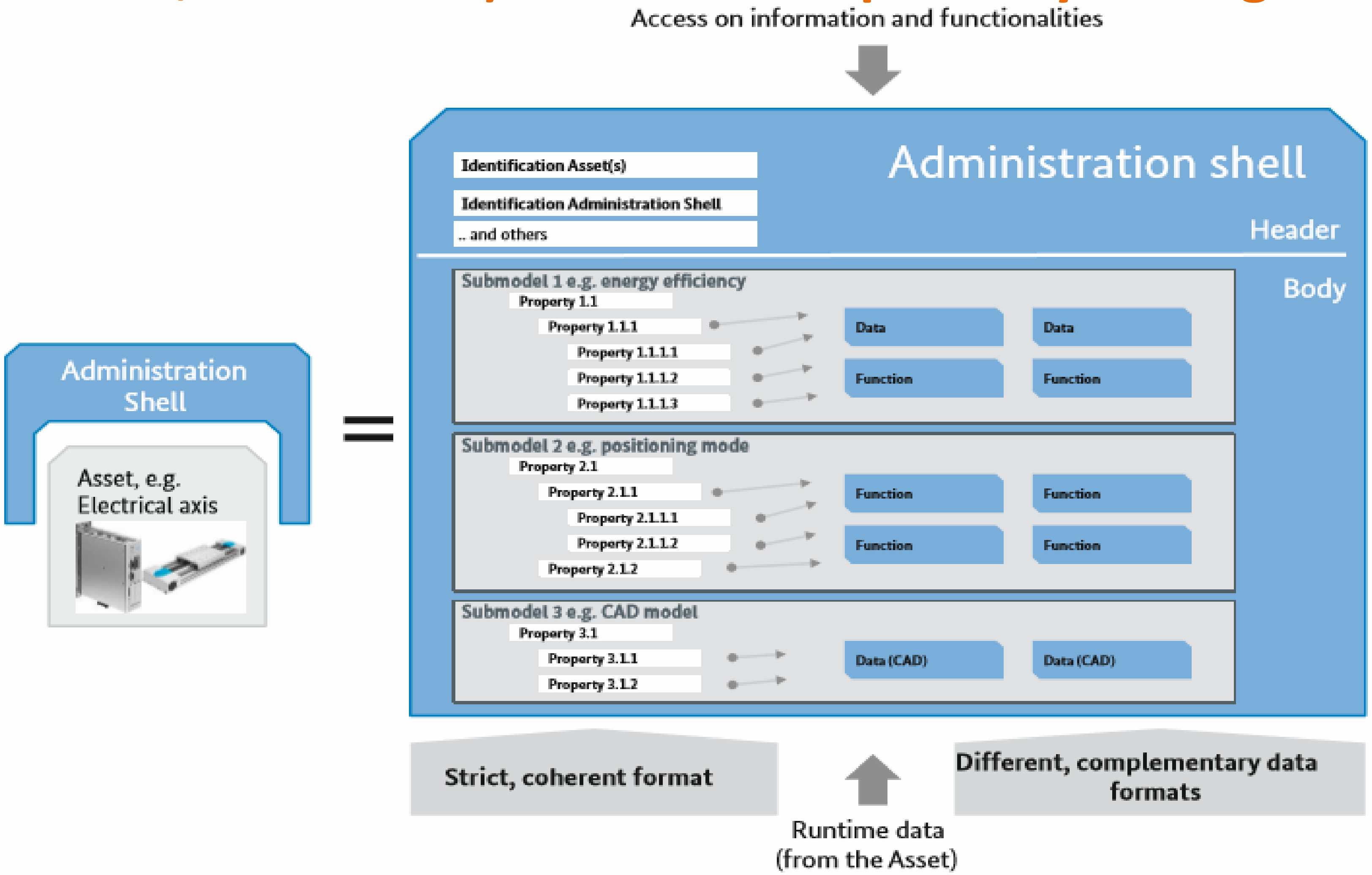
Digital Twin - OPC data model warehouse :

temperature warehouse
temperature outdoor
air quality
trigger
warehouse state
outside door
Inside door

Reason for OPCUA for equipment communication interface standard is the OPC-UA (XML) namespace (object tree) maps well into a digital twin model

Administrative shell for factory equipments, ... Assets (oder VerWaltungsSchale, in German) or in a sense part of your Digital Twin

Digital Twin =
Admin Shell (or VWS)
description of its
data structure
in XML and
accessible
over OPC-UA



Access on information and functionalities

Administration Shell

Asset, e.g.
Electrical axis

=

Administration shell

Header

Identification Asset(s)

Identification Administration Shell

.. and others

Body

Submodel 1 e.g. energy efficiency

Property 1.1
Property 1.1.1
Property 1.1.1.1
Property 1.1.1.2
Property 1.1.1.3

Data | Data
Function | Function

Submodel 2 e.g. positioning mode

Property 2.1
Property 2.1.1
Property 2.1.1.1
Property 2.1.1.2
Property 2.1.2

Function | Function
Function | Function

Submodel 3 e.g. CAD model

Property 3.1
Property 3.1.1
Property 3.1.2

Data (CAD) | Data (CAD)

Strict, coherent format

Runtime data
(from the Asset)

Different, complementary data formats

Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller, April 2018, BMWi,

It is a long way from *Incompatible* to *Interoperable* and beyond

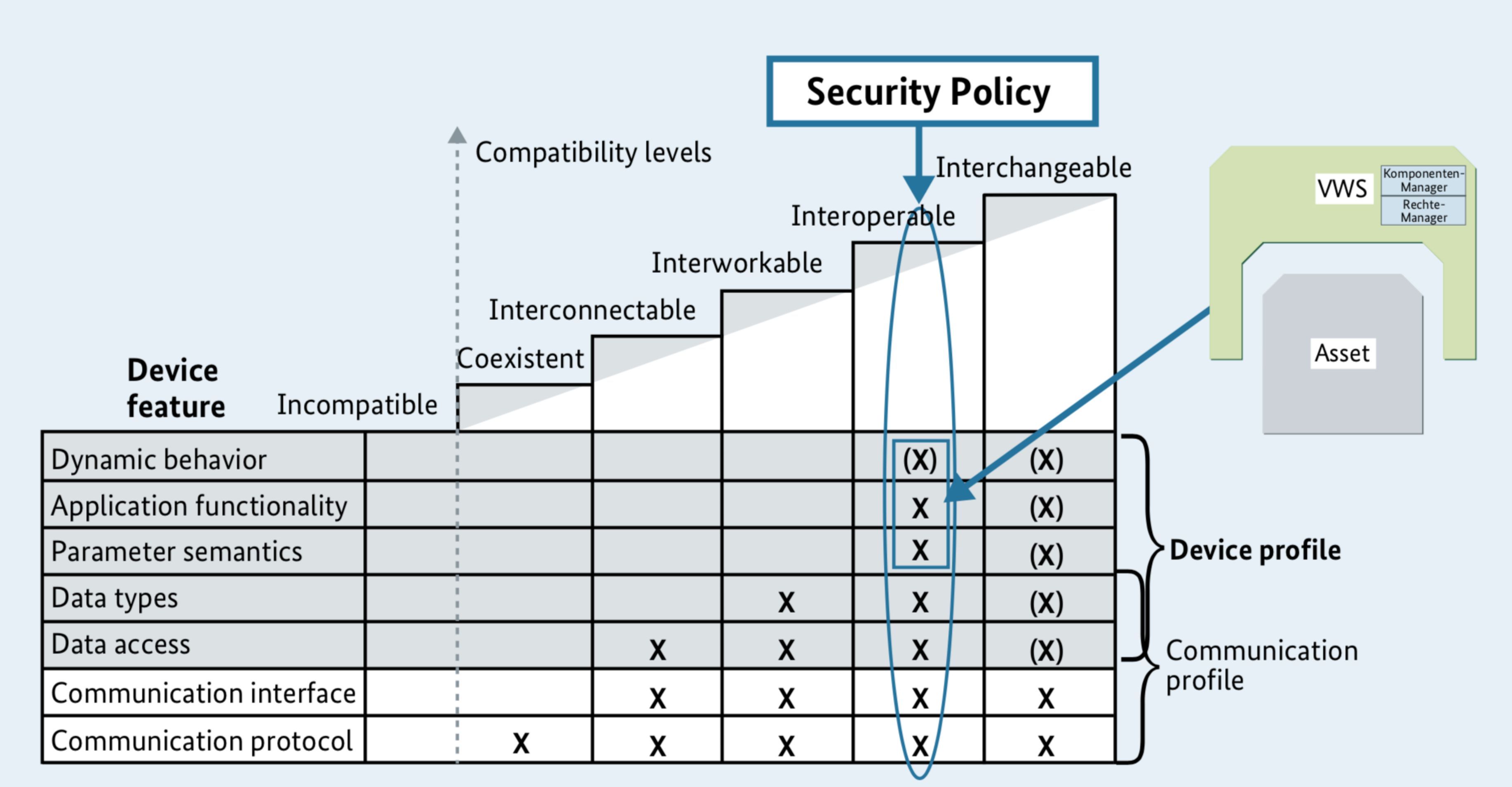
from: Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller

