# Safety, Security and Digital Twins -

The red line between these ecosystems

# Context

- IACS, OT, SAS

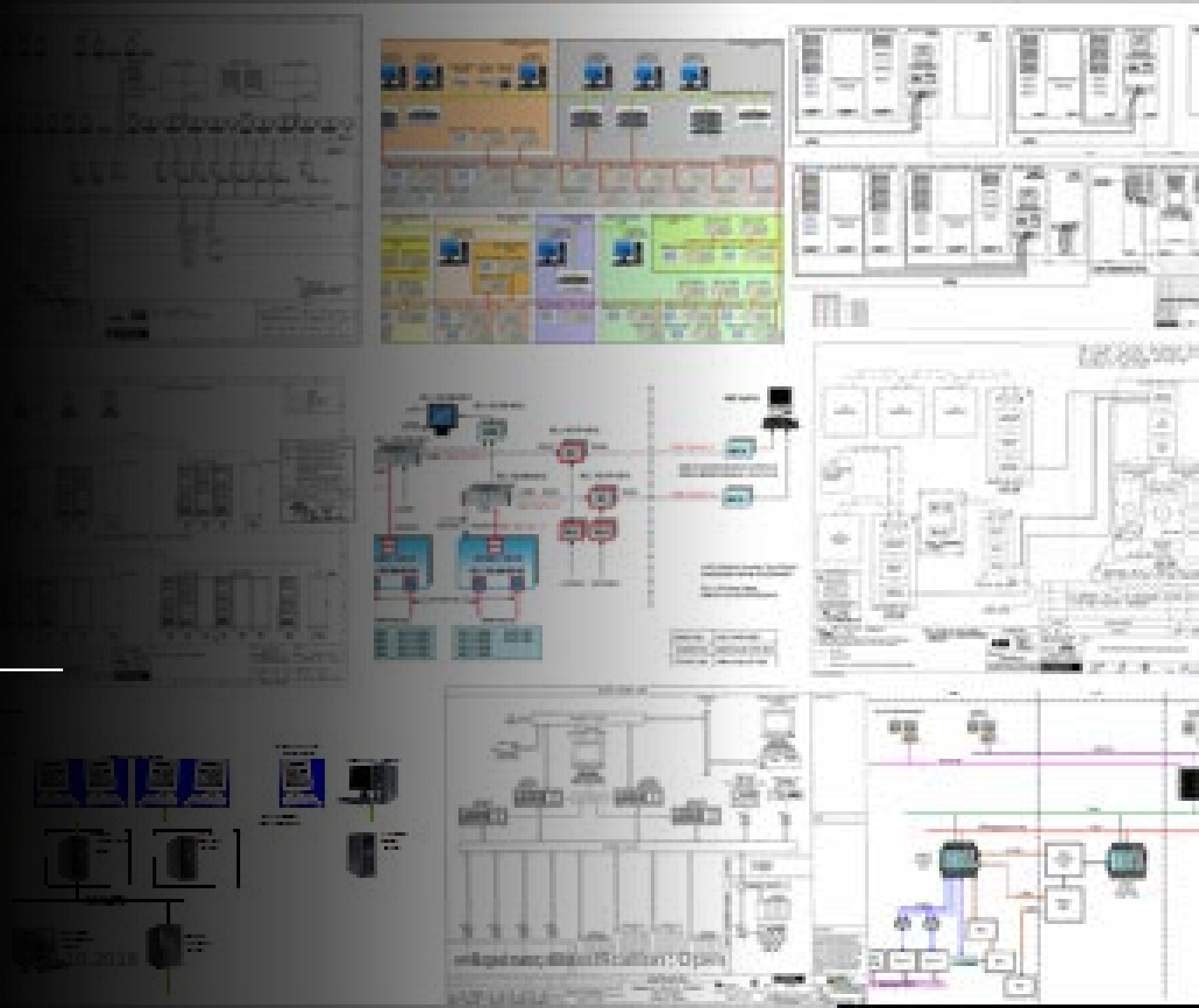
# List of abbreviations

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AAL | Active Assisted Living |
| acatech | German National Academy of Science and Engineering |
| AK_STD | *Arbeitskreis Standardisierung* (Working Group Standardization) |
| AAS | Asset Administration Shell |
| AASX | Asset Administration Shell Explorer |
| ADT | Abstract data type |
| AML | Automation Markup Language |
| B2B | Business-to-Business |
| BITKOM | *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.* (Federal Association for Information Technology, Telecommunications and New Media) |
| BMBF | *Bundesministerien für Bildung und Forschung* (Federal Ministries of Education and Research) |
| BMEcat | Catalog standard for your e-business |
| BMWi | *Bundesministerium für Wirtschaft und Energie* (Federal Ministry for Economic Affairs and Technology) |
| BSD | Berkeley Software Distribution |
| BSI | *Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)* |
| BZKI | *Begleitforschung für zuverlässige Kommunikation in der Industrie (Accompanying Research – Reliable wireless communication in industry)* |
| CDD | Common Data Dictionary |
| CEN | *Comité Européen de Normalisation*/European Committee for Standardization |
| CENELEC | *Comité Européen de Normalisation Électrotechnique*/ European Committee for Electrotechnical Standardization |
| CPPS | Cyber Physical Production System |
| CPS | Cyber Physical System |
| CVRF | Common Vulnerability Reporting Framework |
| DEI | Digitising European Industry |
| DG CONNECT | Directorate Generale CONNECT |
| DG GROW | Directorate General GROW |
| DG RTD | Directorate General Research and Innovation |
| DIN | *Deutsches Institut für Normung e. V.* (German Institute for Standardization) |
| DIN SPEC | DIN Specification |
| DKE | *Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE* (German Commission for Electrical, Electronic & Information Technologies of DIN and VDE) |
| DNS | German Standardization Strategy |
| EBN | R & D phase standardization |
| EDDL | Electronic Device Description Language |
| EN | *Europäische Norm* (European Standard) |
| EPL | Eclipse Public License |
| ERP | Enterprise Resource Planning |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| GL | *Grundlagen* (Fundamentals) |
| GMA | *VDI/VDE Gesellschaft Mess- und Automatisierungstechnik* (VDI/VDE Society for Measurement and Automatic Control) |
| GUI | Graphic User Interface |
| HAZOP | Hazard and Operability Process |
| HE | *Handlungsempfehlung* (Recommendation for action) |
| HTTP | Hypertext Transfer Protocol |
| IACS | Industrial Automation and Control System |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| ICT | Information and communications technology |
| IML | Fraunhofer Institute for Material Flow and Logistics |
| IOSB | Fraunhofer Institute of Optronics, System Technologies and Image Exploitation |
| ICT | Fraunhofer Institute for Information and Communications Technologies |
| IoT | Internet of Things |
| IPA | Fraunhofer Institute for Process Automation |
| IIoT | Industrial Internet of Things |
| IPA | Fraunhofer Institute for Manufacturing Engineering and Automation |
| IP45G | Information platform for 5 G – Industrial Internet |
| ISA | International Society of Automation |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITA | Industry Technical Agreement |
| ITG | *Informationstechnische Gesellschaft im VDE* (VDE Information Technology Society) |
| ITU | International Telecommunication Union |
| ITU-R | International Telecommunication Union, Radiocommunication Sector |
| JETI | JTC1 Emerging Technology and Innovation |
| JIS | Joint Initiative on Standardization |
| JTC | Joint Technical Committee der IEC und ISO |
| JSON | JavaScript Object Notation |
| JWG | Joint Working Group |
| AI | Artificial Intelligence |
| KMU | *Klein- und Mittelständische Unternehmen* (Small- and mid-sized enterprises, SMEs) |
| LGPL | Lesser General Public License |
| LNI 4.0 | Labs Network I 4.0 |
| M2M | Machine-2-machine |
| MOM | Manufacturing operations management |
| MPL | Mozilla Public License |
| MRK | *Mensch-Roboter-Kollaboration* (human-robot collaboration) |
| NA/NIA | DIN Standards Committee on Information Technology and Selected Applications |
| NAMUR | User Association for Automation in Process Industries |
| NIST | National Institute of Standards and Technology (USA) |
| NLF | New Legislative Framework |
| DNS | German Standardization Strategy |
| OGC | Open Geospatial Consortium |
| OMG | Object Management Group |
| OPC-UA | Open Platform Communications – Unified Architecture |
| OpenAAS | Open Asset Administration Shell |
| OT | Operational Technologies |
| PAiCE | Platforms, Additive Manufacturing, Imaging, Communication, Engineering |
| PAS | Publicly Available Specification |
| PPP | Public Private Partnership |
| RAMI 4.0 | *Referenzarchitekturmodell Industrie 4.0* (Reference architecture model Industrie 4.0) |
| RDF | Resource Description Framework |
| RoboPORT | *Crowd-Engineering-Plattform für Robotik* (Crowd-Engineering platform for robotics) |
| RM-SA | *Referenzmodell-Systemarchitektur* (Reference model for system architecture) |
| ROSIN | *Qualitätsgesicherte ROS-Industrial-Softwarekomponenten* (Quality-assured ROS industrial software components) |
| SC | Sub-committee |
| SCI 4.0 | Standardization Council I 4.0 |
| SDO | Standards Developing Organization |
| SemAnz40 | *Semantische Allianz 4.0* (Semantic Alliance 4.0) |
| SeRoNet | *Service Roboter Netzwerk* (Service Robot Network) |
| SG | *Strategiegruppe* (Strategy Group) |
| SIL | Safety Integrity Level |
| SMCC | Smart Manufacturing Coordinating Committee (ISO) |
| SMB | Standardization Management Board (IEC) |
| SOA | *Service-orientierte Architektur* (Service-oriented architecture) |
| SSO | Standards Setting Organization |
| SyC SM | System Committee Smart Manufacturing (IEC) |
| TACNET 4.0 | *Taktiles Internet – Konsortium* (Tactile Internet – Consortium) |
| TC | Technical Committee |
| TCP | Transmission Control Protocol |
| TR | Technical Report |
| TS | Technical Specification |
| UK | *Unterkomitee* (Subcommittee) |
| UML | Unified Modelling Language |
| VDE | *Verband der Elektrotechnik, Elektronik und Informationstechnik e. V.* (Association for Electrical, Electronic & Information Technologies) |
| VDE AR | VDE Application rule |
| VDI | *Verein Deutscher Ingenieure e. V.* (Association of German Engineers) |
| VDI/VDE GMA | *VDI/VDE Gesellschaft Mess- und Automatisierungstechnik* (VDI/VDE Society for Measurement and Automatic Control) |
| VDMA | *Verband Deutscher Maschinen- und Anlagenbau e. V.* (German Engineering Federation) |
| VV | Administrative regulation |
| VWS | Administration shell |
| VWSiD | Administration shell in detail |
| W3C | World Wide Web Consortium |

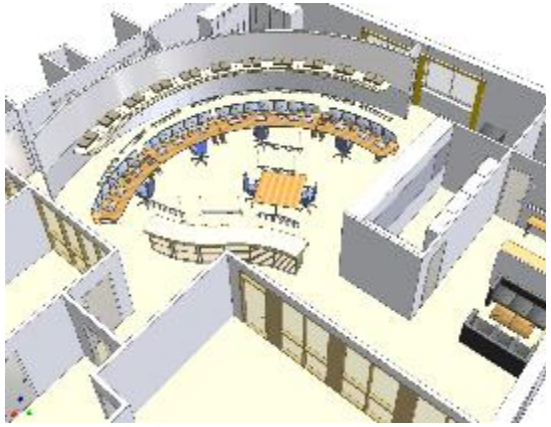
| | |
|---|---|
| WG | Working Group |
| WTO | World Trade Organization |
| WoT | Web of Things |
| XML | Extensible Markup Language |
| ZDKI | *Zuverlässige drahtlose Kommunikation* (reliable wireless communication) |
| ZVEI | *ZVEI Zentralverband Elektrotechnik- und Elektronikindustrie e. V.* (Central Association of the Electrical and Electronics Industry) |

# What is a typical IACS?

**I**ndustrial
**A**utomation and
**C**ontrol
**S**ystems



# Industrial Automation and Control Systems



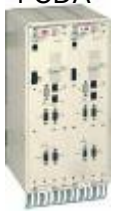
Meetering

Vistanet

CCC

Modbus

PCDA



Ethernet

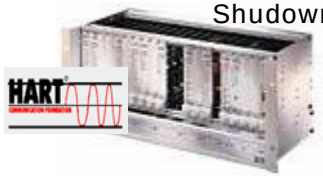
Safety Systems

H51q

Package unit

Electrical control

merge.ncy Shudown

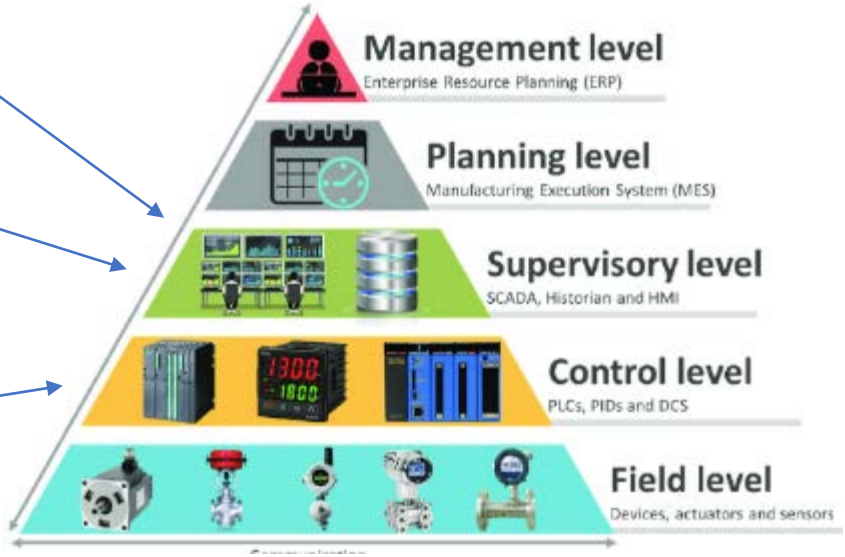




MCMS:

Speed drives

# Automation Pyramid



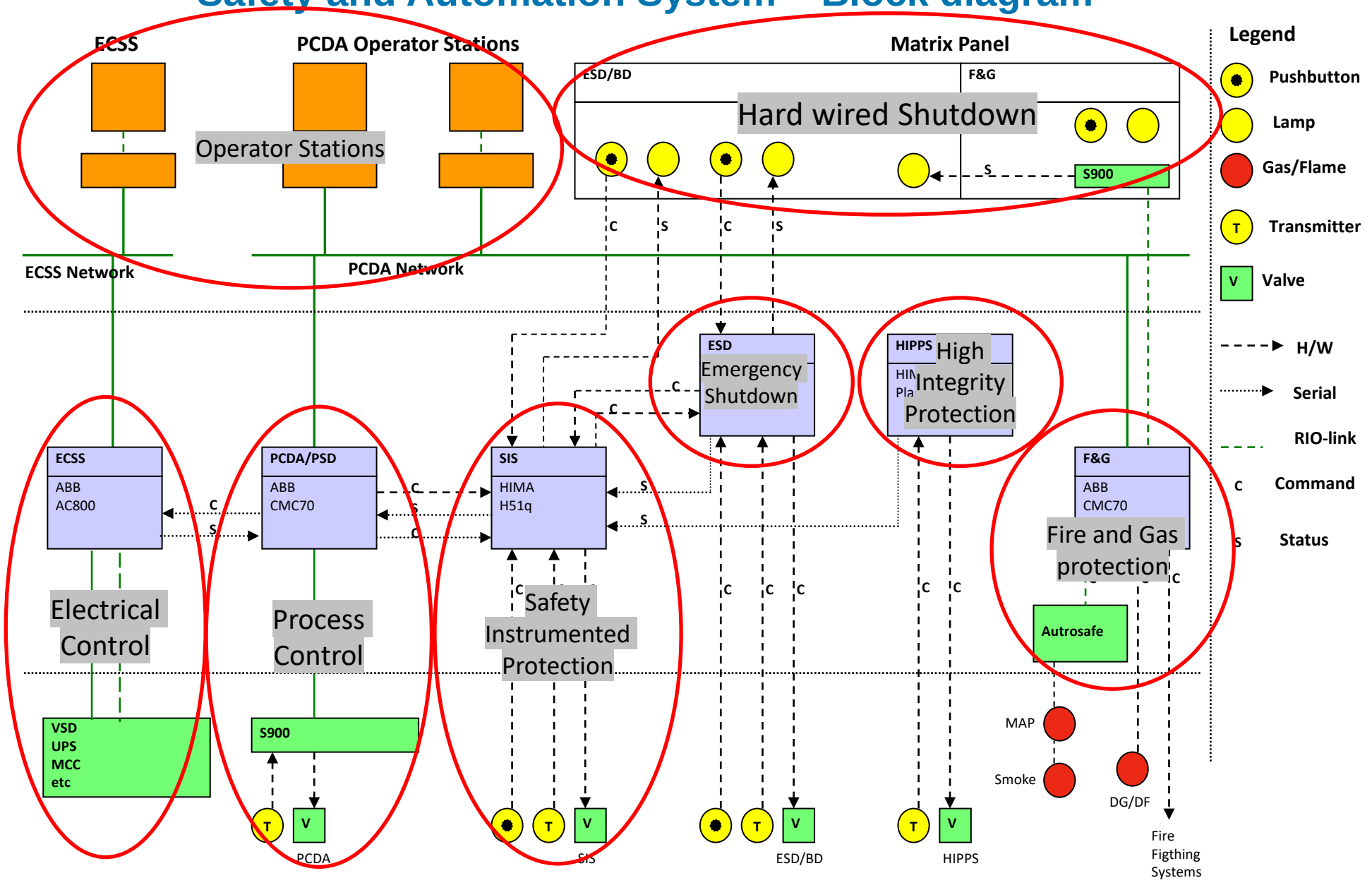
# IACS is:

- Connected systems
- High availability
- High consequence for equipment, people…
- Independent systems
- Several of them are part of the Performance Standards in the barrier management system (PS1-PS23)
- AIC vs CIA
- ….

