iaHAZOP: Digital Twin-based Risk Management

Michael Pfeifer

EPSC Webinar, 4th July 2024

Add value.
Inspire trust.

TÜV SÜD at a glance

1

Provider of comprehensive and specific solutions

150+

Years of experience in the fields of safety and sustainability

1.000+

Locations worldwide

26.000+

Employees

€ 2,9

Billions
Annual sales

100 %

Independent and objective

TÜV SÜD experts around the world support you with a comprehensive portfolio of technical solutions to assess risks, build trust in technologies, enable progress and create access to your target markets.

It’s all about events…

Production = **Value Creation**

KPI’s

Production:
Processes
Technology
Humans

Guardians of Value Creation:
HSE + Maintenance

Events:
Human error
Degradation mechanisms
Technical errors

What if there would be 0 events?

What will the event statistics / KPI look like …

Production = **Value Creation**

Production:
Processes
Technology
Humans

Events:
Human error
Degradation mechanisms
Technical errors

vs.

Tech. Risk management:
manual
excel based

Aggravating boundary conditions

… when the workload & capacity gap grows?

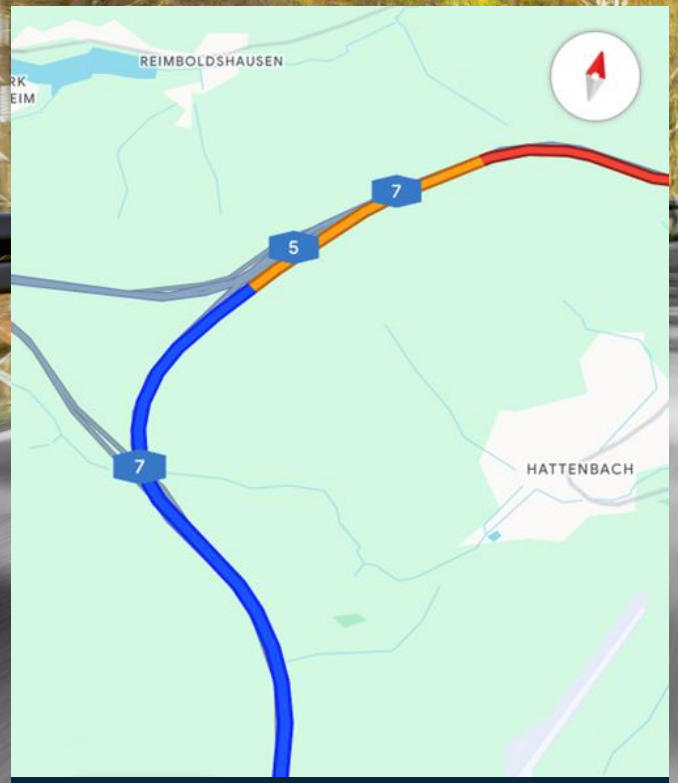
What if this mindset exists in the company…

We have always done it this way.

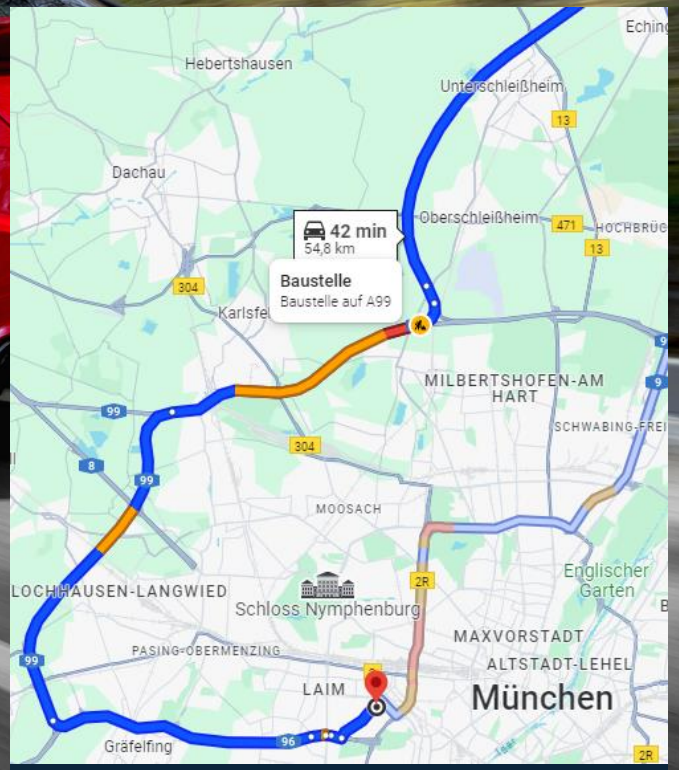
That's the only possible way.