XML is beyond HTML
(Hyper Text Markup Language)

```
<!DOCTYPE html>
 <html>
   <head>
     <title>This is a title</title>
  </head>
  <body>
     <p>Hello world!</p>
  </body>
</html>
```

XML (Extensible Markup Language)

TCP/IP & Ethernet



Device feature	Incompatible	Coexistent	Interconnectable	Interworkable	Interoperable	Interchangeable
Dynamic behavior					(X)	(X)
Application functionality					X	(X)
Parameter semantics					X	(X)
Data types				X	X	(X)
Data access			X	X	X	(X)
Communication interface			X	X	X	X
Communication protocol		X	X	X	X	X

Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller,
April 2018, BMWi,

Legal issues - Sensor Data, Copyright, Databank regulation

Copyright is well known, but applies only on creative/intellectual labor by humans

Sensor data is not copyright protected!!!!!

Sharing Data delen requires legal contracts, and if not careful results in high costs for lawyers

Smart Industry Dare-2-Share example/templates

Don't give others direct data/internet access to your equipment

due to legal reasons, next to cyber risks

(in slide above focus on value chains, but in practice also for service/maintenance of equip.)

but collect it inside your factory yourself first from your OT-subnets

and then start using IT-secured data sharing ecosystems as IDS (Gaia-X)

for inter company data exchanges or intercloud data traffic

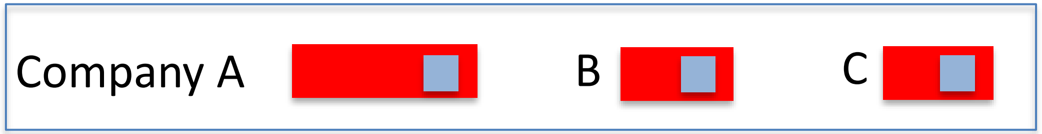
Technology of Data platforms: single- and multi-side market models

🟥 Confidential –own use

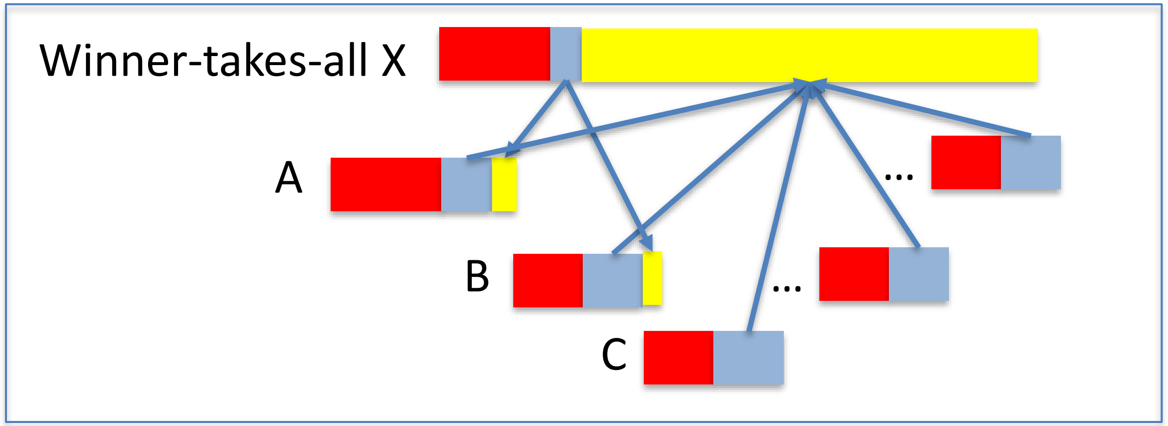
🟦 Shareable

🟨 Data from other(s)

Isolated island with little open data:
players limits their operations as
they can only use own data:

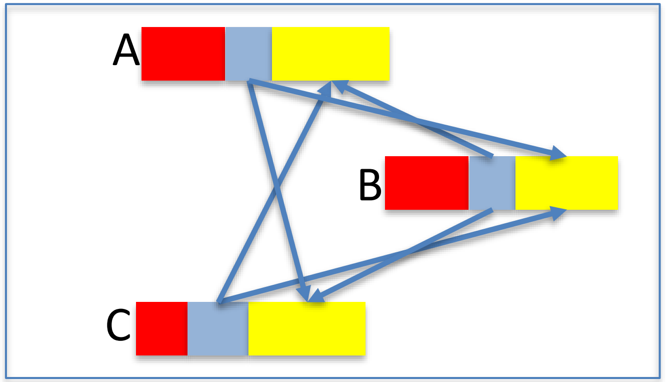


Winner-takes-all: (single party/single market model)
Company X get data from many parties
and has control over what others can use
Other players are limited,
only A & B get a little back, C and rest nothing

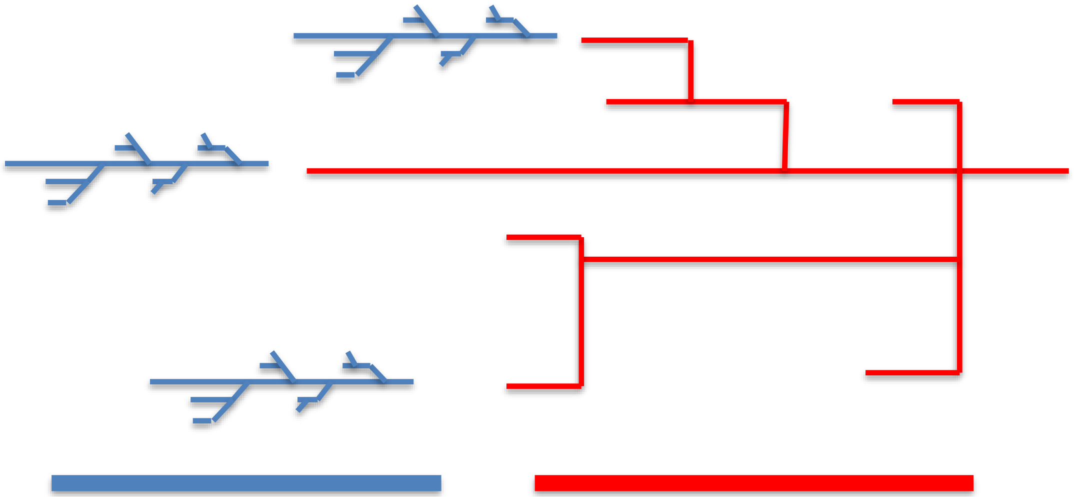


Alliance/Commons Model:
Companies share data on equal contractual basis
and can perform more using data from DES partners

e.g. GSM operator getting roaming info from other GSM
intercloud systems/networks (e.g in manuf.: IDS, Gaia-X)