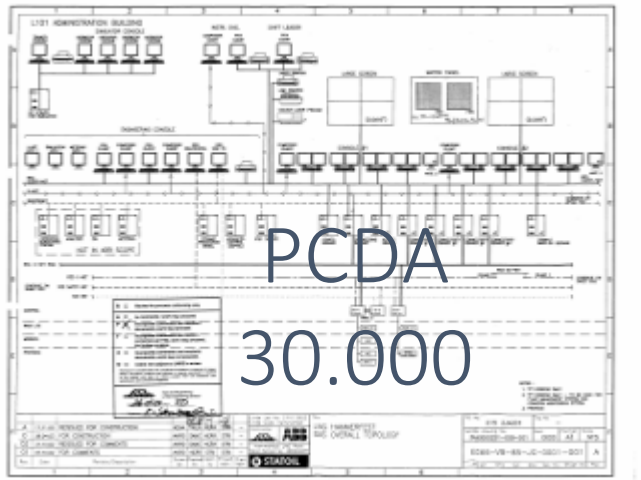
- Example:

Utility systems:
- Metering
- Machine control (turbo)
- Vibration

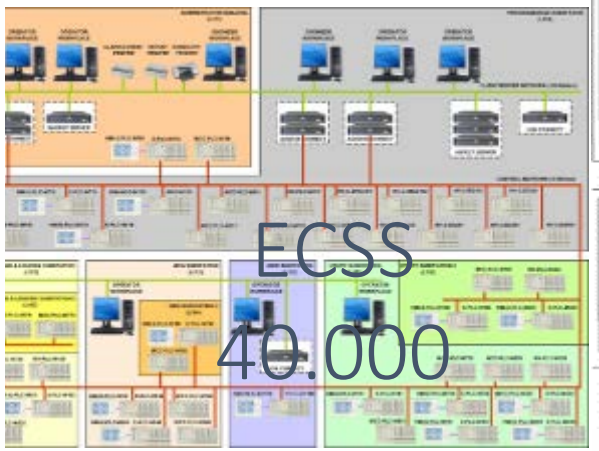
## Safety and Automation System – Block diagram



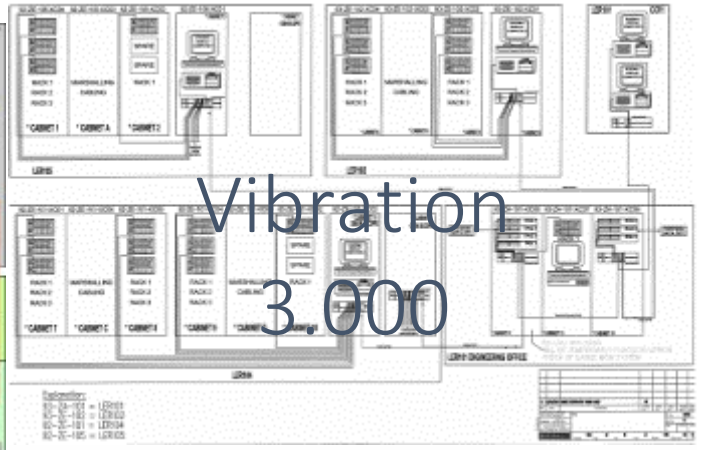
# Much spaghetti (Signals)



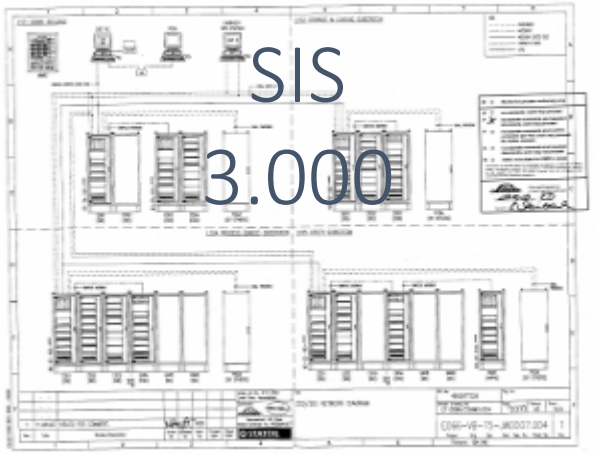
PCDA
30.000



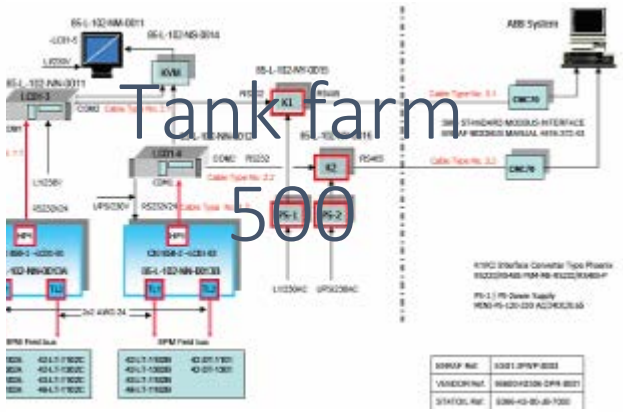
ECSS
40.000



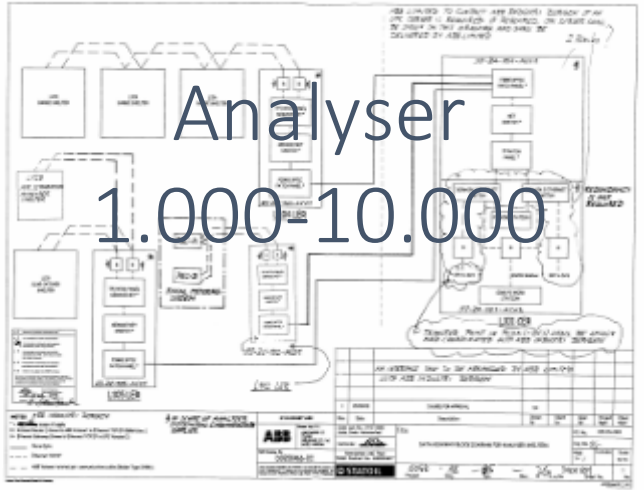
Vibration
3.000



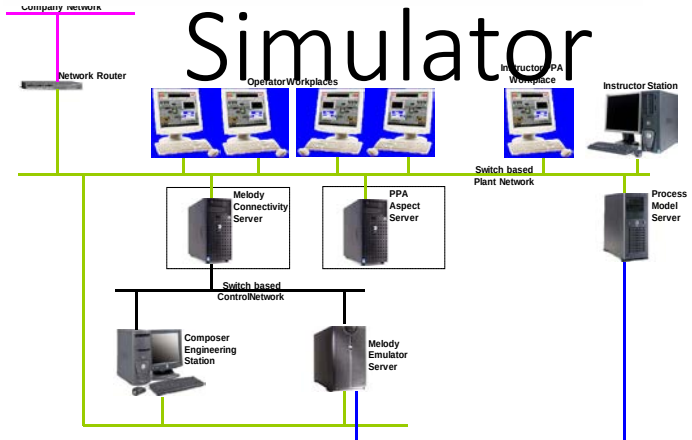
SIS
3.000



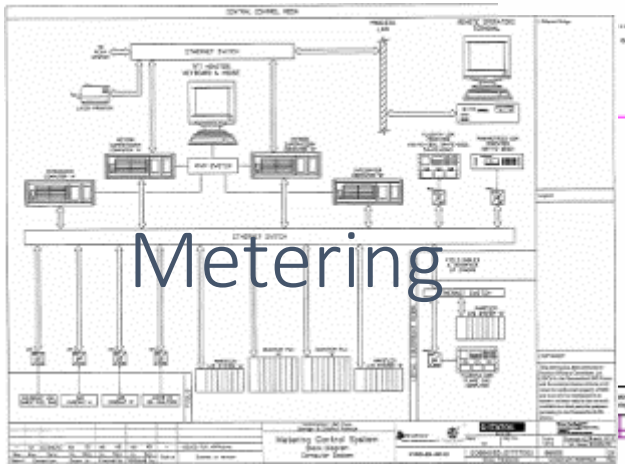
Tank farm
500



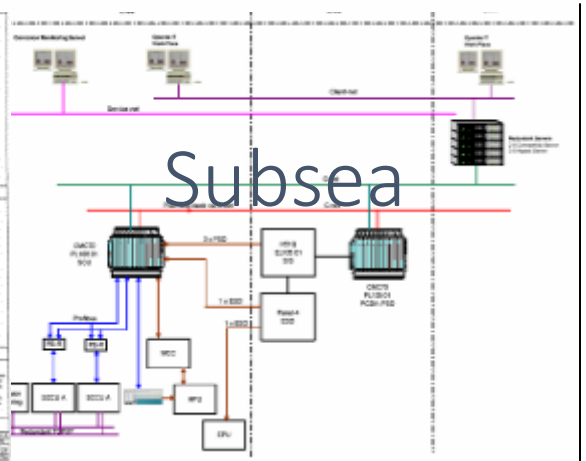
Analyser
1.000-10.000




Simulator



Metering



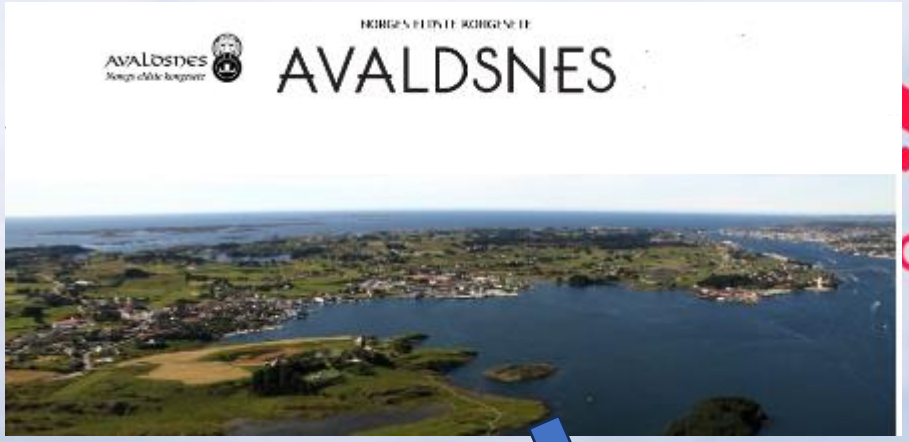
Subsea

# Some references before the rest of the story (i.e. anchoring of the story)

**Develop a resilient and scalable digital foundation to drive business agility**

- Modernised ERP solutions to increase business agility

# It is so cool to see the Equinor Technology Strategy and the historical “sus” over it




Industry 0?

**Extend lifetime and re-use of infrastructure**

- Improve safety in operations and design

Karmsundet

**Accelerate data-driven decision making**

- Industry 4.0 for interoperability within the energy industry

# The future of automation (still anchoring the stuff):

- What is the future of automation in a context of industrial control systems

In the context of industrial control systems (ICS), which are used to manage and control industrial processes, the future of automation holds several key trends and developments

**Industry 4.0 and IIoT Integration**

**Advanced Data Analytics**

**Edge Computing**

**Cybersecurity and Resilience**

**Autonomous Systems and Robotics**

**Predictive Maintenance**

**Human-Machine Collaboration**

**Digital Twins**

**Regulatory and Standards Evolution**

**Decentralized Control**

**Skill Upgradation**

# Says who?

Default (GPT-3.5)

# And, by the way

IEC TC 65 main topics at their plenary meeting this year:

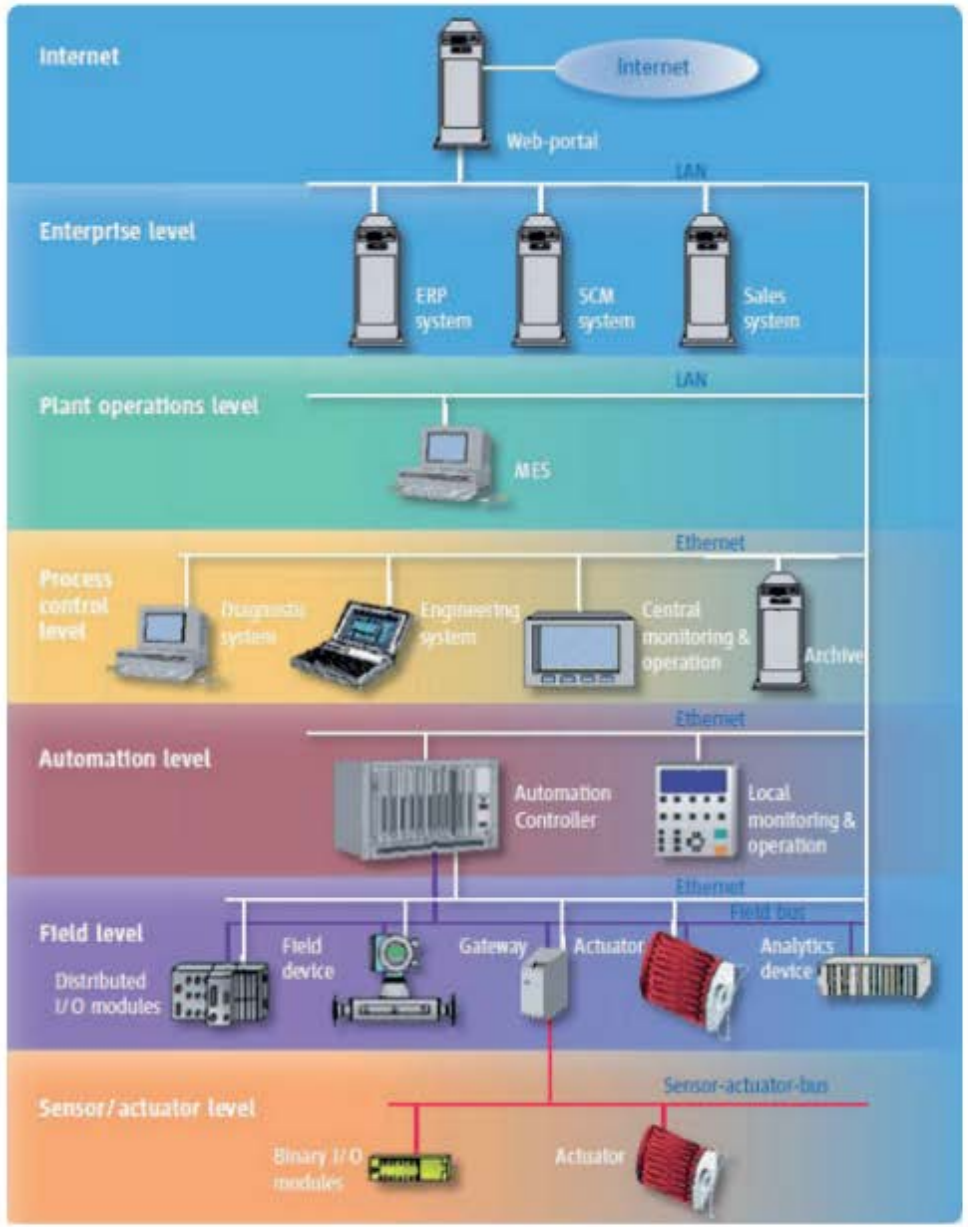
# IEC TC 65 New and planned projects: 2023 London

| | | |
|---|---|---|
| 1 | Opening | Ingo W |
| 2 | CDD, Digital name plate, Identification Link and digital product passport (SC65E: WG2, AG4)<br>• Submodel Name plate (Thomas HADLICH)<br>• Covered and not covered aspects of CDD contents (Joachim NEUHAUS, Klaus DICKMANN) | Koji DE<br>Klaus D<br>Thoma |
| 3 | Field Devices (SC65B all WGs, SC65E: WG6, WG7, WG10, WG12)<br>• Device integration (Christian Diedrich)<br>• Device Integration (Takuya(Tak) IIJIMA)<br>• Intelligent Device Management (Ian VERHAPPEN) | Ian VE<br>Christia<br>Cheng(<br>Domin |
| 4 | Break | |
| 5 | Modular Type Package (MTP) (SC65E: WG14) | Benjam |
| 6 | NAMUR open architecture (NOA) | Tim LE |
| 7 | Presentation of potential new project<br>• Registering information model of ISO 20140-5 into CDD<br>• A project related to the Collaborative Safety | Koji DE |
| 8 | Presentation of potential new project<br>• RAMI 4.0, a application of URMSM<br>• Human Factors for functional safety | Ingo W |
| 9 | Presentation of potential new project<br>• Predictive maintenance algorithm evaluation method<br>• AUTBUS series standard expansion (long-distance transmission, motion control, safety communication)<br>• Review of IEC PAS 63178 on "Manufacturing Resources/Capabilities for SM Service Platform" | Lu Ding |