… what will the return of invest in 5 years look like?

Let’s rethink technical Risk Management: iaHAZOP



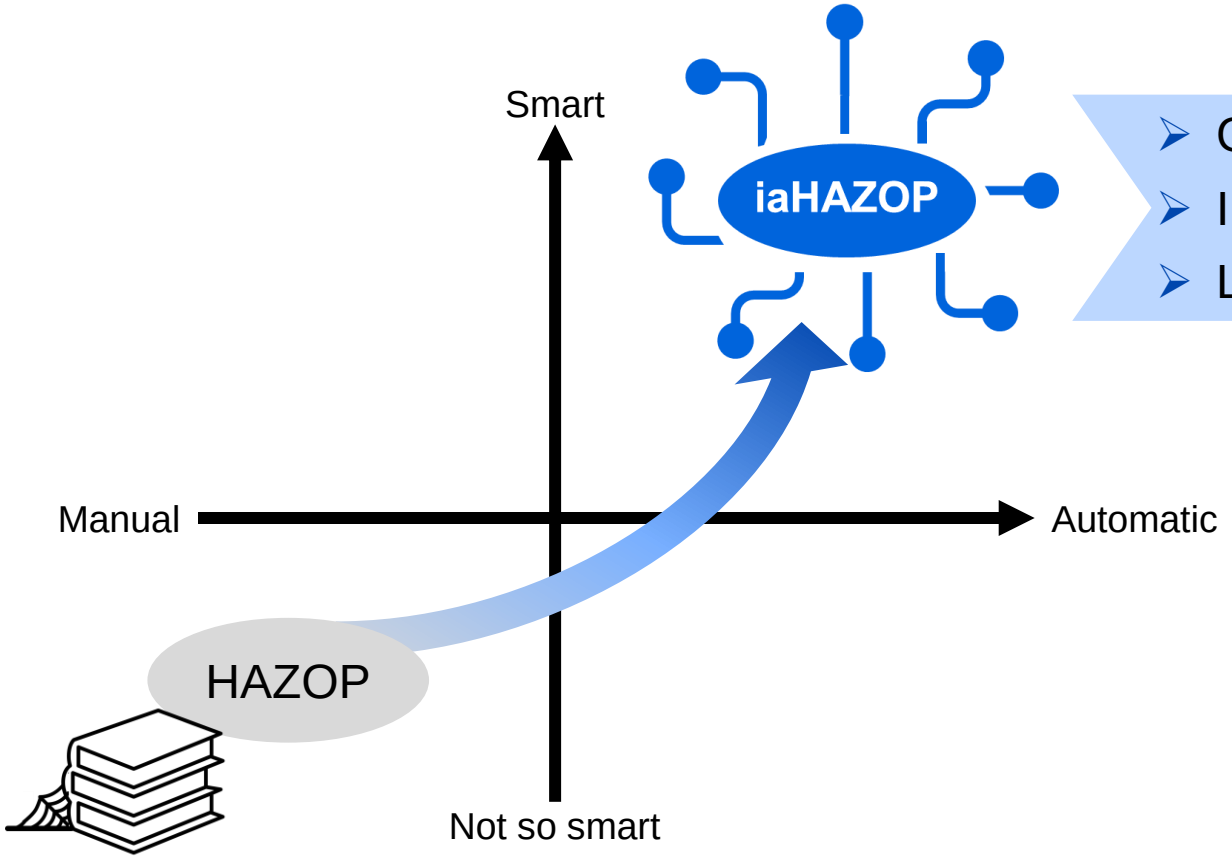
Runtime Risk Management @ Operation



Virtual Risk Assessment @ Planning

Map picture source: google maps

Target Image



- Get information on time
- Improve decision support
- Less incidents

- More **Uptime**
- Higher **Productivity**
- Increased **Efficiency**

Get more out of your HAZOP!