Value chain -> it’s far more complex: value constellations

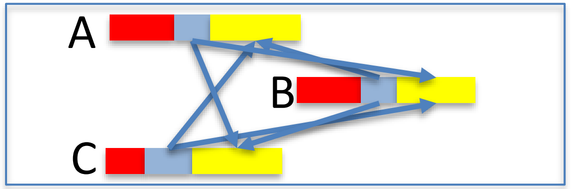


Multiple source

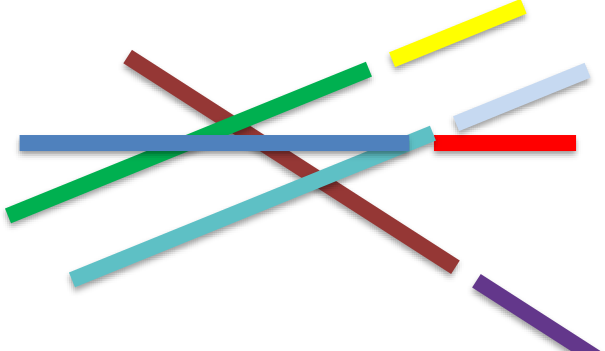
Multiple BOM elements

McKinsey: reimagining industrial supply chains

- Automotive: 250 1st-tiers to 18.000 total subtiers
- Aerospace manuf.: 200 1st-tiers to 12.000 total
- Tech companies: 125 1st tiers to 7.000 all subtiers



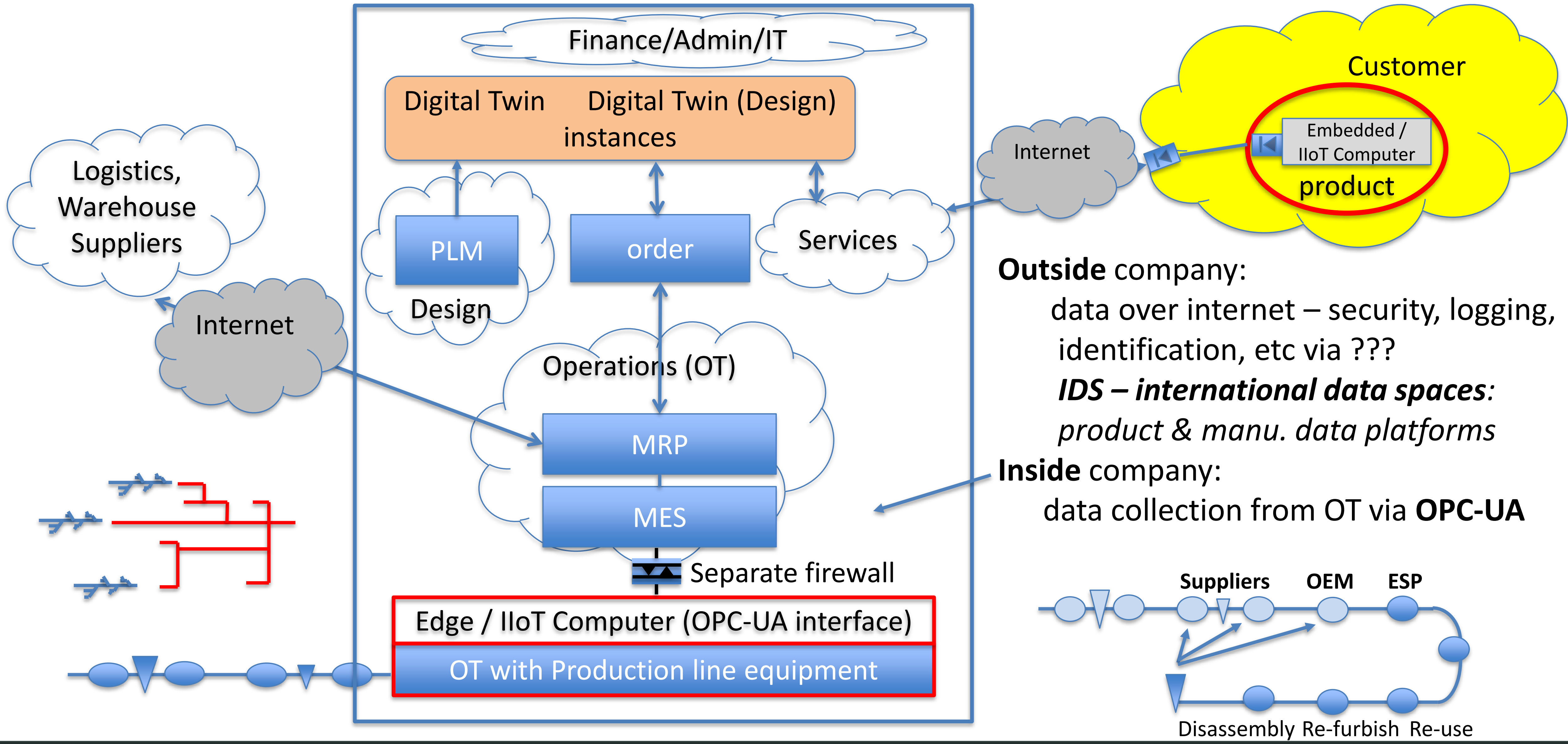
Manufacturing data platform to exchange data for deep chain planning & control



Many different value chains => value constellation

Optimize not one chain, but your whole manufacturing eco-system

Data Collection from supply chain, production and product usage



Outside company:

data over internet – security, logging, identification, etc via ???

IDS – international data spaces:

product & manu. data platforms

Inside company:

data collection from OT via **OPC-UA**

Content – data driven business and cyber security at the factory floor and value chains

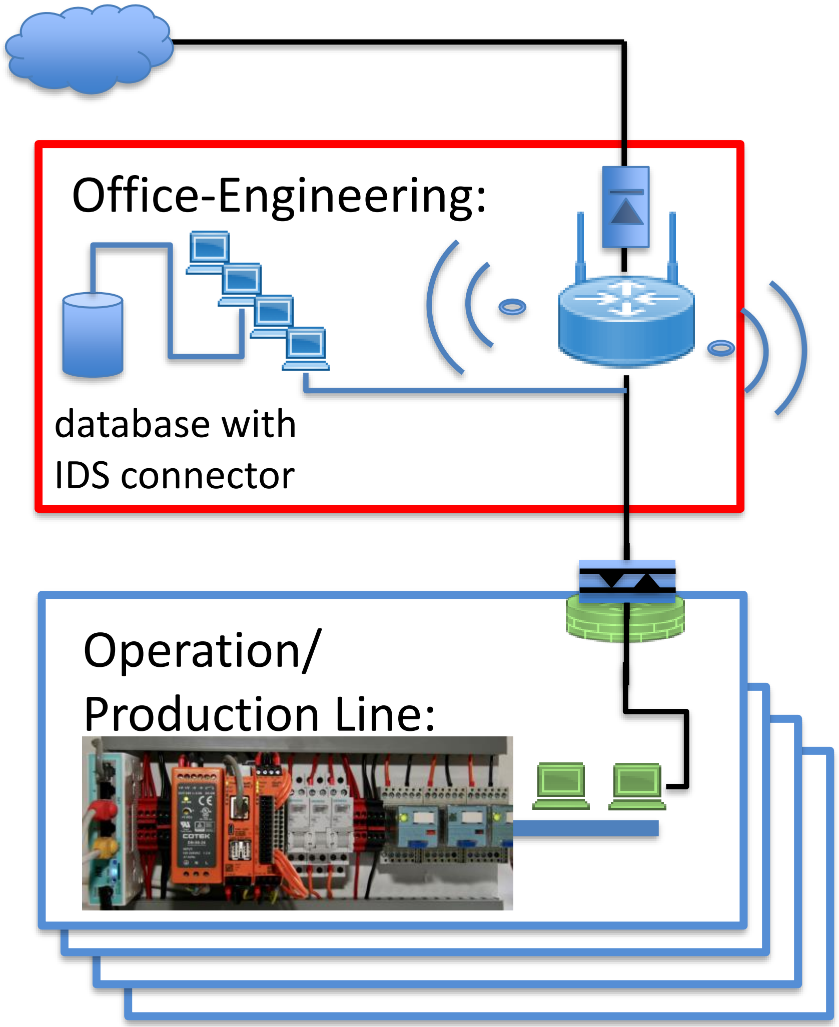
Flexible Manufacturing
Smart Products
Advanced Manufacturing
Servitization
Manufacturing technologies
3D
Smart Industry
Network Centric
Digitization
1100110100
1110001100
10011000
Smart Working
Digital Factory
Sustainable Factory
Connected Factories

1. Introduction
2. Vision – from digital via smart to sustainable

   more and more all data driven
3. Data – from machine data to digital twinning

   and legal issues and data eco-systems/platforms
4. OT-data - focus on cyber securing the data from the factory production line
5. Training workshop - Factory floor cyber security in a day / open source training
6. Conclusion - Life-long learning on digital skills

Factory subnet network for IIoT data sharing and cyber security in factories



Business-2-Business/Customer data exch:
IDS for B2B (IDS= international datas spaces)
(intercloud standard with clearing, etc)

IT-environment
Company database/storage, cloud interface (int. & ext.)