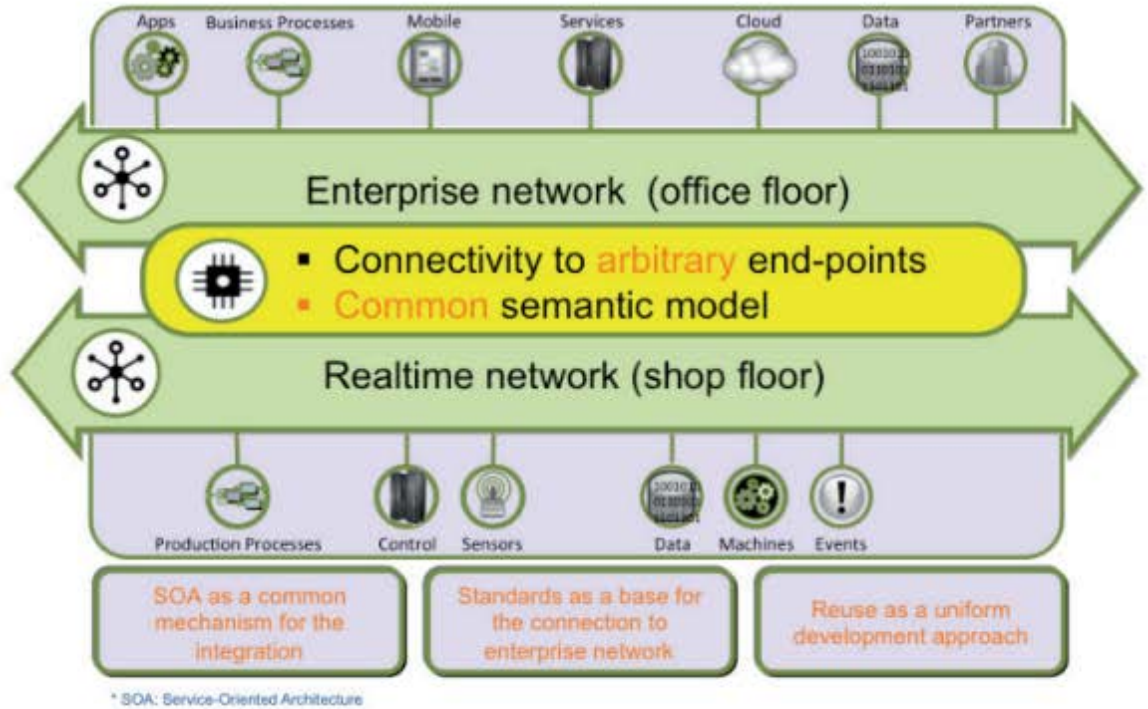
# Industry 4.0

- Yes, some think like this
- But,

# From the automation pyramid to Industrie 4.0




Source: Prof. Martin Wollschlaeger, TU Dresden




Source: ZVEI

PLATTFORM INDUSTRIE 4.0

# Industrie 4.0
## What's new, really?

### That's already possible today

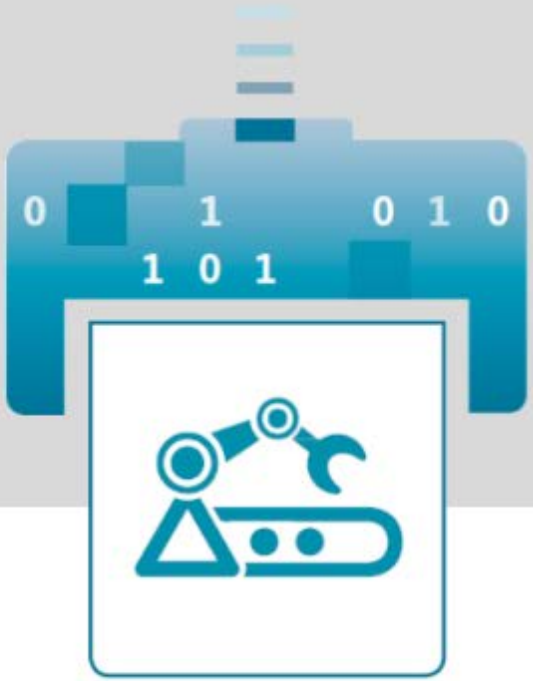
- The cloud
- The network
- Automation devices with Internet access
- Internet-based services

### Industrie 4.0: This is new

- **Added value** by exchanging information between value chain partners
- From **Intranet** to **Internet**
- **Neutral and common standards** for communication, services and semantics across companies and sectors

A large number of new **applications** and **business models** will emerge.

# Asset Administration Shell
## implements the Digital Twin




### Digital Twin

Definition (Industrial Internet Consortium (IIC) & Plattform I4.0): Digital representation, sufficient to meet the requirements of a set of use cases

***Digital representation = information that represents characteristics and behaviors of an entity (asset)***
***i.e. the Asset Administration Shell is the implementation of the Digital Twin for Industrie 4.0***

Plattform Industrie 4.0 Glossary http://i40.iosb.fraunhofer.de/

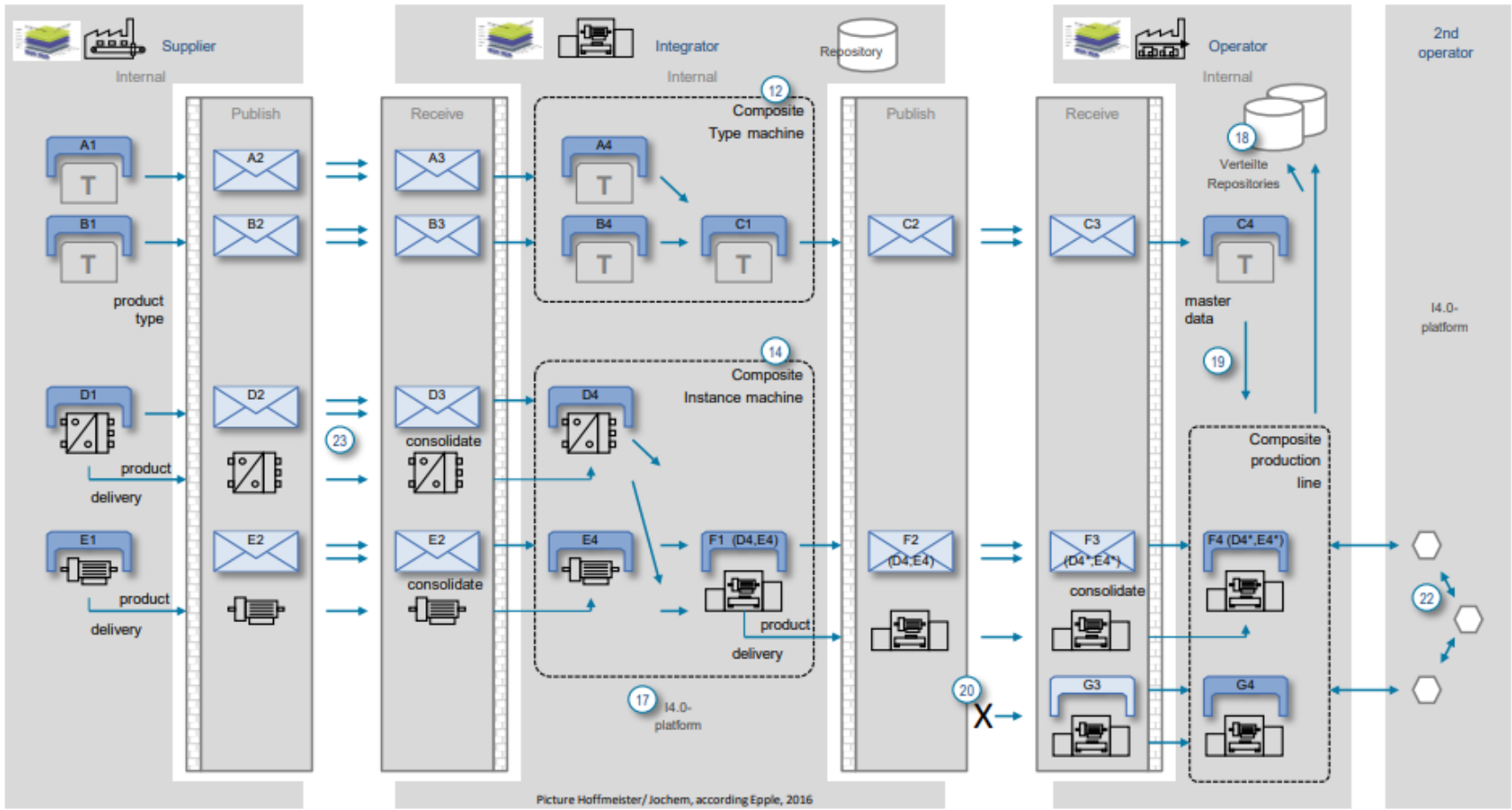
# Asset Administration Shell

## Why?


- The Asset Administration Shell is the **implementation of the „Digital Twin“** for Industrie 4.0
- The Asset Administration Shell establishes **cross-company interoperability**.
- The Asset Administration Shell is available for **non-intelligent and intelligent products**.
- The Asset Administration Shell covers the **complete life cycle** of products, devices, machines and facilities.
- The Asset Administration Shell enables **integrated value chains**.
- The Asset Administration Shell is the **digital basis for autonomous systems and AI**.

# Details of the Asset Administration Shell

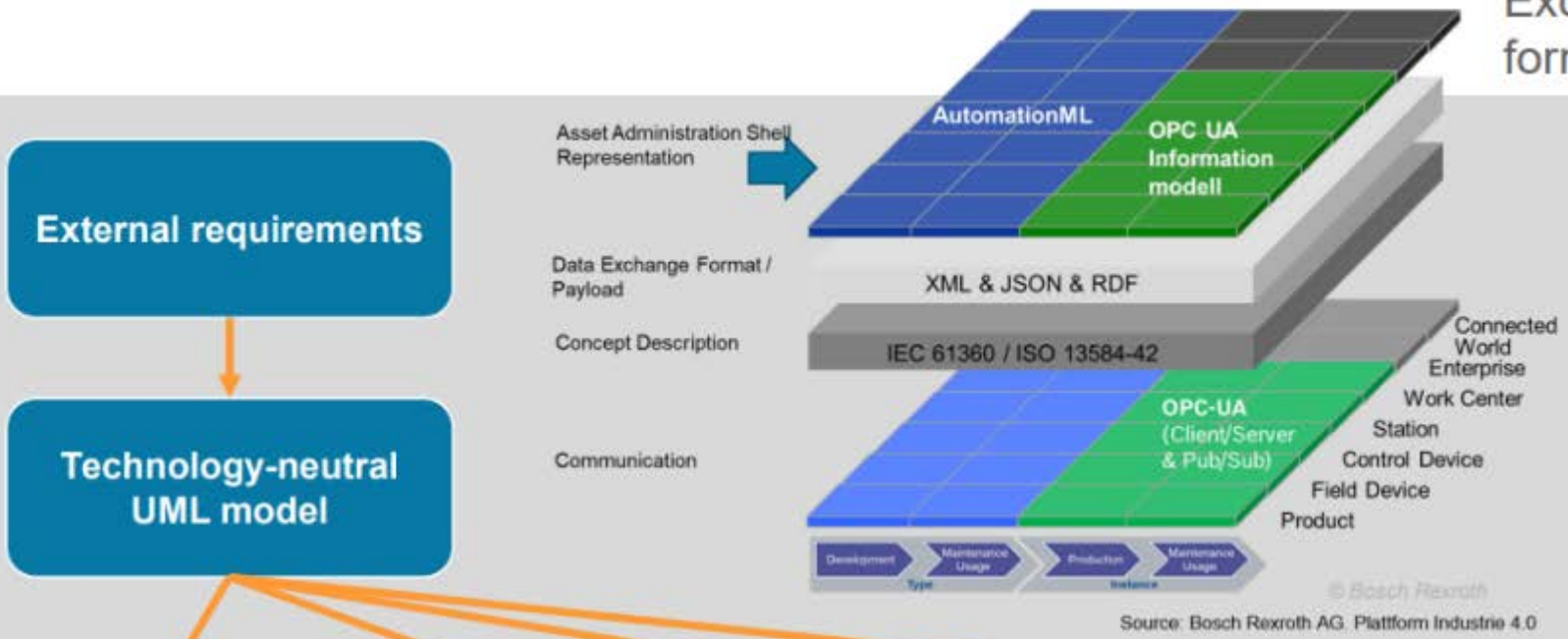
## Leading picture for Use Cases: a three-step value chain