Reactive “firefighting” ➔ **Predictive Risk Management**

What if a system had predicted…

Maintenance of a valve

- Boiler still hot with water in it
- Low residual pressure overlooked
- LMRA → ok
- Maintenance staff scalded by steam → Hospital
- Work had to be compensated by others

→ **Longer unplanned maintenance time**

→ **liability event & - xx xxx xxx €**

Change of a System

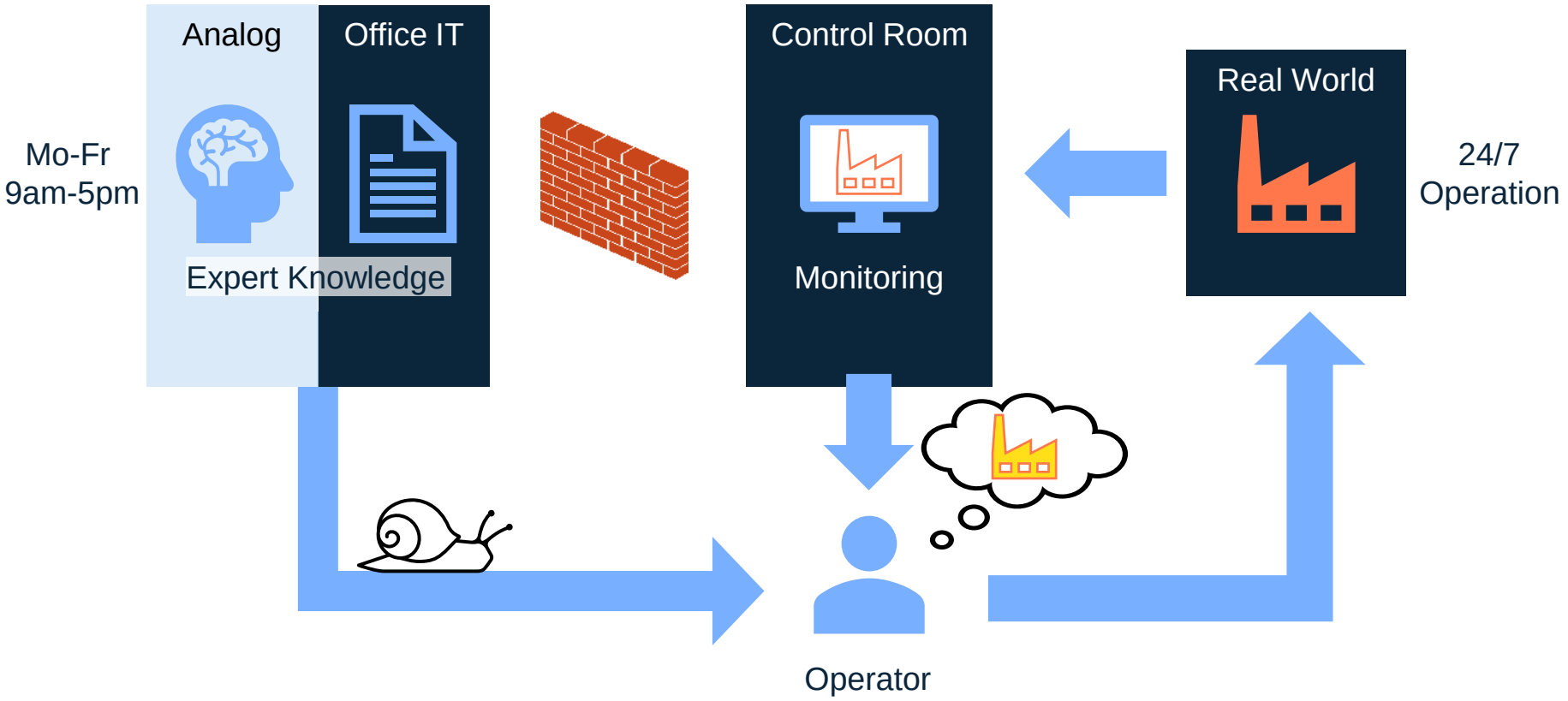
- Risk assessment has not been updated
- Damage mechanism overlooked
- Leakage of nitric acid
- Other system parts affected
- Major cleaning operation and replacement of many flange screws