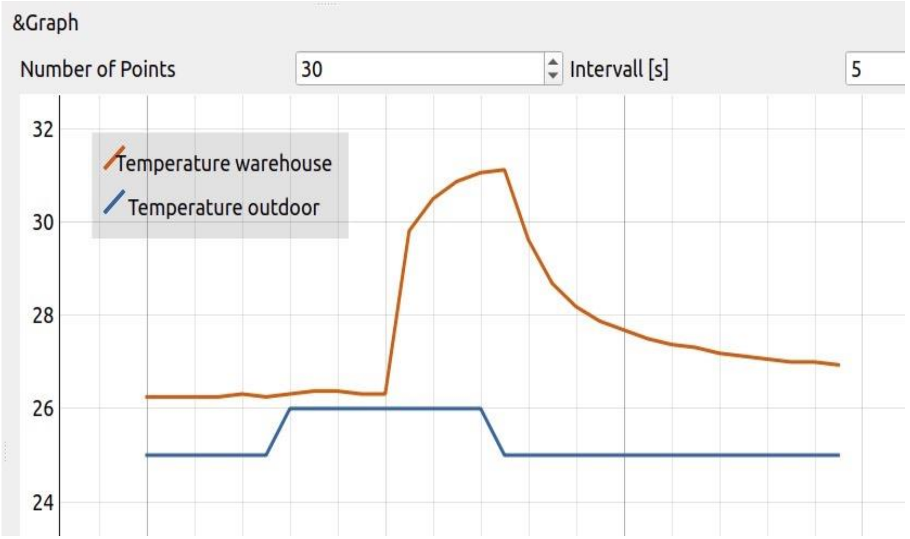
OT-environment
no Wifi, no USB, locked firewall with only OPC-UA passing

So IoT/equipment data goes first through your own firewall with OPC-UA into your database and there you decide which data could be shared using IDS with others.

But how?
No-one told us

Digital skills??

Example data collection workshop: Temperature monitoring on 2 streams

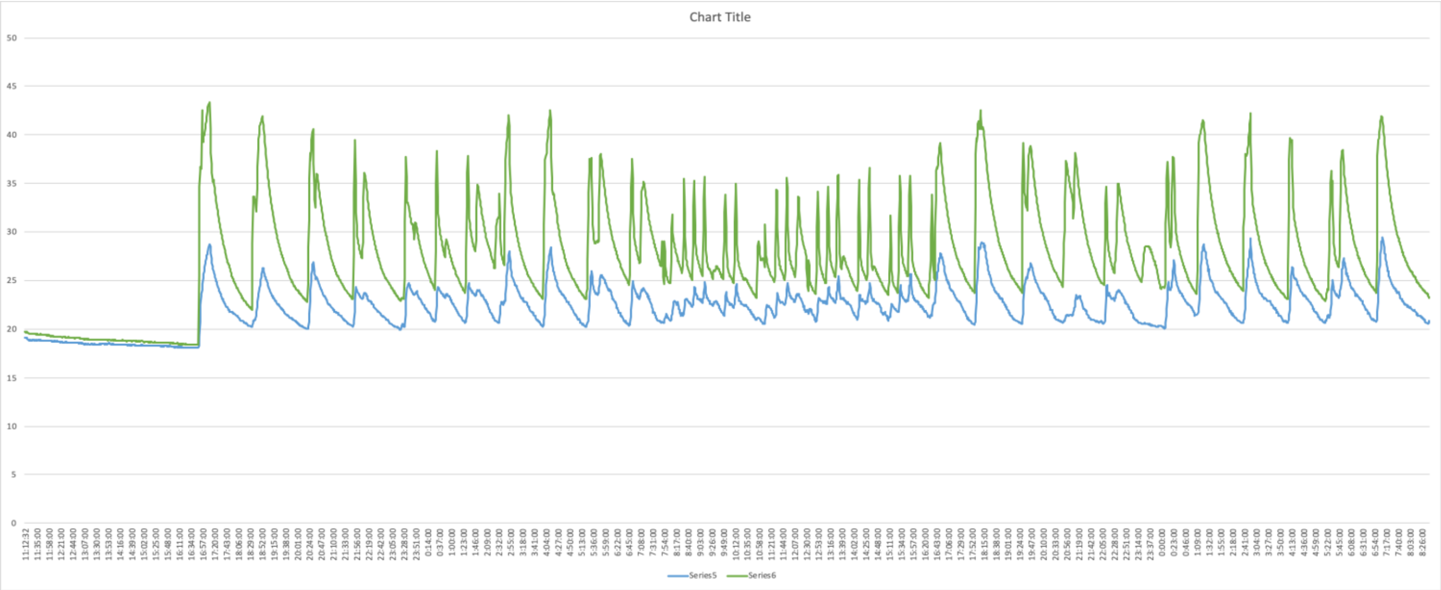


&Graph

Number of Points 30

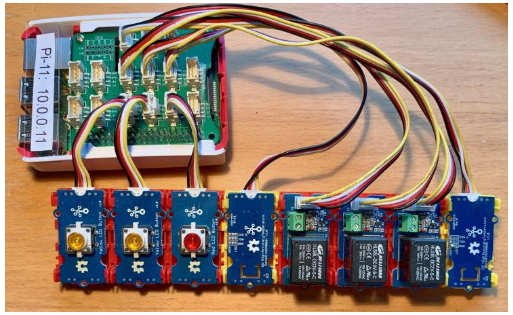
Intervall [s] 5

a few test points



More realistic: 3 days, every minute

500 € Kunbus + 24VDC IO



100 € Pi with 5V IO

```
....
async with opc_server:
   while True:
      await asyncio.sleep(60)
      await opc_temperature.set_value(tem.tem)
      time_stamp = datetime.now()
      print('{}, '.format(time_stamp.strftime("%X")),
         '{0:.1f}'.format(tem.tem))
....
```

In workshop participants collect data using Pi+Python

IIoT (Industrial Internet-of-Thing, sometime edge) computing with industrial graded (24VDC) data collection

Kunbus Revolution Pi: RevPi (www.evolution.kunbus.de)

RevPi: hardware based on RaspberryPi

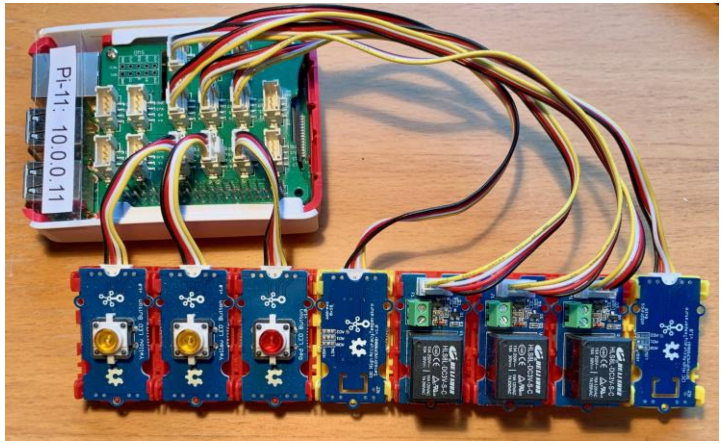
local: HDMI screen, USB keyboard+mouse

network: Ethernet/IP (remote login SSH, ….)