# Overview of the Asset Administration Shell

## Current approach

RAMI4.0 - Exchange formats




Source: Bosch Rexroth AG, Plattform Industrie 4.0

External requirements

Technology-neutral UML model

AutomationML

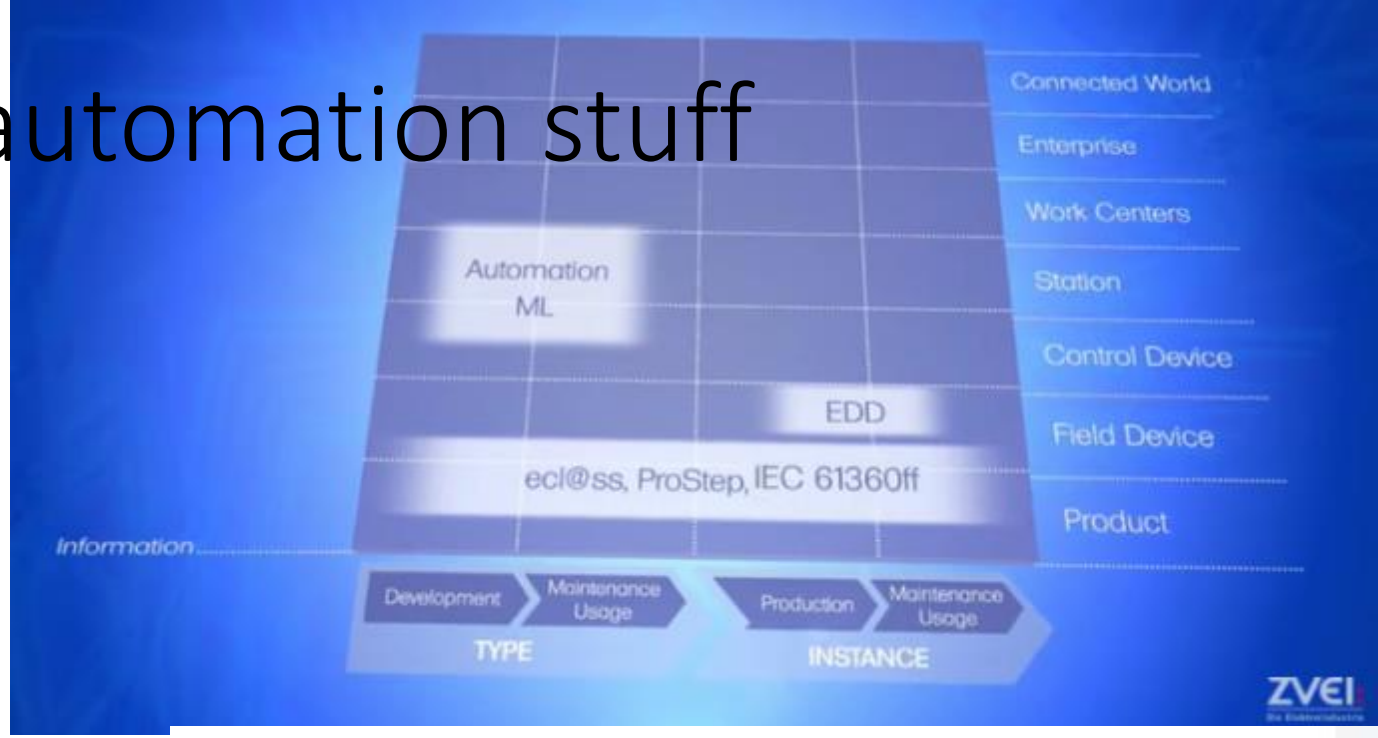
XML, JSON

RDF

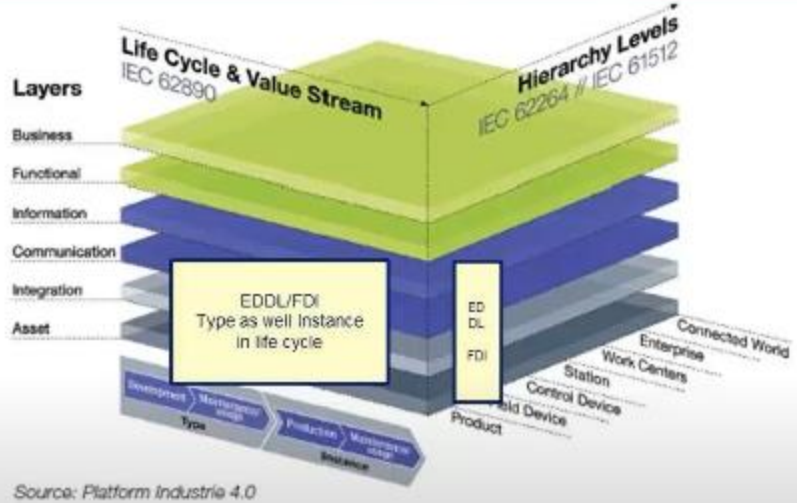
OPC UA Information Modell

**Security by Design**

# I.e. RAMI put our cool automation stuff into context:



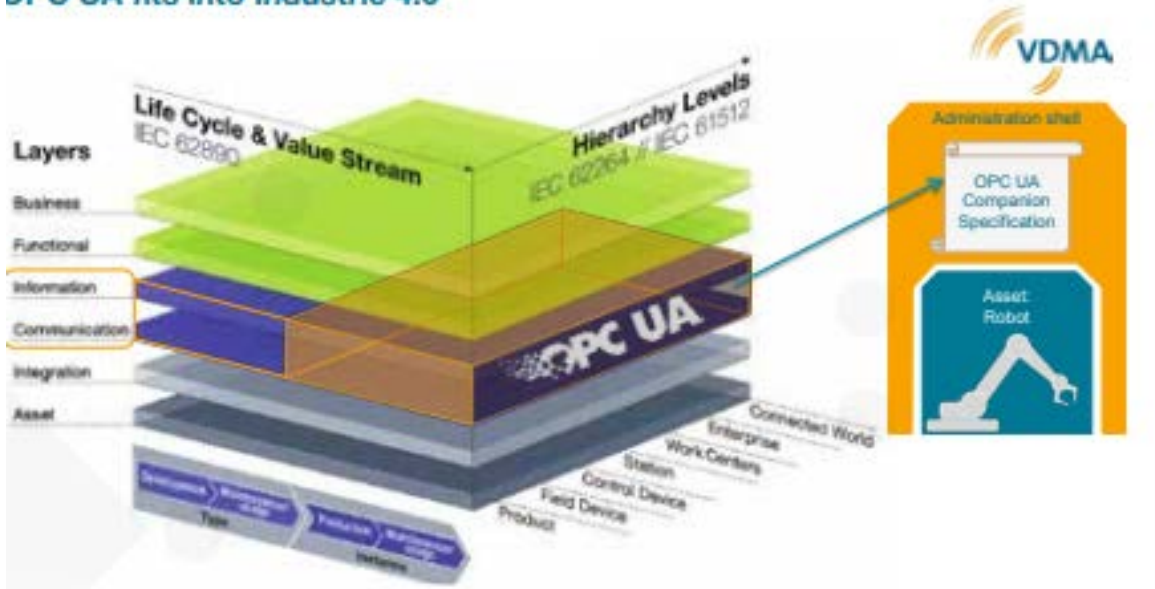

## Relation of EDDL/FDI to RAMI 4.0



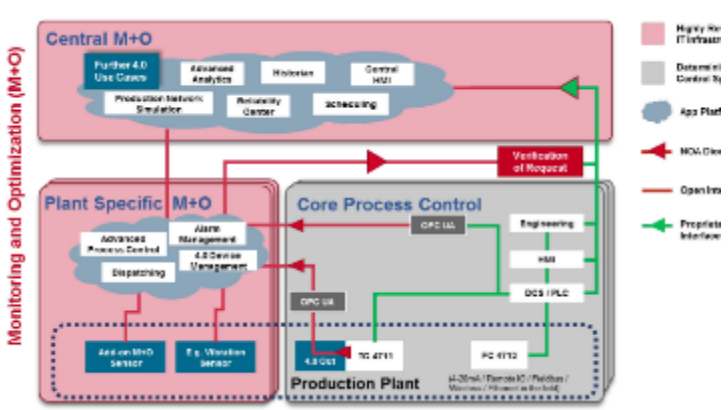

Source: Platform Industrie 4.0

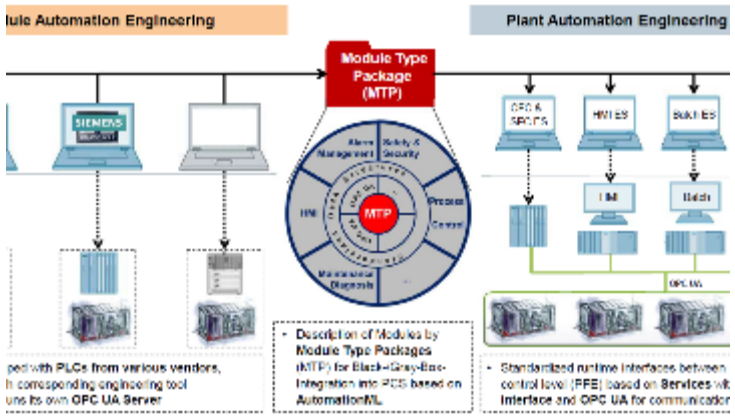
- EDDL/FDI is related to field devices
- EDDL/FDI covers device functions, device parameters (information), device configuration (integration), communication
- EDDL/FDI contribute to the entire life cycle of production assets

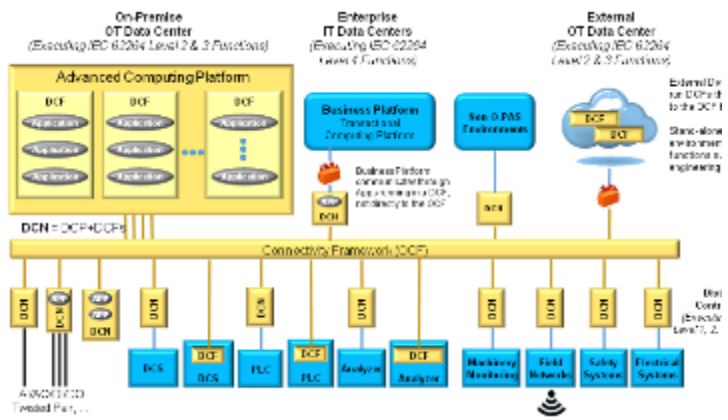
## OPC UA fits into Industrie 4.0

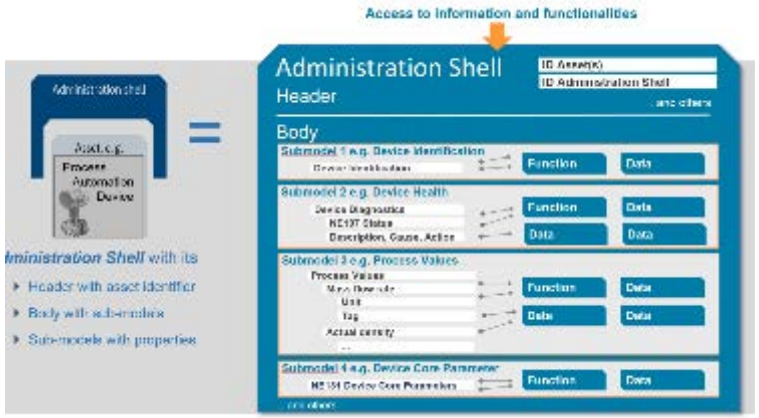


# Evolution of Industrial Automation and Control Systems



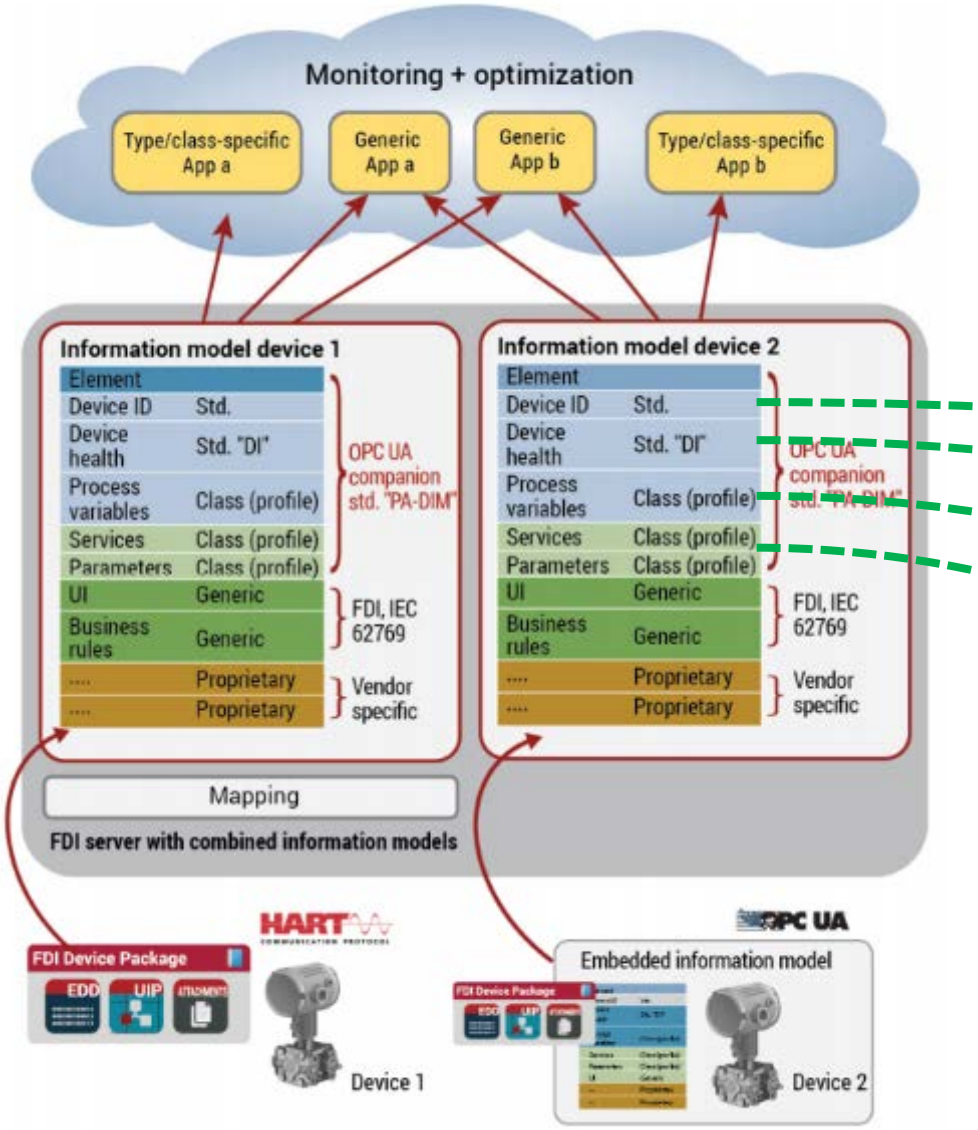



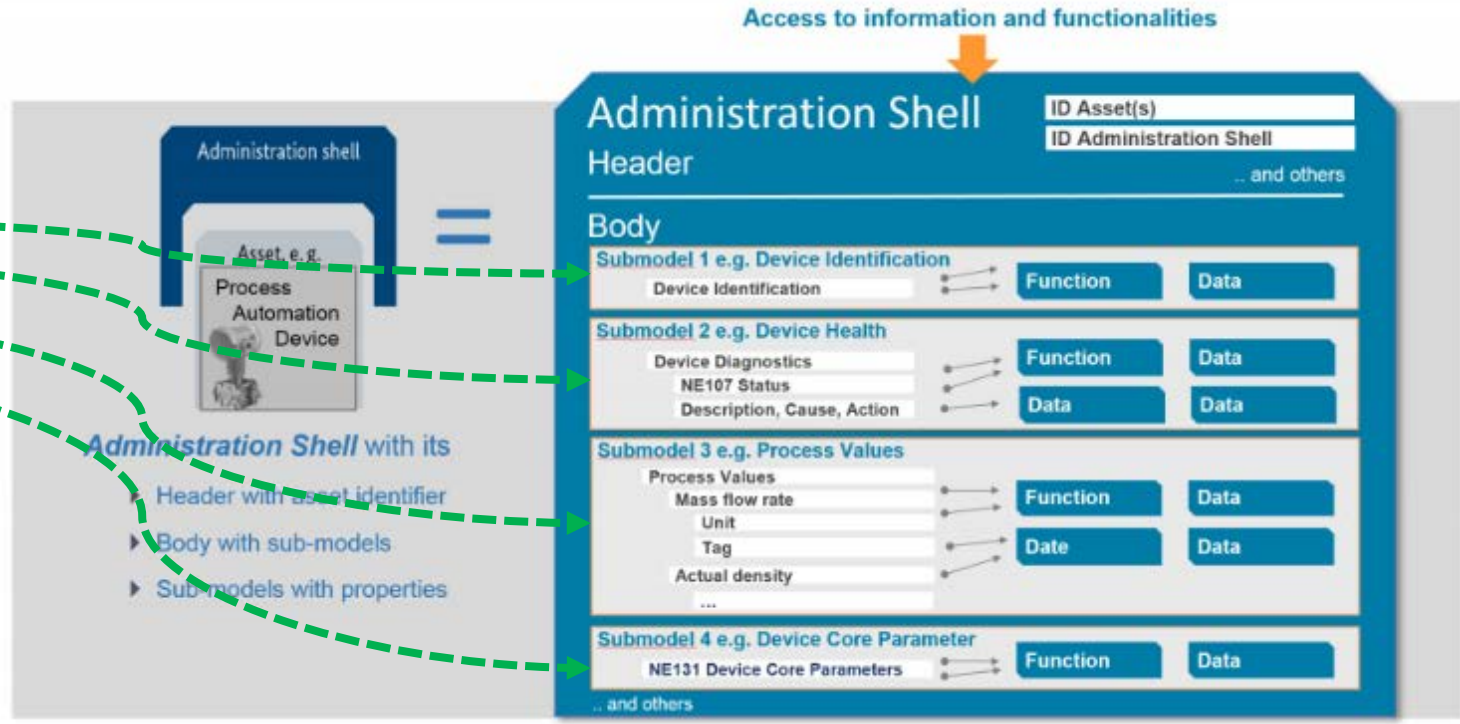

- Industrie 4.0
  - AAS, Asset Administration Shell
- OPA, Open Process Automation
- NOA, Namur Open Architecture
- MTP, Module Type Package

# Eureka! i.e. Instruments/Devices -> AAS

Current Devices

Future devices as an AAS



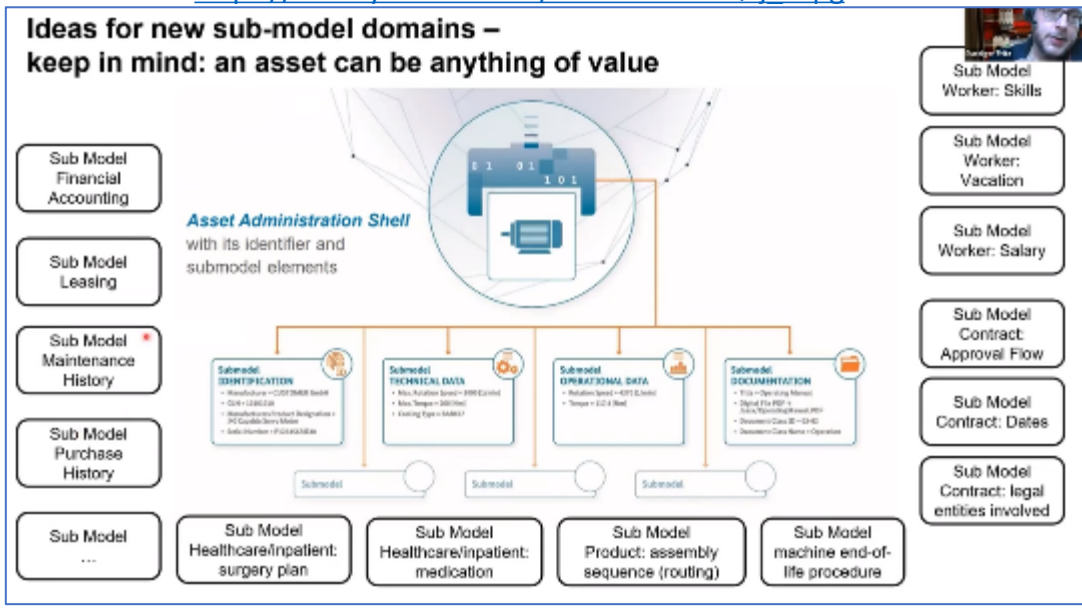



# I4.0/AAS is here!

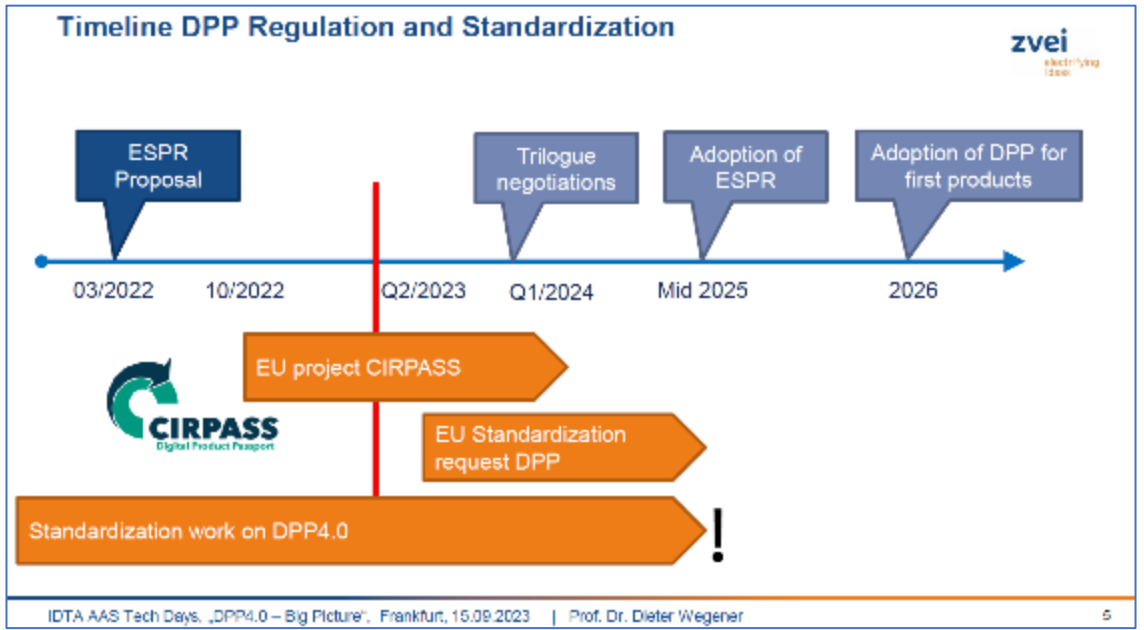
https://demo-digital-twin.r-stahl.com/?lang=en


# SAP is waking up

https://www.youtube.com/watch?v=FTkQoj_Yepg




# EU introduce DPP



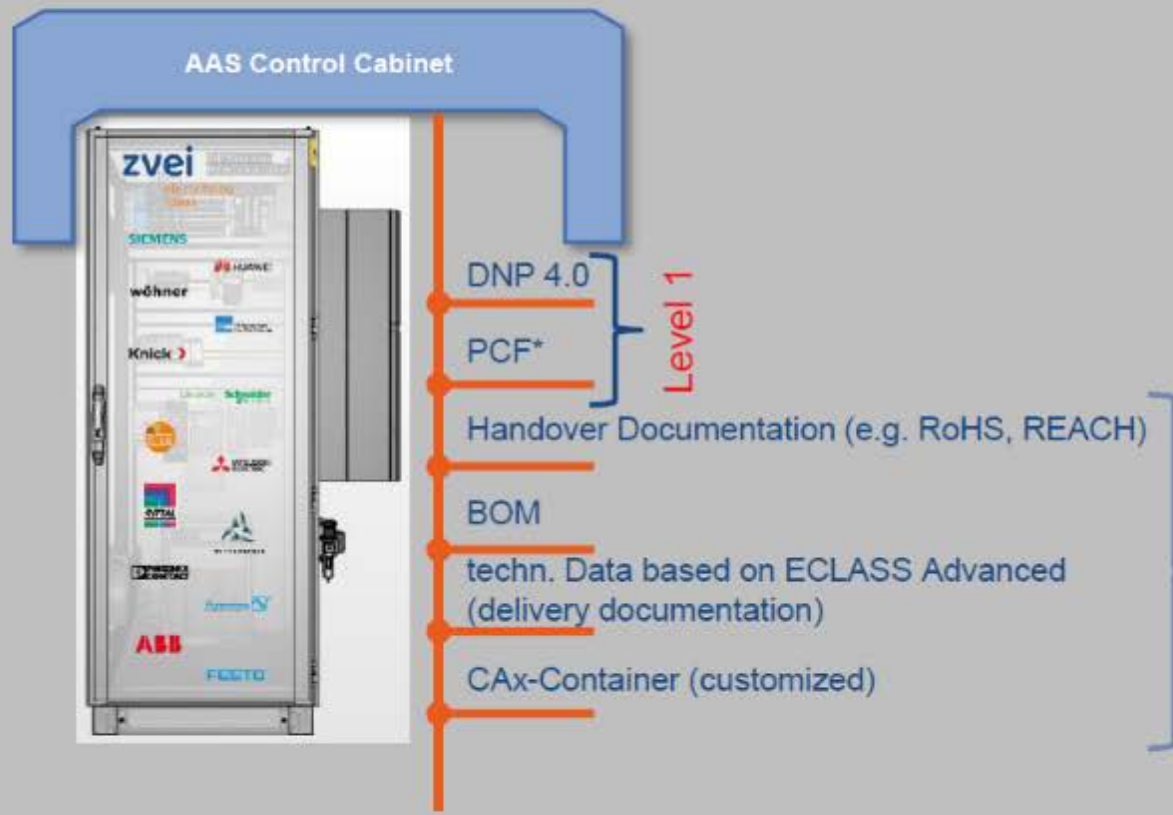
# ZVEI-Show-Case “CO2@Control Cabinet”

## Digital Twin Level 2 (Hannover Fair 2023)

zvei
electrifying ideas


## Implementation View

### New Submodels for AAS




* PCF = Product Carbon Footprint, equals CO2-Footprint, Cradle-to-Gate-Calculation

# Live Demo: Example Siemens

Product

ID-Link

i.siemens.com >

Package

Online
Digital Nameplate

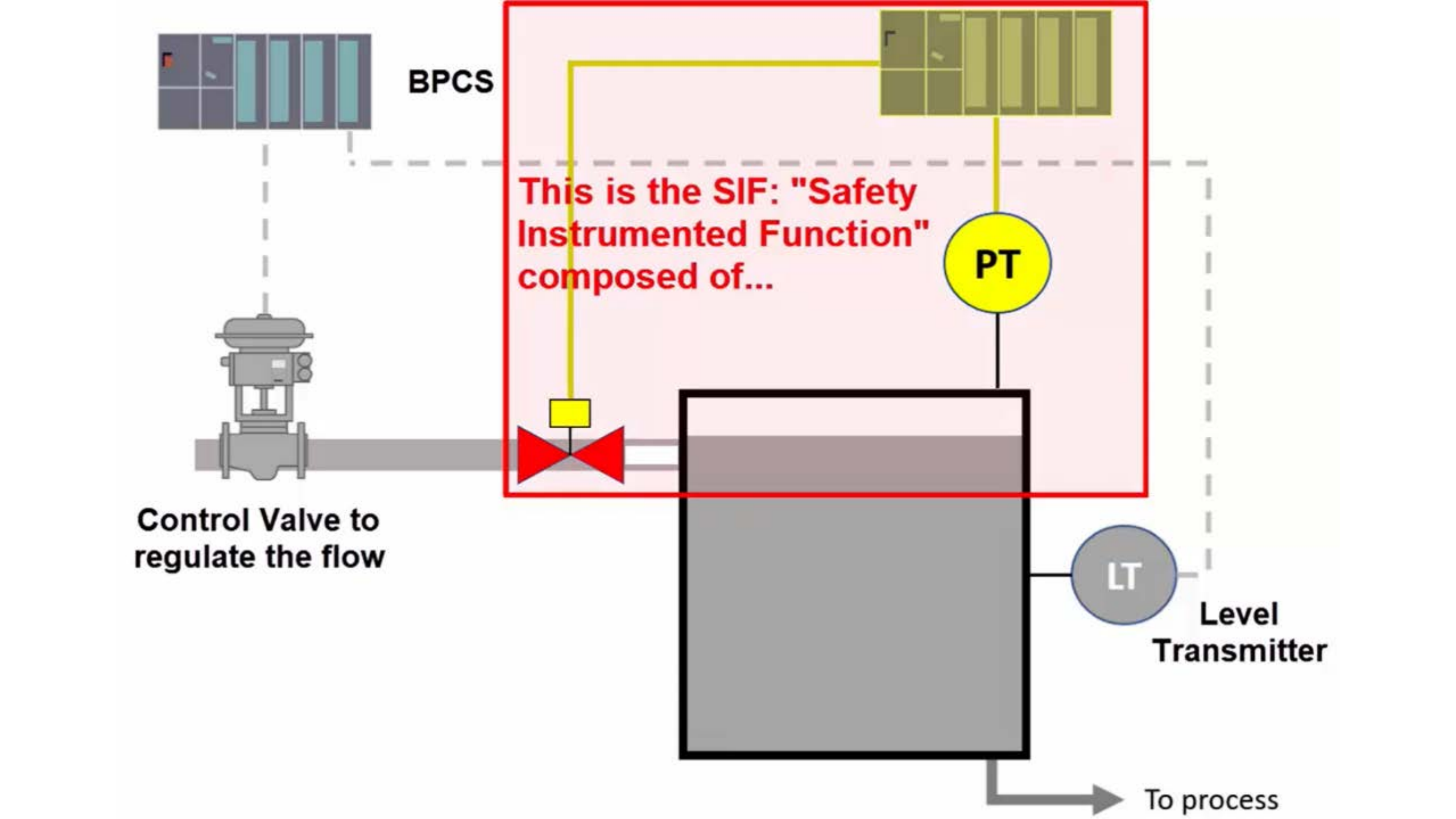

Online Declaration
of Conformity

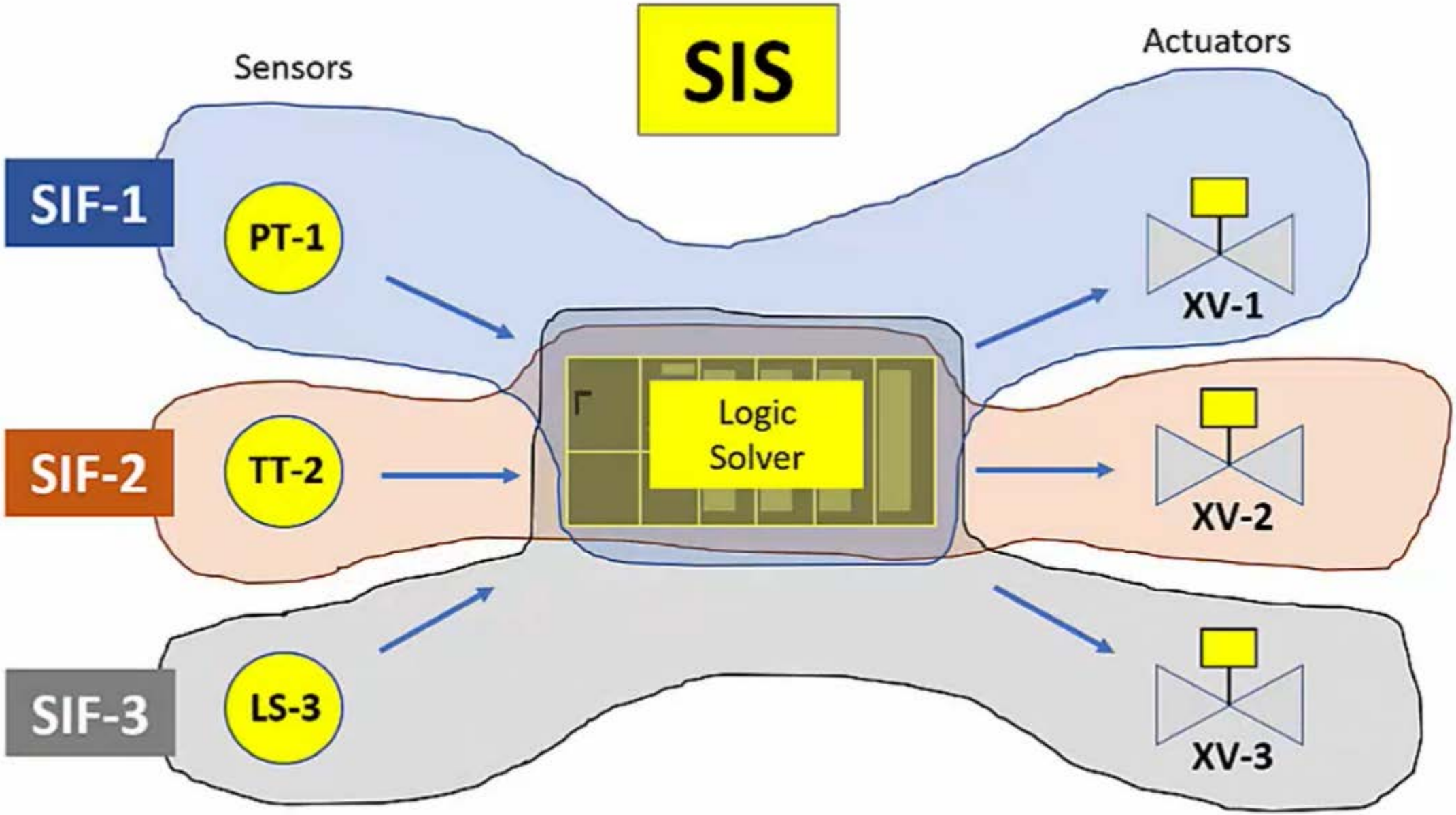

PDF of original
Dec. of Conf.


Source: | © Siemens 2022 |

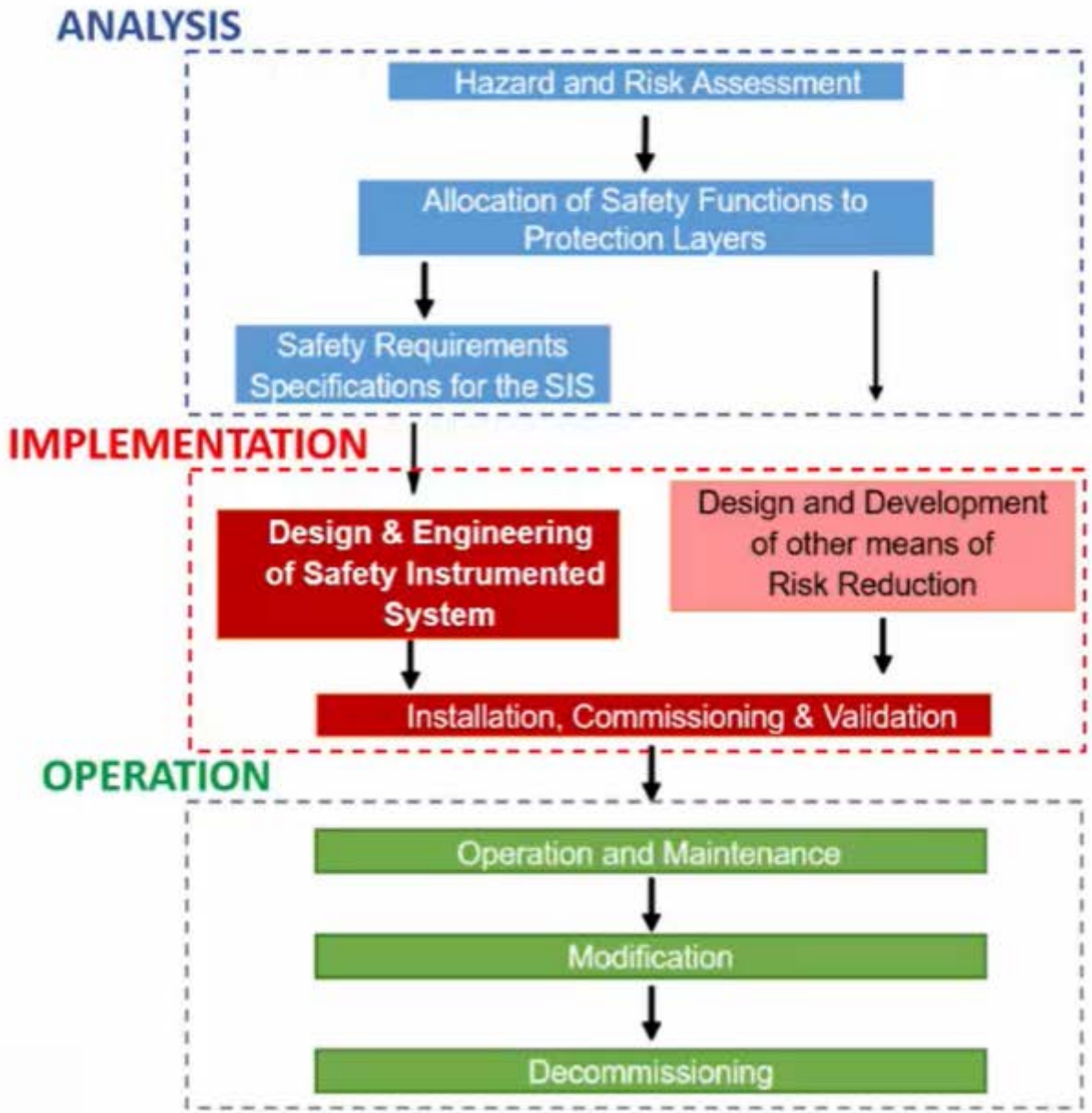
# Safety

- Some safety stuff as a kick-off for the story


BPCS
This is the SIF: "Safety Instrumented Function" composed of...
PT
Control Valve to regulate the flow
LT
Level Transmitter
To process


SIS
Sensors
Actuators
SIF-1
PT-1
SIF-2
TT-2
SIF-3
LS-3
Logic
Solver
XV-1
XV-2
XV-3

# Life Cycle of the SIS - IEC61511

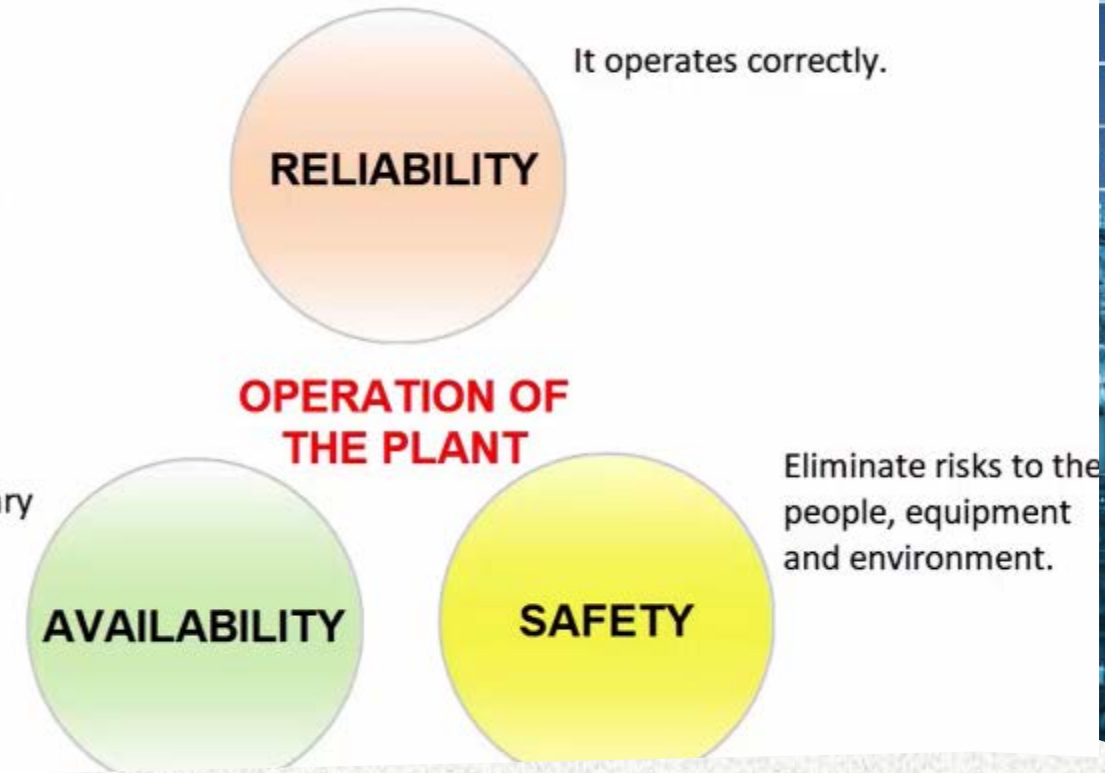



Process Risk Analysis
Protection Layers
Definition of SIFs
Determination of SIL
**Safety Requirement Specification**
Functional Safety Assessment

Technology Selection
Design of SIFs
Proof Test definition
**Verification, FAT, SAT**
**Validation & FSA**

**Maintenance Plan of the SIS,**
Training, use of bypass, proof tests, repairing, spare parts, alarms, inspections, calibration, recording, modifications, FSA