RevPi: software www.revpimodio.org (open source)

OS: Raspbian with realtime adaption, open source Linux

App: Programmable in Python, C or IEC 61131



Raspberry Pi

with Seeed I/O

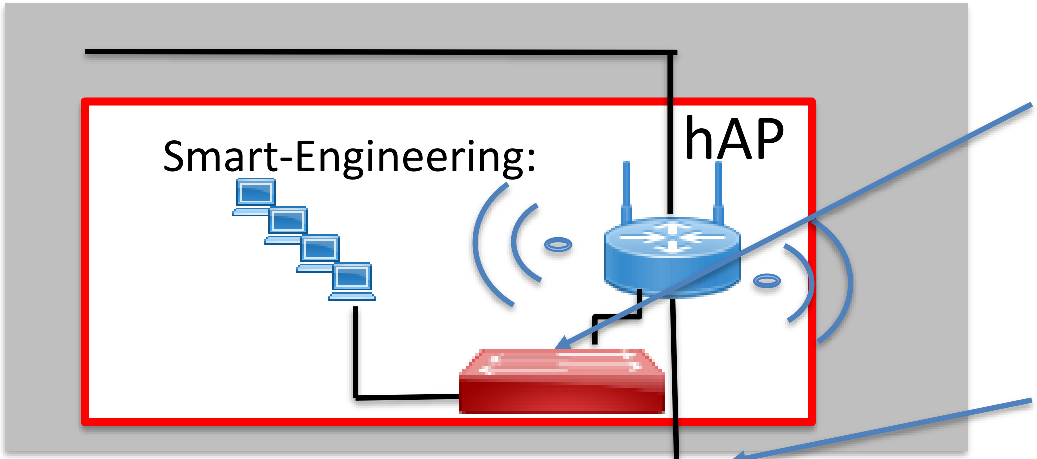
3 input button with light

3 relays

2 temperature sensors

Once workshop participants start to receive data, they are hacked, and hacked and hacked again …..

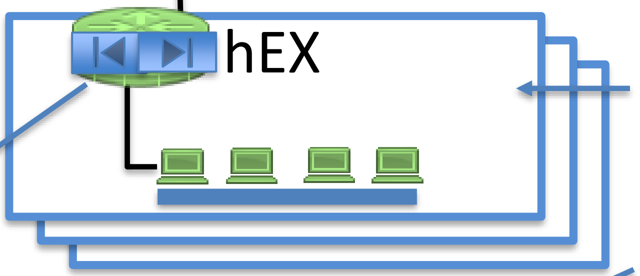
Factory 10-net and behind 10.0.0.254 Production line 192-subnet



10.0.0.1 = LAN side of router/firewall 1 (the Mikrotek 100 E hAP)

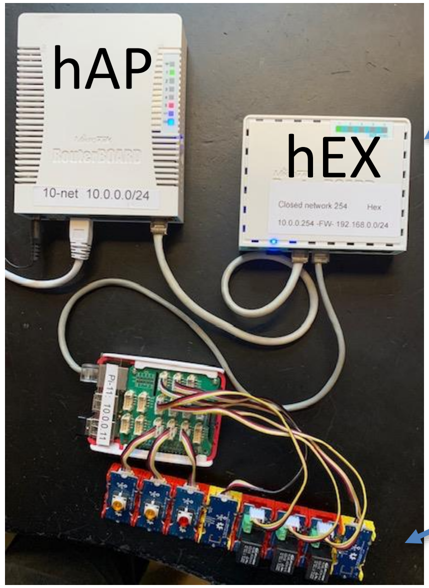
10.0.0.20-100 = notebook PC’s on Wifi network with OPCUA client

10.0.0.253 = WAN side of router/firewall 2 (the 50 Euro hEX)



192.168.0.1 = LAN side of router/firewall 2

192.168.0.11 = Pi-11 (with OPCUA server)



Note: handy PoE supply from port 5 of hAP to port 1 of the hEX

Standard password changes, hidden users, hidden software, … grrrh Ultimately, they put their Pi behind a double locked (in/out) firewall)

Firewalls: some basics

Traffic between LAN’s passing a router with firewall rules

Traffic to the router (INPUT), from the router (OUTPUT), going through (FORWARD) & (src/dst) NATs

Rules for INPUT chain protects the router, rules for the FORWARD chain controls flow into/from the LAN

Rules behave as “if condition then action’ as in: *IF invalid packet THEN drop*

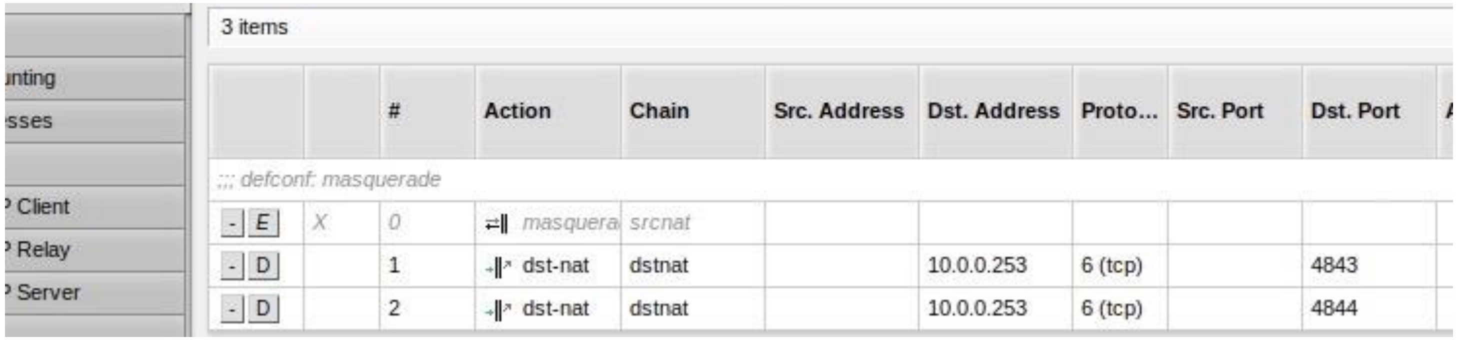
Rules are grouped in chains and executed in following order,

so first protect your router (INPUT chain), then look in FORWARD chain, etc

Mikrotik routerOS example firewall rules:

chain=dstnat **dst-address=10.0.0.253 dst-port=4843 protocol=tcp to-addresses=192.168.0.3 to-ports=4840**

add action=dst-nat log=yes comment=“allow OPC-UA (port 4843) client at firewall (10.0.0.254) go for OPC-UA server (4840) on 192.168.0.3 (RevPi-3)”