**When designing, installing and maintaining the SIS, SAFETY is not the only important thing.**

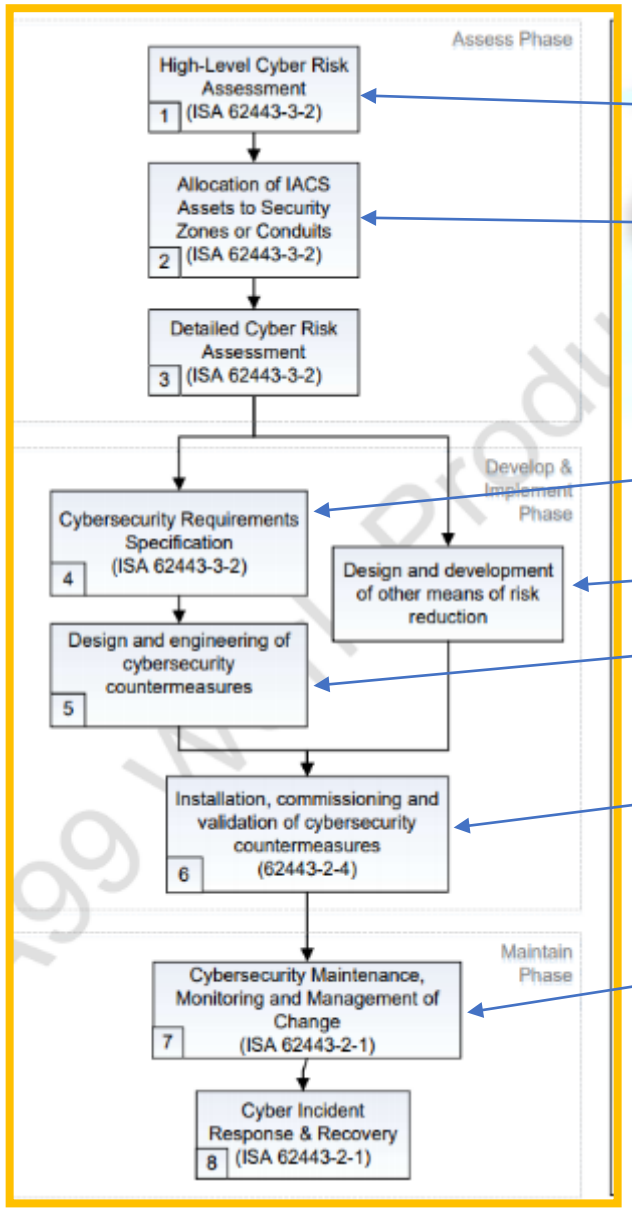


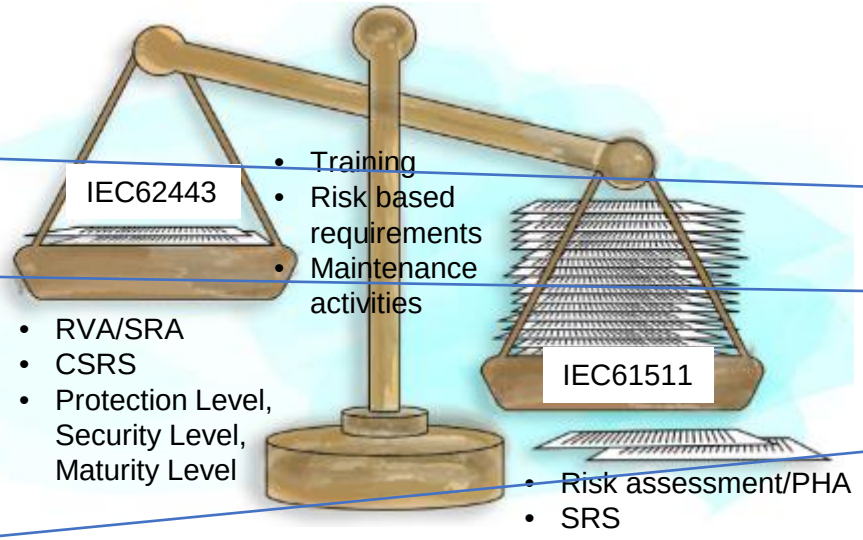

# Cybersecurity

- Digital Twin

# Cybersecurity: Based on foundations from Safety Life-cycle

## Security Life-cycle, IEC 62443




- Training
- Risk based requirements
- Maintenance activities

- RVA/SRA
- CSRS
- Protection Level, Security Level, Maturity Level

- Risk assessment/PHA
- SRS
- Safety Instrumented Function
- Safety Integrity Level

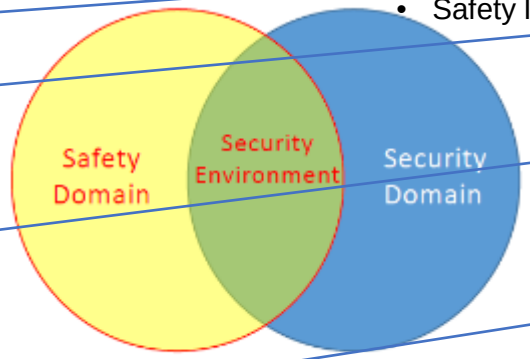
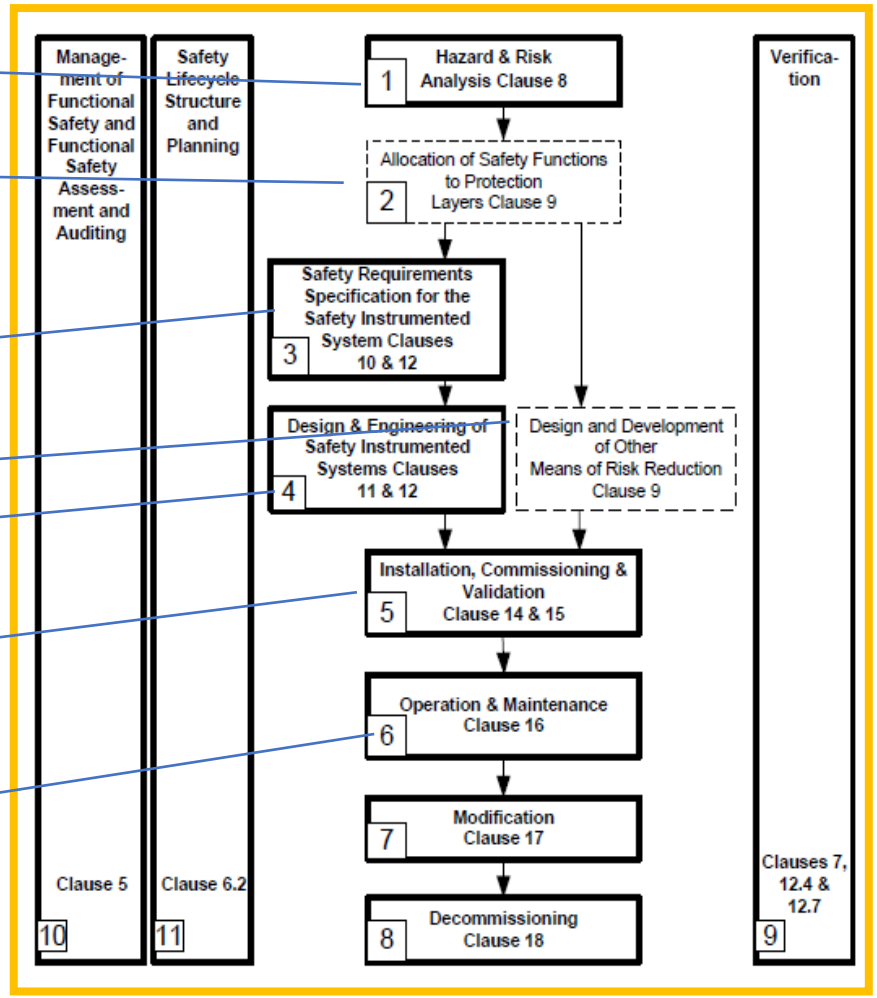



Figure 1 — Safety domain and security domain

IEC 63069

## Safety Life-cycle, IEC 61511



# Safety

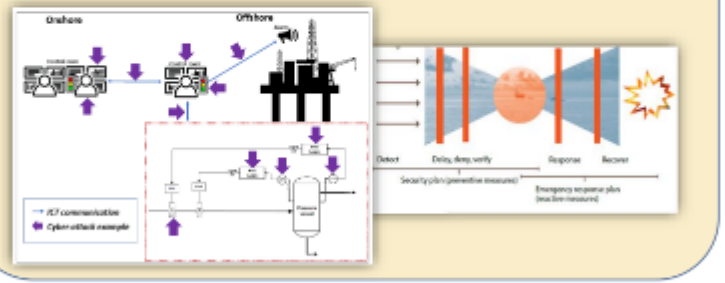
## Cybersecurity

CBM

KSP-project Petromaks 2 (2021 – 2026) NOK 20 mill

**Cybersecurity Barrier Management**

**Integrating the safety and security domain to ensure that cybersecurity does not interfere with safe operation**



SINTEF NTNU – Trondheim Norwegian University of Science and Technology AkerBP equinor

## Twin

APOS : Develop knowledge and specifications that can help automating the process for monitoring of SIS

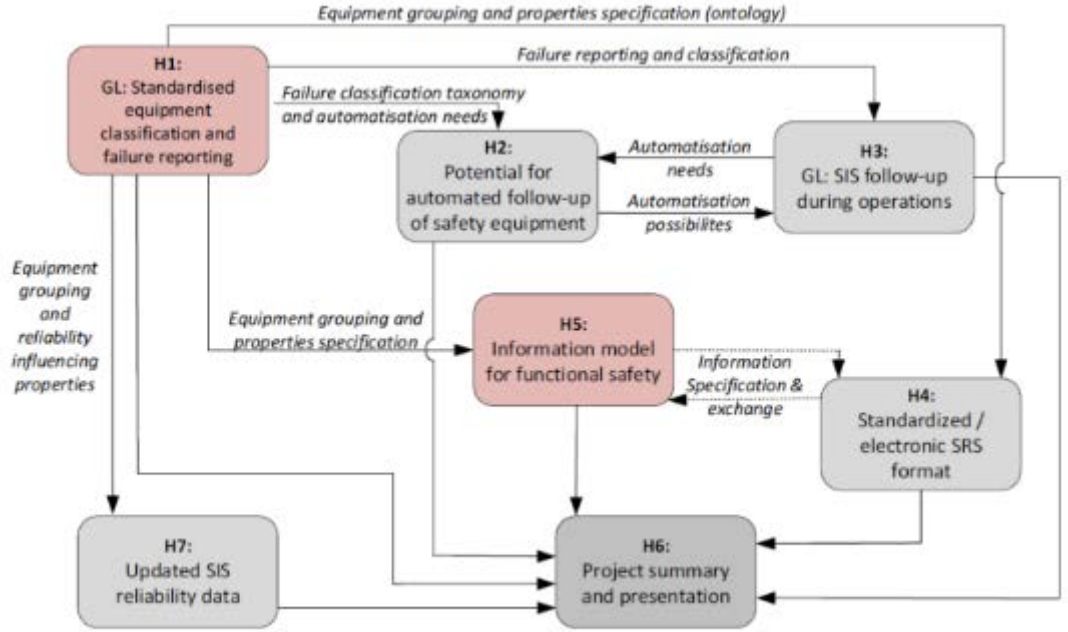
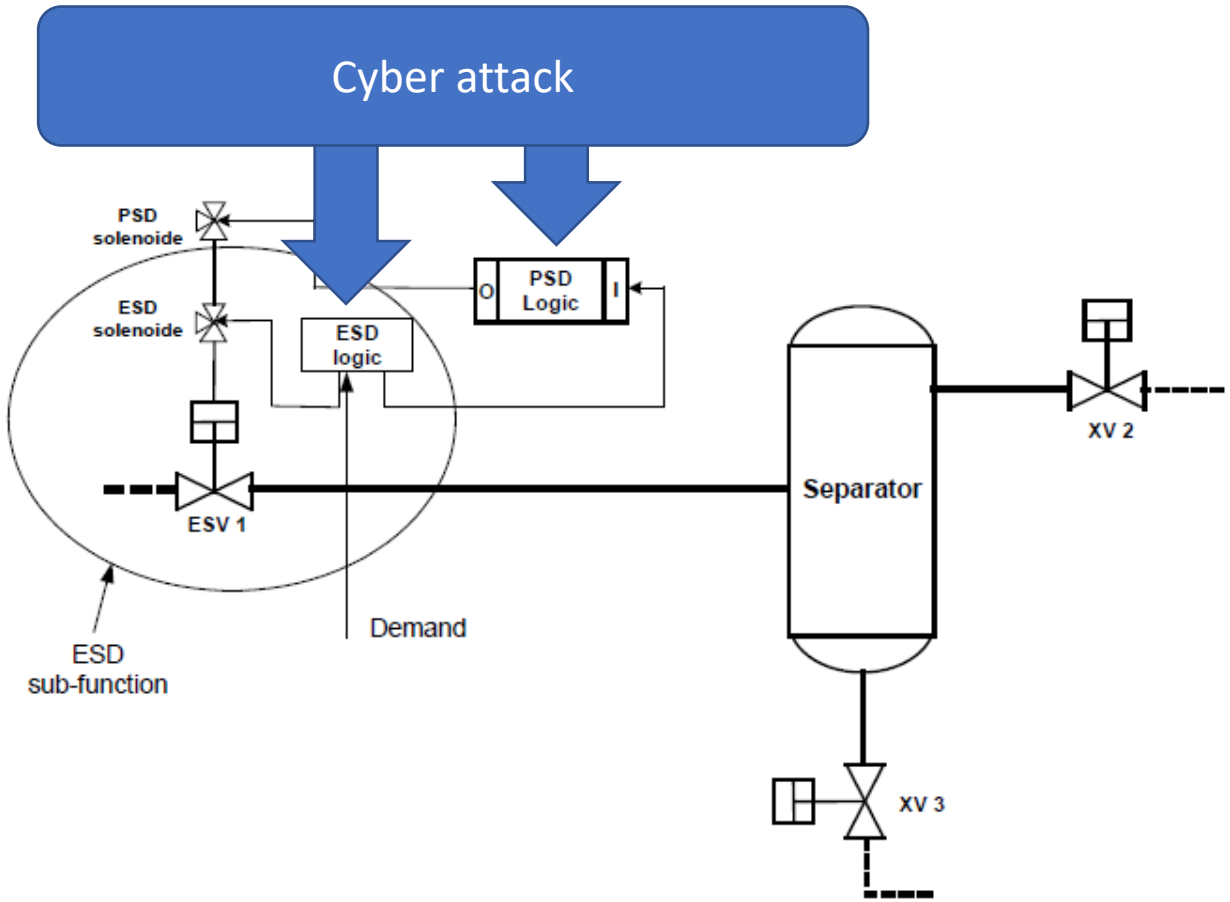



*Figure 5 APOS activities*

# SecureSafety - R&D questions

How to protect safety functions when the threat landscape is mostly unknown?

- What is the major accident risk resulting from cyber-attack?
- Which safety functions are particularly vulnerable to cyber-attack?
- What are the basic cybersecurity countermeasures (barriers) that must be addressed during design?
- How to improve cybersecurity without making the system inoperable?
- How to verify security levels of a proposed design?
- How to integrate the human component in cybersecurity barrier management?
- How to maintain cyber security barriers?
- How to monitor cybersecurity barriers during operations, including alarm management?



IEC 63278-1 ED1

# Structure of an AAS & relation to external roles

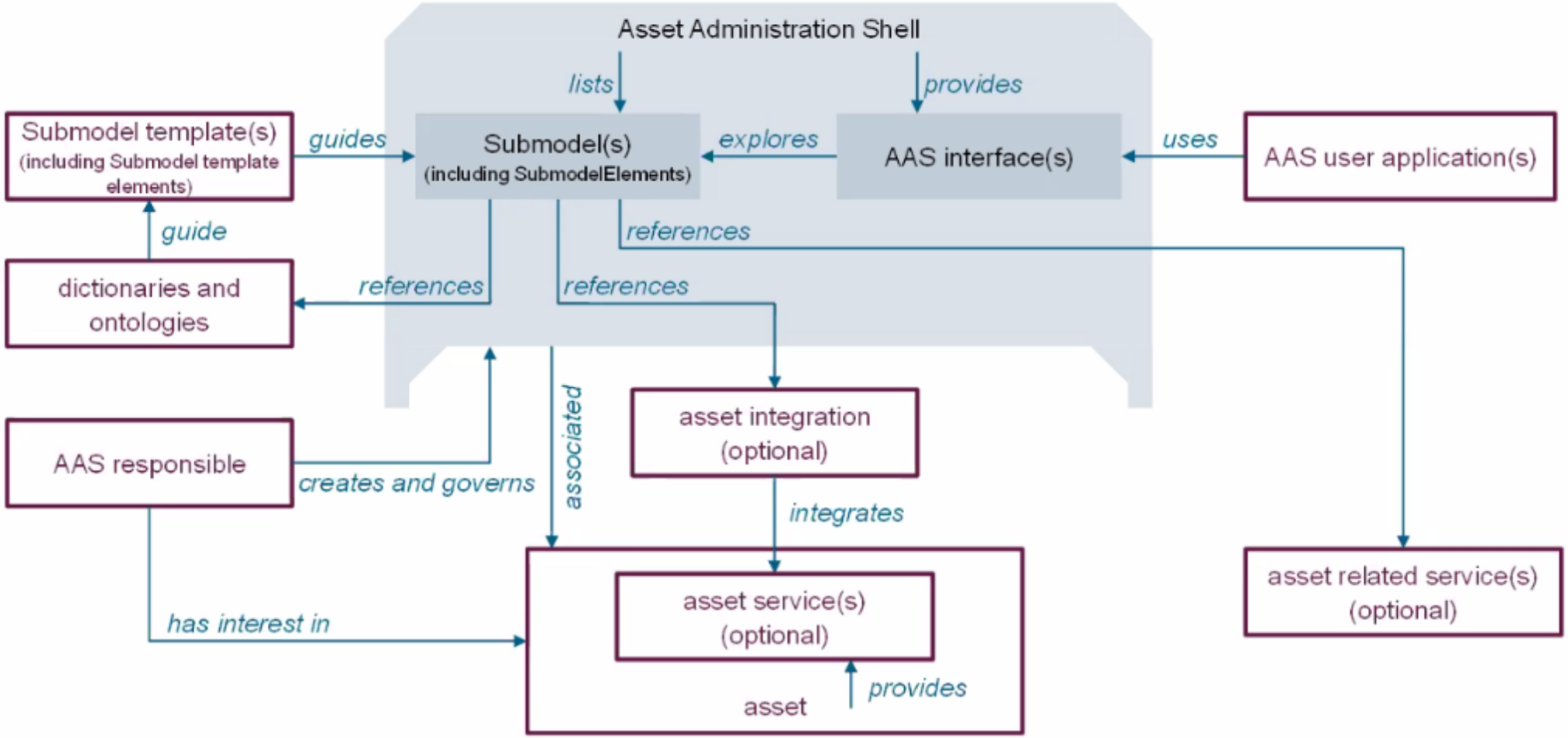
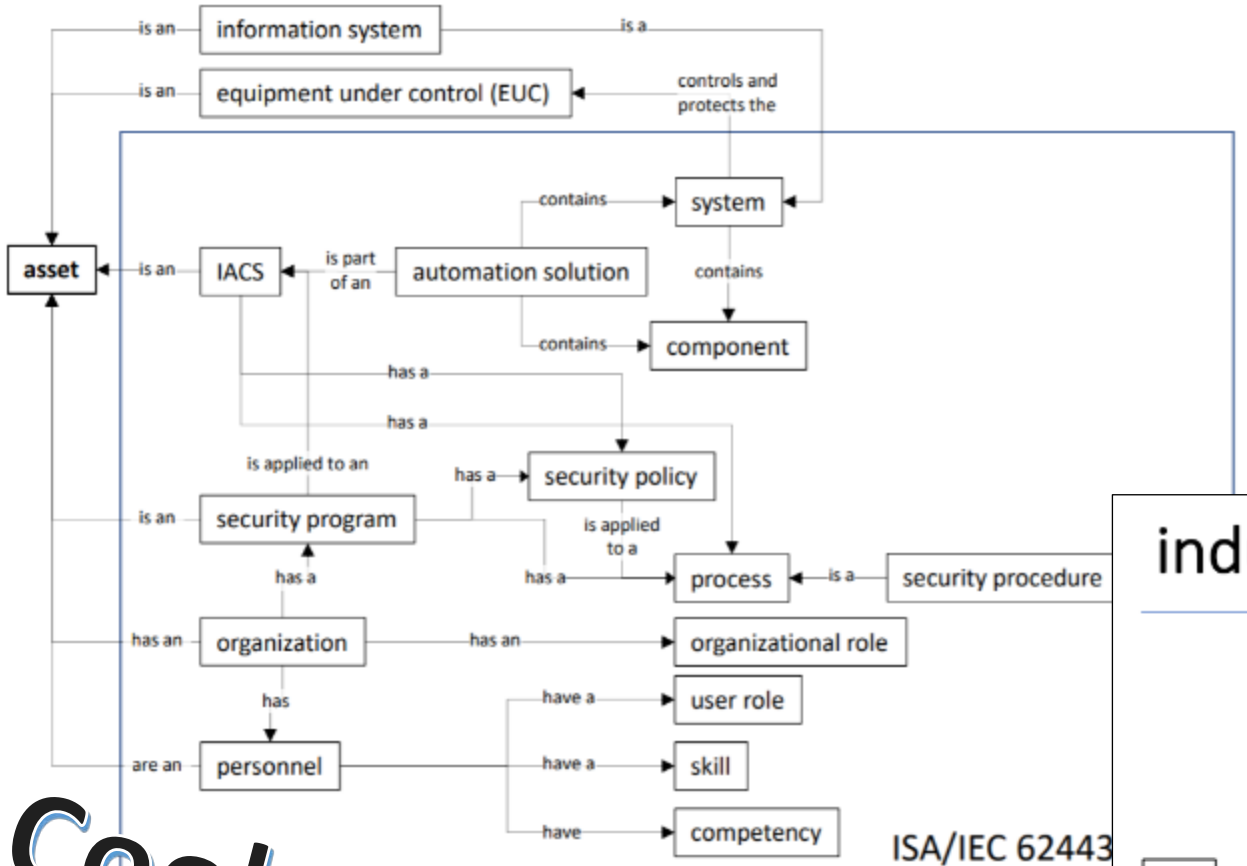
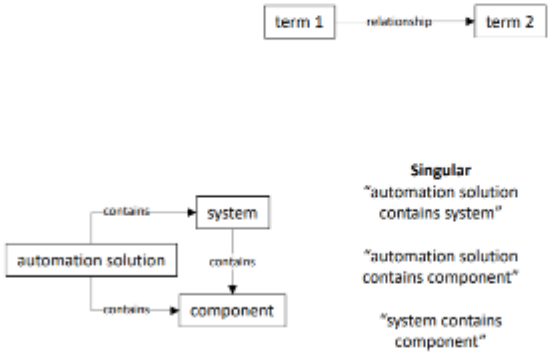



Figure 3 of IEC 63278-1 CD2 – Detailed overview of Asset Administration Shell and related roles

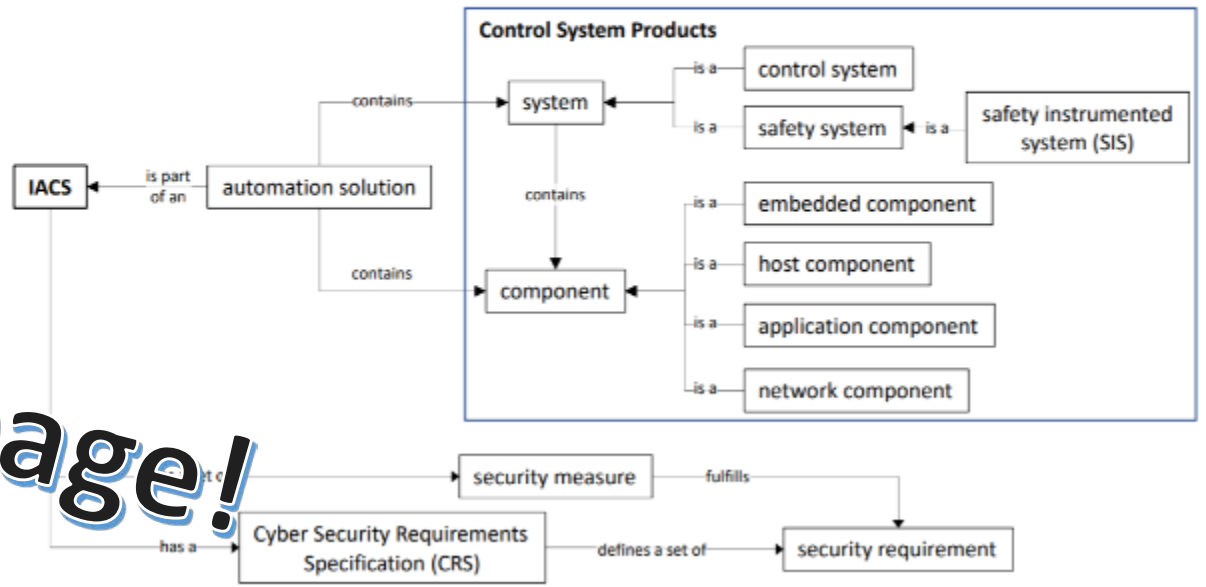
# asset




# How to read an ontology

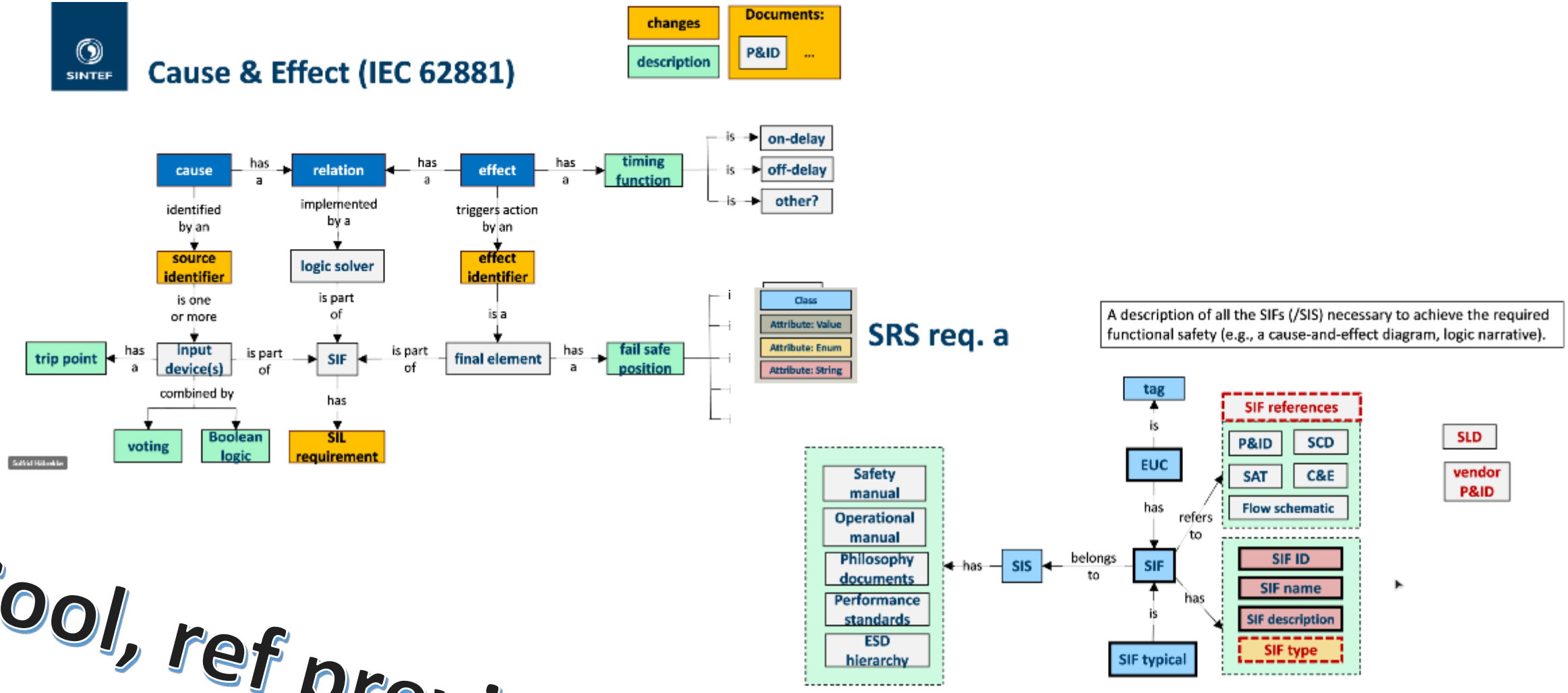



# industrial automation and control system (IACS)




Cool, ref previous page!

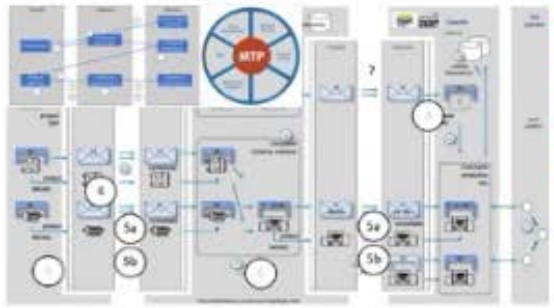
# Cause & Effect (IEC 62881)



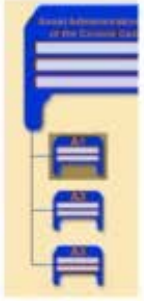

Cool, ref previous page!

# Piloting activities

# I4.0 AAS studies 2023 – Use cases

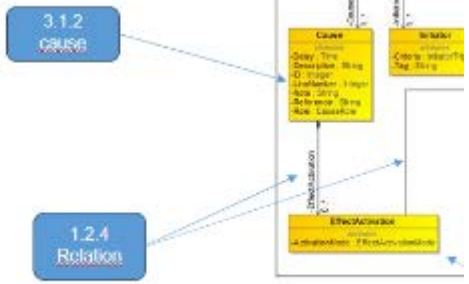







| ABB | Siemens Energy + S-AG | Kongsberg Maritim | Sintef/NTNU |
|---|---|---|---|
| • AAS for Small process system (Demonstrate life cycle)<br>• Use DEXPI P&ID model to create and map MTP HMI picture<br>• MTP mapping to AAS (Demonstrate relation)<br>• Demonstrate how to connect an AAS instance to a running system (virtual/real)<br>• Data sharing via AAS Server | • AAS for Control Cabinets (Demonstrate life cycle)<br>• Digital Nameplate, PCF Data, BOM, Certificates, doc.<br>• Replacement of components (Demonstrate management of change - MoC)<br>• Demonstrate how to connect an AAS instance to a running system (virtual/real)<br>• Data sharing via AAS Server | • Information modelling of SIF for SIS – (AAS / AML / UA)<br>• Support Sintef in defining information models for the Safety Instrument System (UA/AML)<br>• Create C&E IM (Information Model)<br>• Demonstrate how to connect an AAS instance to a running system (virtual/real)<br>• Data sharing via AAS Server | • Modelling of SIF Engineering<br>• Information Model for SRS (AAS / **AML** / UA)<br>• Connection to Fraunhofer, Rainer Draht (AML) |

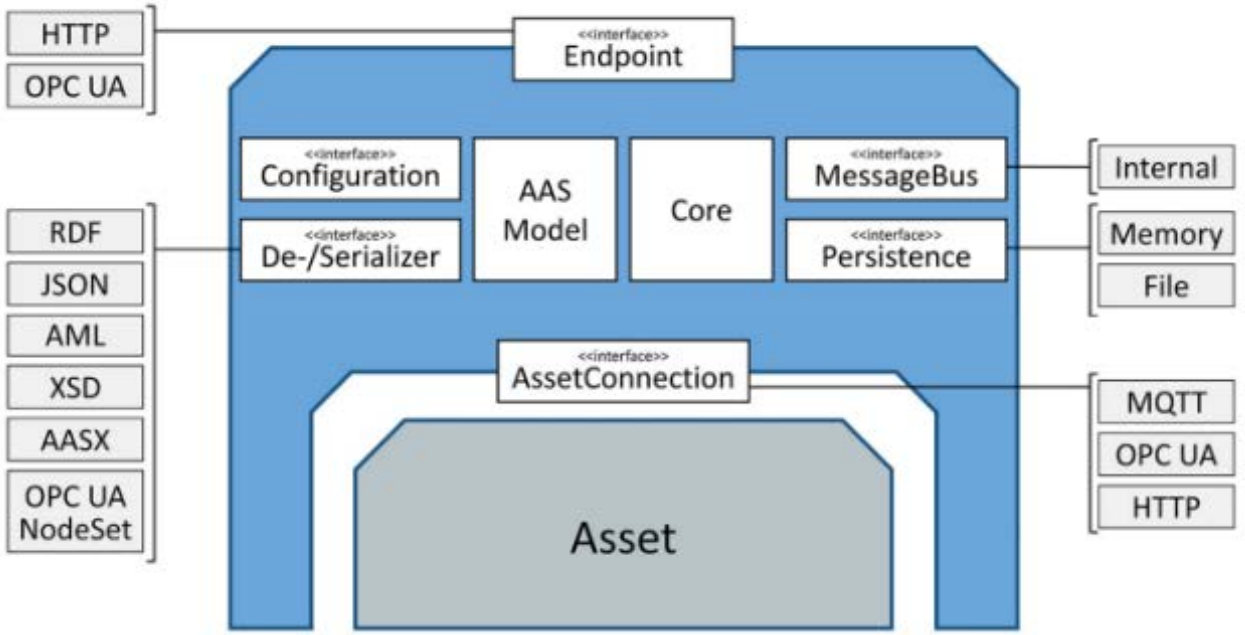
Relasjon mellom
KM UML modell og
IEC 62881



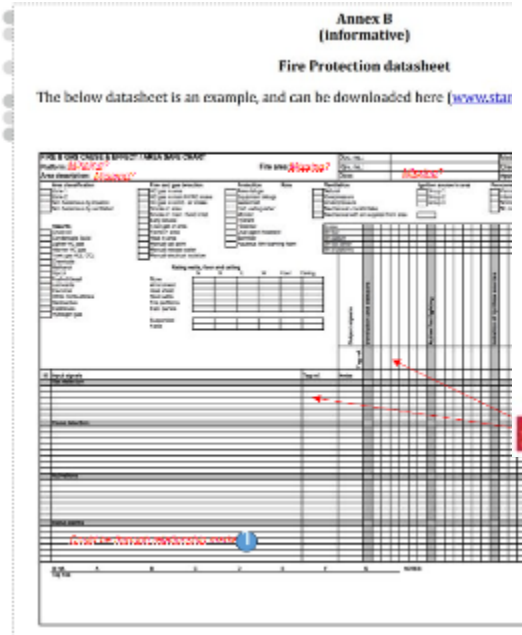



AIR I4.0 AAS Study 2023

# AAS Architecture




(Credit Fraunhofer)



Annex B
(informative)

Fire Protection datasheet

The below datasheet is an example, and can be downloaded here (www.star



KONGSBERG

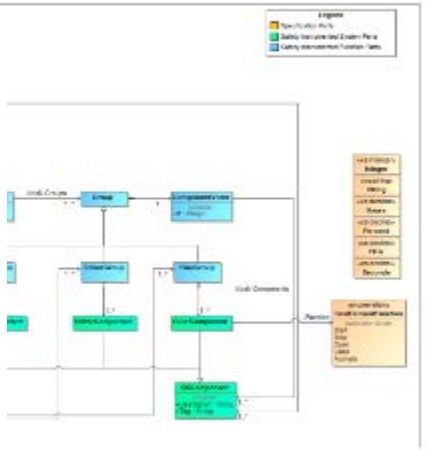
See Statement of Proprietary Information