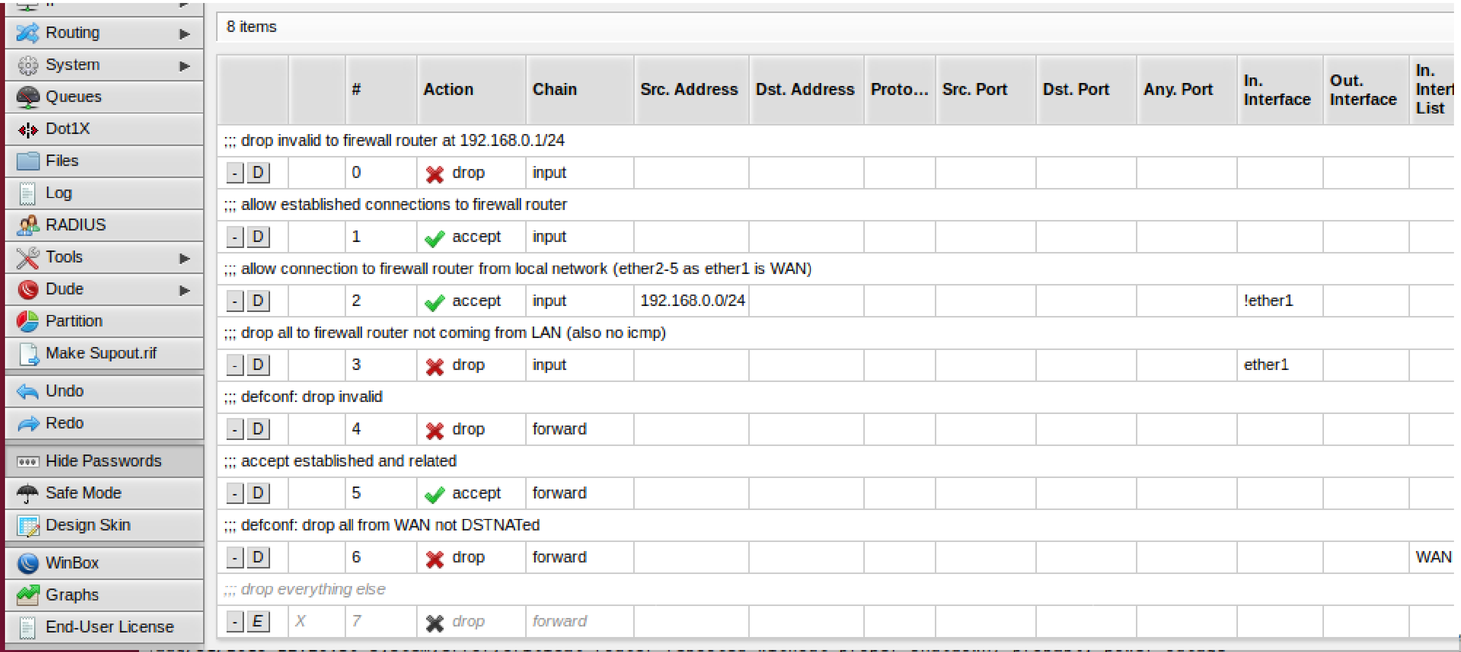


3 items

		#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
;;; defconf: masquerade									
- E	X	0	⇄ masquera	srcnat					
- D		1	dst-nat	dstnat		10.0.0.253	6 (tcp)		4843
- D		2	dst-nat	dstnat		10.0.0.253	6 (tcp)		4844

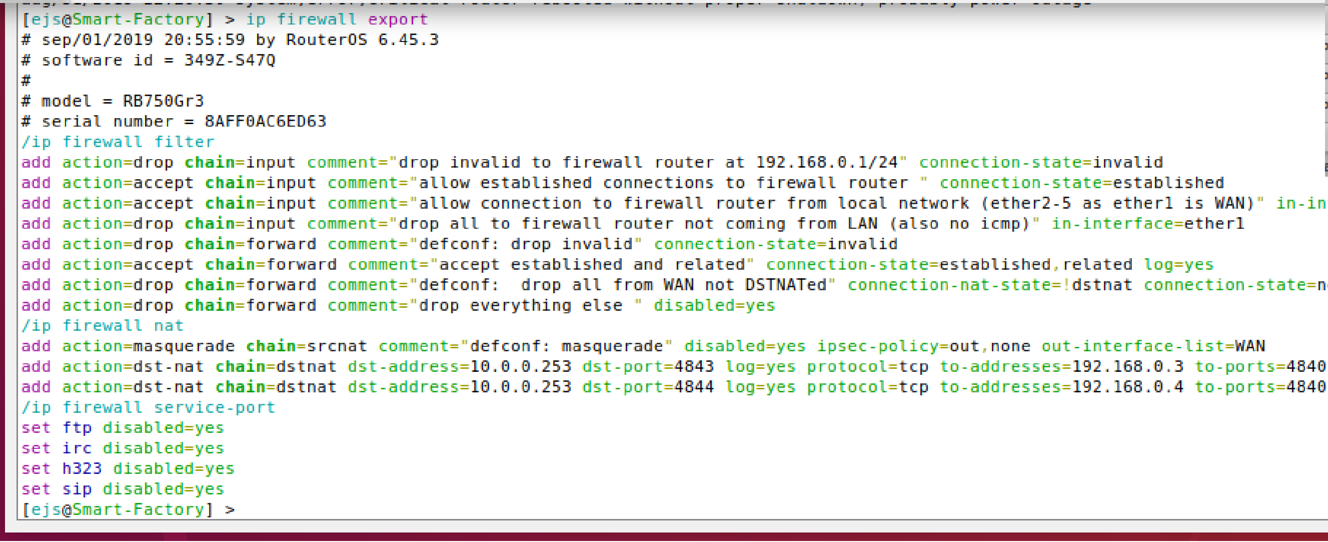
Firewalls can be very complex,
But in this case, it is simple,
block all traffic except OPC-UA

Smart-Factory: details

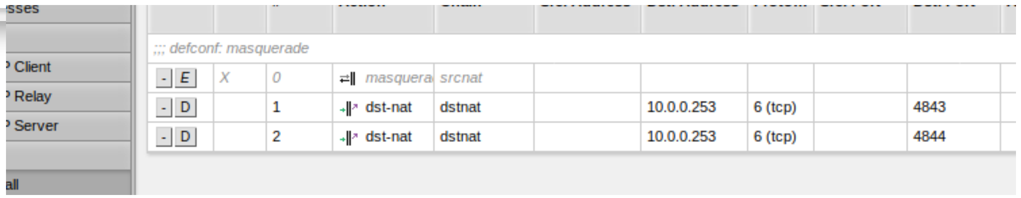


8 items

		#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interf List
;;; drop invalid to firewall router at 192.168.0.1/24													
-	D	0	✗ drop	input									
;;; allow established connections to firewall router													
-	D	1	✓ accept	input									
;;; allow connection to firewall router from local network (ether2-5 as ether1 is WAN)													
-	D	2	✓ accept	input	192.168.0.0/24						!ether1		
;;; drop all to firewall router not coming from LAN (also no icmp)													
-	D	3	✗ drop	input							ether1		
;;; defconf: drop invalid													
-	D	4	✗ drop	forward									
;;; accept established and related													
-	D	5	✓ accept	forward									
;;; defconf: drop all from WAN not DSTNATed													
-	D	6	✗ drop	forward									WAN
;;; drop everything else													
-	E	X	7	✗ drop	forward								



```
[ejs@Smart-Factory] > ip firewall export
# sep/01/2019 20:55:59 by RouterOS 6.45.3
# software id = 349Z-S47Q
#
# model = RB750Gr3
# serial number = 8AFF0AC6ED63
/ip firewall filter
add action=drop chain=input comment="drop invalid to firewall router at 192.168.0.1/24" connection-state=invalid
add action=accept chain=input comment="allow established connections to firewall router " connection-state=established
add action=accept chain=input comment="allow connection to firewall router from local network (ether2-5 as ether1 is WAN)" in-interface=!ether1 src-address=192.168.0.0/24
add action=drop chain=input comment="drop all to firewall router not coming from LAN (also no icmp)" in-interface=ether1
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=forward comment="accept established and related" connection-state=established,related log=yes
add action=drop chain=forward comment="defconf:  drop all from WAN not DSTNATed" connection-nat-state=!dstnat connection-state=new in-interface-list=WAN
add action=drop chain=forward comment="drop everything else " disabled=yes
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" disabled=yes ipsec-policy=out,none out-interface-list=WAN
add action=dst-nat chain=dstnat dst-address=10.0.0.253 dst-port=4843 log=yes protocol=tcp to-addresses=192.168.0.3 to-ports=4840
add action=dst-nat chain=dstnat dst-address=10.0.0.253 dst-port=4844 log=yes protocol=tcp to-addresses=192.168.0.4 to-ports=4840
/ip firewall service-port
set ftp disabled=yes
set irc disabled=yes
set h323 disabled=yes
set sip disabled=yes
[ejs@Smart-Factory] >
```



;;; defconf: masquerade										
-	E	X	0	masquera	srcnat					
-	D		1	dst-nat	dstnat		10.0.0.253	6 (tcp)		4843
-	D		2	dst-nat	dstnat		10.0.0.253	6 (tcp)		4844

Tightly locked down OT subnet

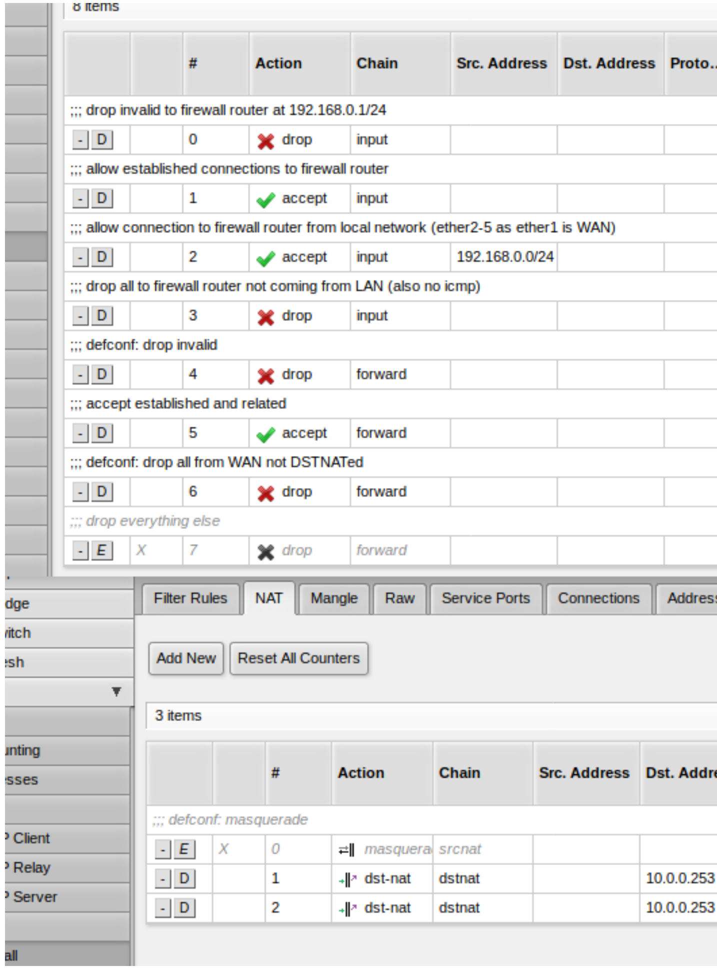
- Only local traffic
- Only input to router from OT-subnet
- NAT (or scrNat) is blocked
  - that is: no traffic to outside
- Only OPC-UA is *dstNat*
  (i.e. allowed through firewall)
- Rest is dropped

- No other access from outside (WAN), and no traffic from inside (except opc-ua)

Subnet 192.168.0.0/24 – tightly locked down firewall

E.g. router Mikrotik hEX (1 WAN port (ether1=10.0.0.254) + 4-LAN (ether2-5=192.168.0.0/24) Gigabit port router, no wifi)

```
/ip firewall filter
# chain input (to router itself for router managment)
add action=drop      chain=input    connection-state=invalid      comment="drop invalid to firewall router at 192.168.0.1/24"
add action=accept    chain=input    connection-state=established  comment="allow established connections to firewall router "

# allow management connection to firewall router from local network (!ether1 implies ether2-5 (=LAN) as ether1 is WAN),
# so next rules state accept all local LAN traffic, drop all remain WAN traffic
add action=accept    chain=input    in-interface=!ether1     src-address=192.168.0.0/24
add action=drop      chain=input    in-interface=ether1      comment="drop all to firewall router not coming from LAN (also no icmp)"

# chain forward from WAN (ether port 1) to LAN (ether port 2-5) or vice versa
add action=drop      chain=forward   connection-state=invalid                comment="drop invalid"
add action=accept    chain=forward   connection-state=established,related    comment="accept established and related"
add action=drop      chain=forward   in-interface-list=WAN   connection-nat-state=!dstnat      connection-state=new
                                                   comment="drop all from WAN not dstNATed"
add action=drop      chain=forward   disabled=yes                            comment="drop everything else "

/ip firewall nat
# scrnat disabled (source network address translation is e.g. web request (port 80) from a PC to external webserver)
add action=masquerade    chain=srcnat      comment="masquerade" disabled=yes      ipsec-policy=out,none out-interface-list=WAN

# dstnat is request from outside via firewall (10.0.0.254) on port 54843 to internal device (192.168.0.3) with opcua server (port 4840)
add action=dst-nat           chain=dstnat dst-address=10.0.0.254 dst-port=54843 log=yes protocol=tcp to-addresses=192.168.0.3 to-ports=4840

# in LAN everyone can call OPC server at ocp:tcp://192.168.0.3:4840 (port 4840). From outside call the router 10.0.0.254 at port 54843
```



8 items

		#	Action	Chain	Src. Address	Dst. Address	Proto..
;;; drop invalid to firewall router at 192.168.0.1/24							
- D		0	✗ drop	input			
;;; allow established connections to firewall router							
- D		1	✓ accept	input			
;;; allow connection to firewall router from local network (ether2-5 as ether1 is WAN)							
- D		2	✓ accept	input	192.168.0.0/24		
;;; drop all to firewall router not coming from LAN (also no icmp)							
- D		3	✗ drop	input			
;;; defconf: drop invalid							
- D		4	✗ drop	forward			
;;; accept established and related							
- D		5	✓ accept	forward			
;;; defconf: drop all from WAN not DSTNATed							
- D		6	✗ drop	forward			
;;; drop everything else							
- E	X	7	✗ drop	forward			

3 items

		#	Action	Chain	Src. Address	Dst. Addre
;;; defconf: masquerade						
- E	X	0	masquera	srcnat		
- D		1	dst-nat	dstnat		10.0.0.253
- D		2	dst-nat	dstnat		10.0.0.253

See also: www.github.com/ejsol/Smart-industry-zelf-aan-de-slag to download hEX firewall script

Smart Industry Talks channel on Youtube & www.smartindustry.nl/aan-de-slag/academy

In Dutch:

Smart Industry Talk – Overview in NL (white paper) – (18 min) https://www.youtube.com/watch?v=1IlwzUK91MM&t=29s
+ podcast (MP3) + PDF slides on www.smartindustry.nl/aan-de-slag/academy

Whitepaper video‘s in NL

W1: Robuuste waardeketens – (6 min) https://youtu.be/JVGTqgZmp_E
W2: Leven lang leren – (7 min) https://youtu.be/nFcE9ZXFArM
W3: De flexibele fabriek – (6 min) https://youtu.be/BQt6B1zAYDY

Skills video’s

S1: Digitale skills – (2.13 min) https://youtu.be/aZiBDOxaCO4

Tech video’s in NL

T1: Van PLC via IIoT naar Edge systems – (11 min) https://youtu.be/aQhXxUl1FWE
T2: Raspberry Pi, Revolution Pi (IIoT) en de Nvidia Jetsons (AI-edge) – (8,5 min) https://youtu.be/Meu70SwoQEw
T3: Open Systems voor industriële toepassingen – (10 min) https://youtu.be/Fv_Gq_9RTMM
T4: Python I/O control en data collectie demo – (11 min) https://youtu.be/Wi9pho5mSyw
T4a: Pi configuration, Python Libraries and other hand-ons to get started – (12 min) https://www.youtube.com/watch?v=70Gfp0o2wxw
T5: Kunbus Revolution Pi IIoT Python programma‘s – (8 min) https://youtu.be/8h9R-XGnZyE
T6: Ethernet/IP en OPC-UA – (9 min) https://youtu.be/9TAIcokQXJQ
T7: OPC-UA programming and use of the the Raspberry Pi – (8 min) https://www.youtube.com/watch?v=aoJbAsG0y5c
T8: On cyber security in OT environment (shopfloor networks & equipment) – (12 min) https://www.youtube.com/watch?v=3-mUw1aeQFI
T9: A locked firewall blocking in/out traffic except OPC-UA with Mikrotik – (12 min) https://www.youtube.com/watch?v=CyxfYzN-Hew

All open-source material:
(Youtube, Github)
In Dutch due to target audience.
Still to decide on English version,
but slides are all in English.