NTNU SINTEF

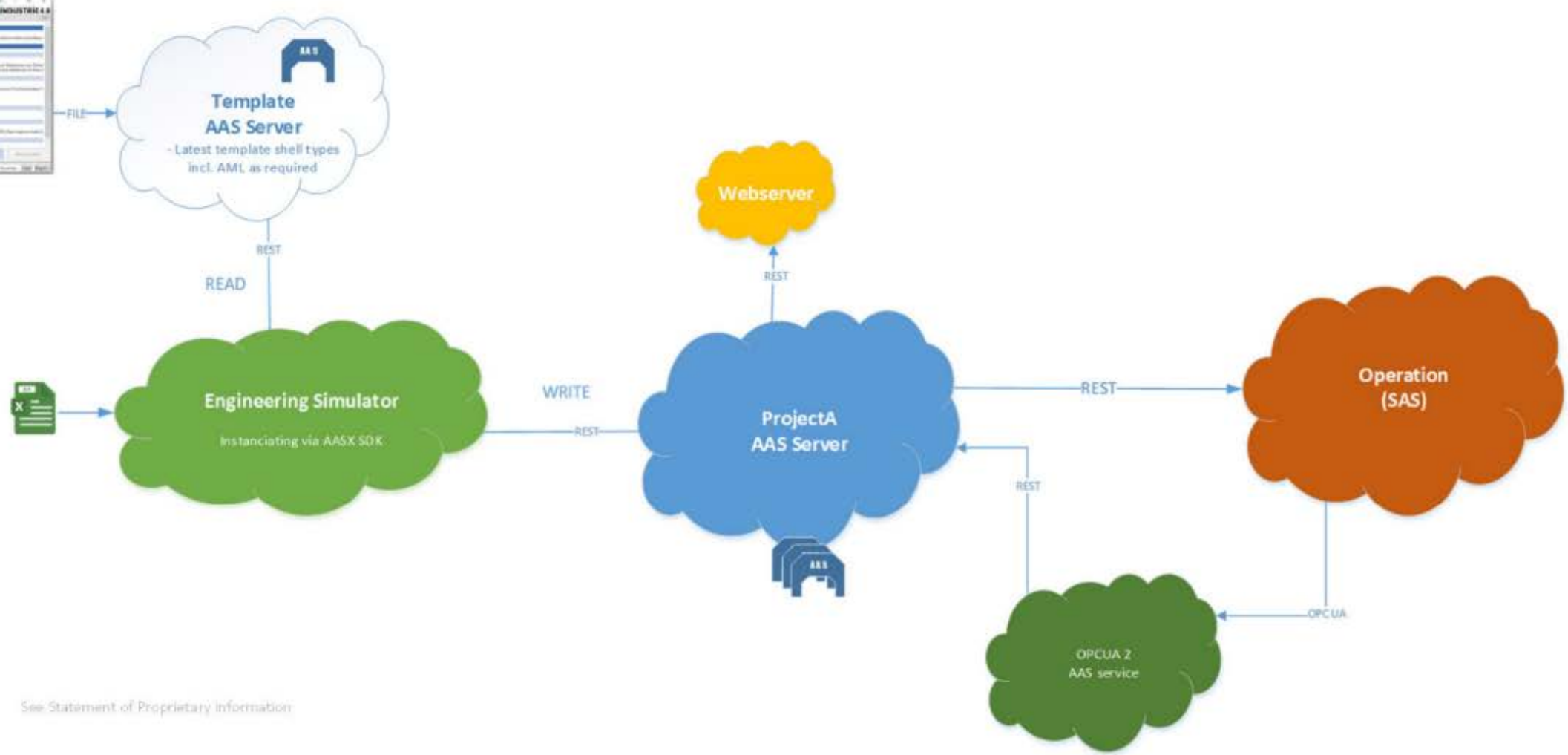
AIR I4.0 AAS Study 2023

## Introduction – SIF model status




# A digital safety ecosystem

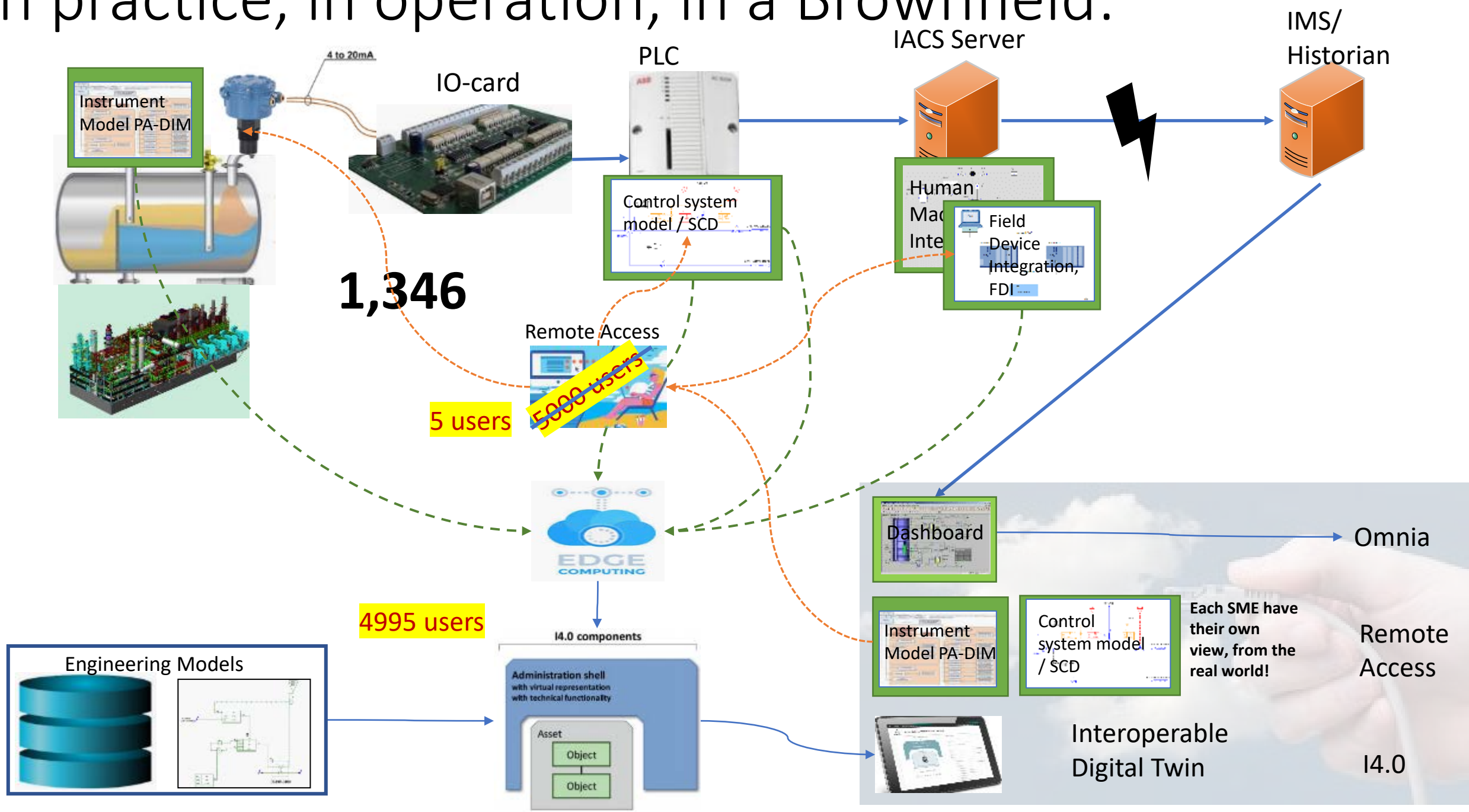
## The total ecosystem

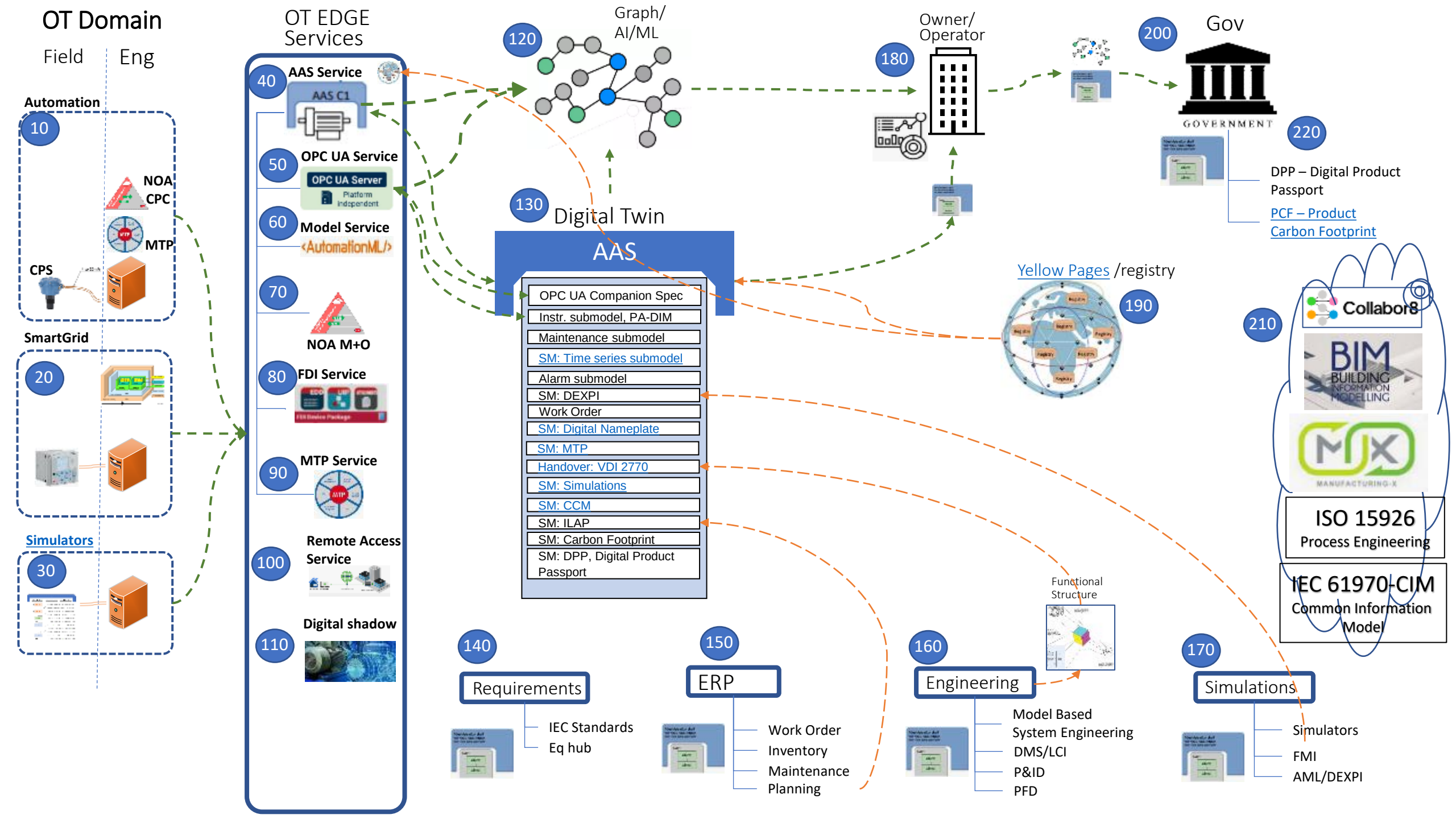


# Red line

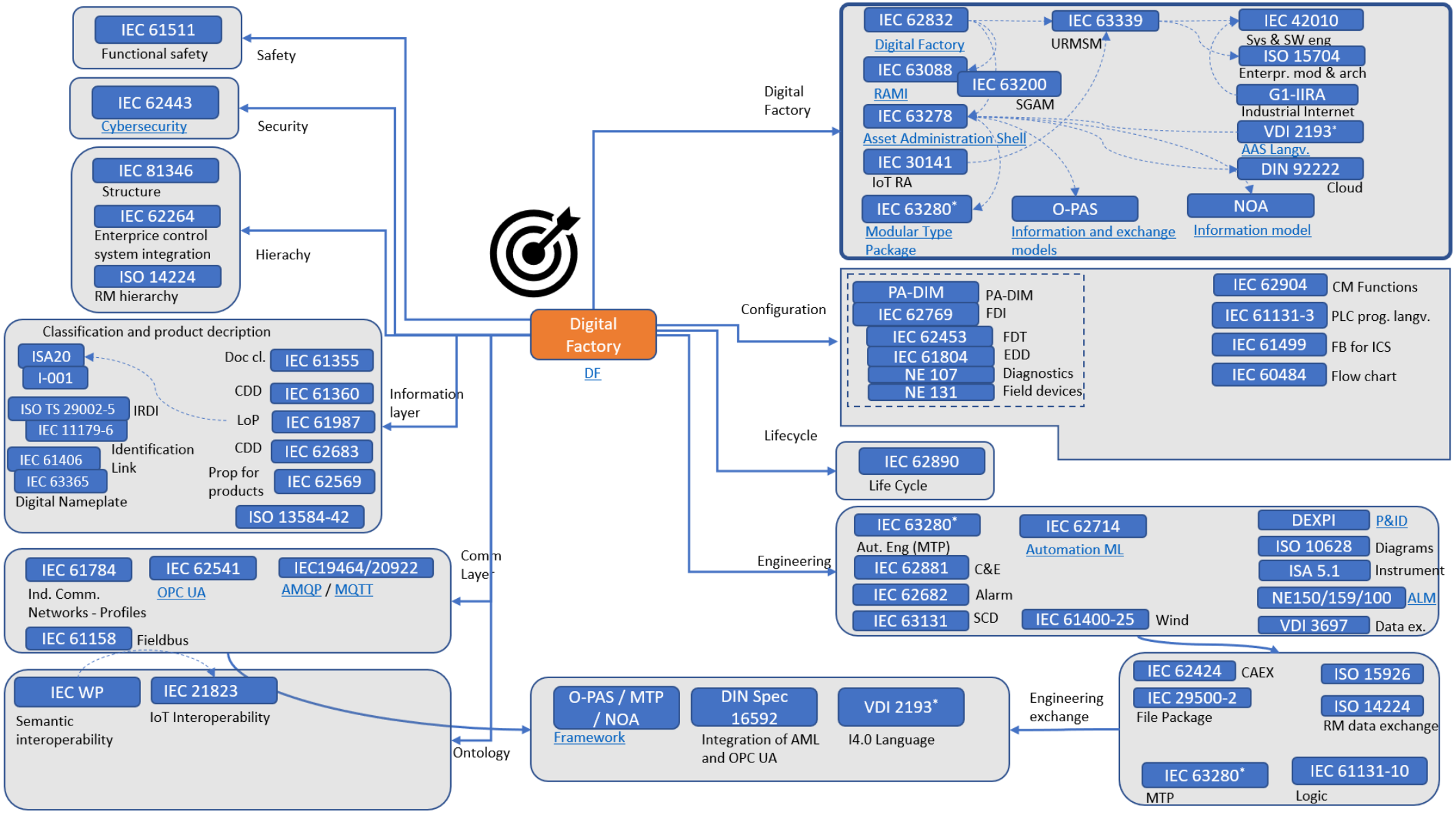
So, this means that the red line between Safety, Security and Digital Twins is like this:

# In practice, in operation, in a Brownfield:




OT Domain
Field
Eng
Automation
10
NOA
CPC
MTP
CPS
SmartGrid
20
Simulators
30
OT EDGE Services
40
AAS Service
AAS C1
50
OPC UA Service
OPC UA Server
Platform Independent
60
Model Service
<AutomationML/>
70
NOA M+O
80
FDI Service
90
MTP Service
100
Remote Access Service
110
Digital shadow
120
Graph/ AI/ML
130
Digital Twin
AAS
OPC UA Companion Spec
Instr. submodel, PA-DIM
Maintenance submodel
SM: Time series submodel
Alarm submodel
SM: DEXPI
Work Order
SM: Digital Nameplate
SM: MTP
Handover: VDI 2770
SM: Simulations
SM: CCM
SM: ILAP
SM: Carbon Footprint
SM: DPP, Digital Product Passport
180
Owner/ Operator
200
Gov
GOVERNMENT
220
DPP – Digital Product Passport
PCF – Product Carbon Footprint
Yellow Pages /registry
190
210
Collabor8
BIM
BUILDING INFORMATION MODELLING
MANUFACTURING-X
ISO 15926
Process Engineering
IEC 61970-CIM
Common Information Model
140
Requirements
IEC Standards
Eq hub
150
ERP
Work Order
Inventory
Maintenance
Planning
160
Engineering
Functional Structure
Model Based System Engineering
DMS/LCI
P&ID
PFD
170
Simulations
Simulators
FMI
AML/DEXPI

# And writing governing documents to explain that story, based on international standards, of cause!!!



# Twin4Safety

OREDA
DNV

SAP

Field Eng

IACS


## SIF Statistics

- SM: Equipment Failure

## SIF Maintenance

- SM: PM (Plant Maintenance)
- SM: Work Order

## Safety Perfomance

- SM:61508 Safety Performance
- SM: Id, Namepl. etc
- SM: Integrity ( Failure/PFD)
- SM: Functional (travel time, Leak etc))

## Safety Perfomance

- SM: Statistics
- SM: SIF Performance

## Engineering Role

- SM: Design requirements

Equinor

PSA
GOVERNMENT

Yellow Pages /registry


Other Plants

**Standardization**

IDTA

Number of our submodels: 61

New submodels
- Work Order
- SIF Design Performance

OPC UA

New Companions Spec
- SIF Operational Performance

# BAARNESKIRENN!!


Finull-
garn

?