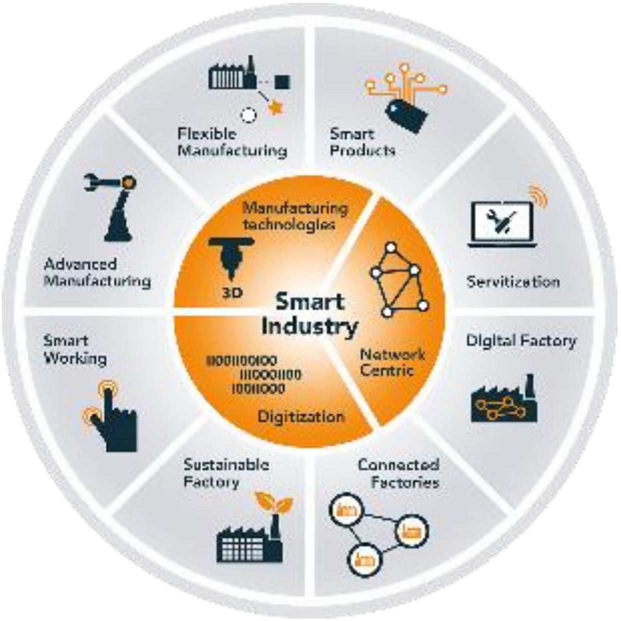
In English

Smart Industry Talk - Overview in English - (22 min) https://youtu.be/rqc2j8AHS2k
+ podcast (MP3) + PDF of slide on www.smartindustry.nl/aan-de-slag/academy

Data Talks - collecting, cleaning/storing, exchange standards, data visualization, data analytics and AI, AI use in manufacturing

Data 1: data ecosystems, ownership, sovereignty, legal – (12 min) https://youtu.be/7LQFNqR8p5c
Data 2: data platforms/eco-systems and cyber security - (8 min) https://youtu.be/B3txm5yv3Dc
Data 3: collecting and visualizing industrial (IoT) data using Python, Excel, .. - (12 min) https://youtu.be/BX3PyByXU9s

Content – data driven business and cyber security at the factory floor and value chains

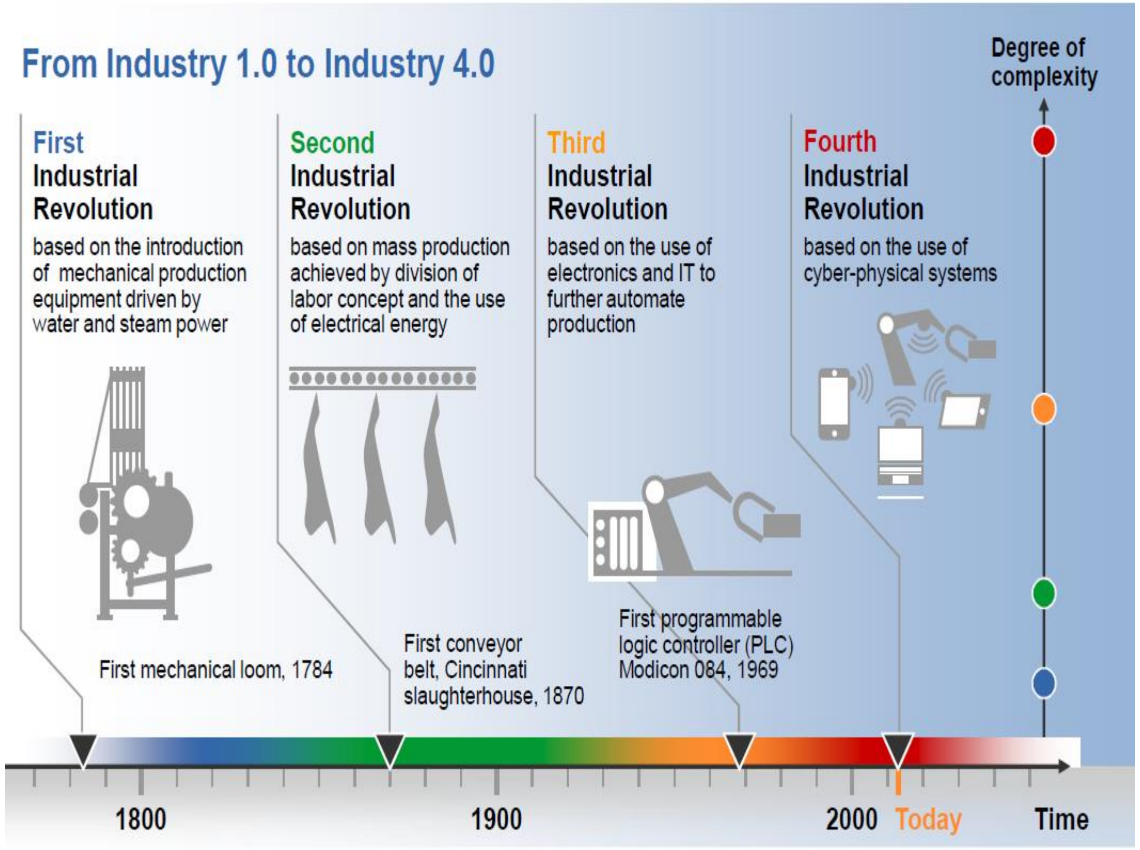


1. Introduction
2. Vision – from digital via smart to sustainable

   more and more all data driven
3. Data – from machine data to digital twinning

   and legal issues and data eco-systems/platforms
4. OT-data - focus on cyber securing the data from the factory production line
5. Training workshop - Factory floor cyber security in a day / open source training
6. Conclusion - Life-long learning on digital skill – *two slides to remember*

Every industrial job will change completely in your life time



From Industry 1.0 to Industry 4.0

First Industrial Revolution
based on the introduction of mechanical production equipment driven by water and steam power

Second Industrial Revolution
based on mass production achieved by division of labor concept and the use of electrical energy

Third Industrial Revolution
based on the use of electronics and IT to further automate production

Fourth Industrial Revolution
based on the use of cyber-physical systems

First mechanical loom, 1784

First conveyor belt, Cincinnati slaughterhouse, 1870

First programmable logic controller (PLC) Modicon 084, 1969

Source: DFKI (2011)

Unrestricted © Siemens AG 2013. All rights reserved.

1600 Sawmill/Sailboat/Wood
180 years, 6 working life generations of 30 years
craftsmanship went from father to son

1780 Steam Engine/Steel
110 years, 4 generations

1890 Conveyor belt Mass prod.
70 years, 3 generations

1960 Mainframe, PLC, Robots
40 years, 1 generation

2000 Internet (of Things)
25 years, < 1 generation
& life-long learning a must

2030 Servitisation & Sustainability – all digital value chains

Never ever in mankind: Lifelong learning becomes a must

If you are **35 years and older**, you were in 2000 15 year or older
and you did had Internet at school and did **not get any digital training at school**

Now we have Internet of Things (IoT) and as a result Smart Industry:
connecting everything with everything

Within 10 years artificial intelligence and quantum computing will impact
and we can't predict what the industrial consequences will be,
but life-long learning is, the first time in mankind, a must.

We designed a 1-day cyber security on the shopfloor workshop,
But what else can we do?

Smart Industry

This work was made possible by TNO with support for the ministry of economic affairs and climate (EZK) of the Netherlands

Smart Industry is a program by FME, Metaalunie, Chamber of Commerce, min. Of EZK and TNO, the Dutch research & tech. org.

More information and other videos www.smartindustry.nl

(topics: strategy, data, and technology in English and Dutch)

Egbert-Jan Sol (TNO) has a PhD in robotics, 40-year experience in industry and research and is currently program director of Smart Industry program
and previous CTO of TNO Industry/director of TNO High-tech Systems & Materials
From 1990-1998 he was part-time full professor Industrial Automation at the TU/e
and from 2012-2020 professor Innovation mgt at the Radboud University, Nijmegen.