→ **Plant shutdown for several weeks**

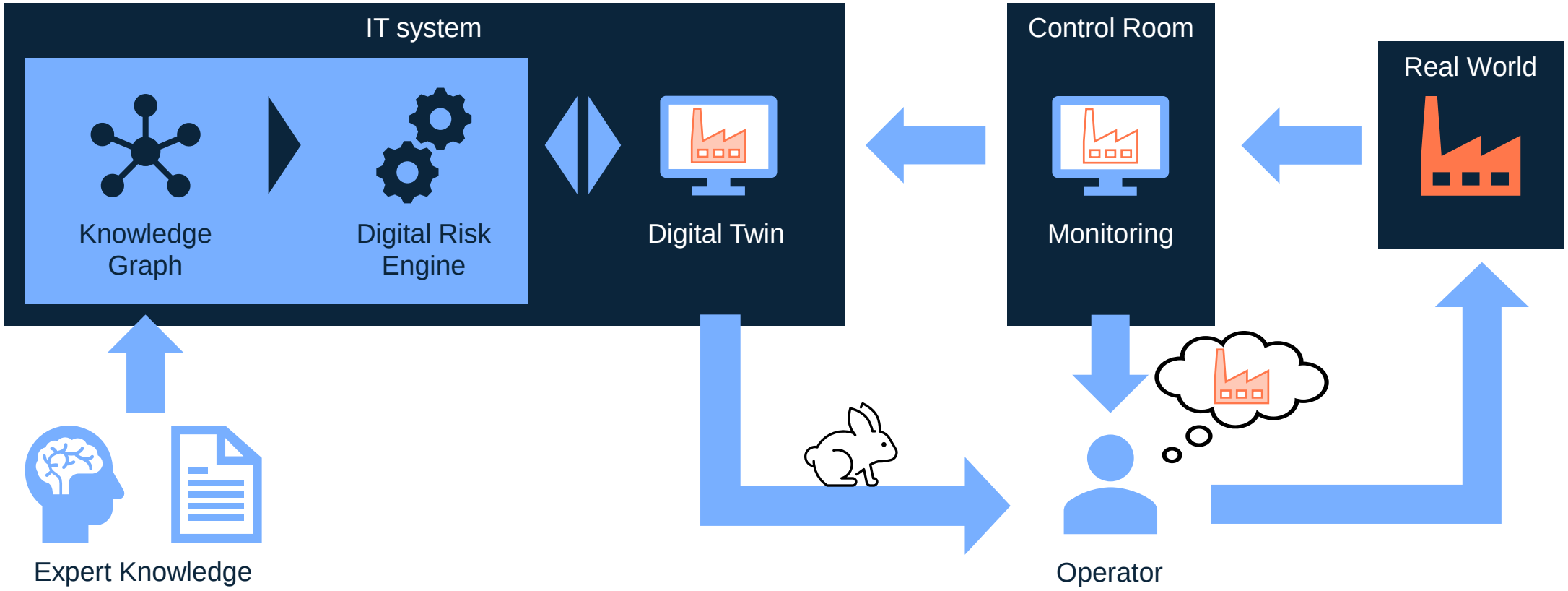
→ **unfulfilled supply contracts & - xxx xxx xxx €**

➔ Small cause, big (avoidable) Effect

Today: Interrupted Information Flow



Solution: iaHAZOP for Resilient Operations



Architecture - How does it work…

Behavior model

Digital Twins
- Machines
- Components
- Workpieces or Process media

Sensor Data

Current status

Regulatory framework
(Risk Acceptance level)

Defines Risk number allowed

Hazard & Safety Rules

Rule based approach

Plausibility check

System
Adaptive
Safety
Security

Digital Risk Engine*

Comparison risk number allowed - achieved

Digital Twin based Safety

- Risk Score
- Context sensitivity
- Decision Support

It's like having a risk buddy 24/7 onsite!

*Patented

Formalizing the Language of Risk

Today's Risk Assessment

Traditional methods tailored to human needs

Digitalization

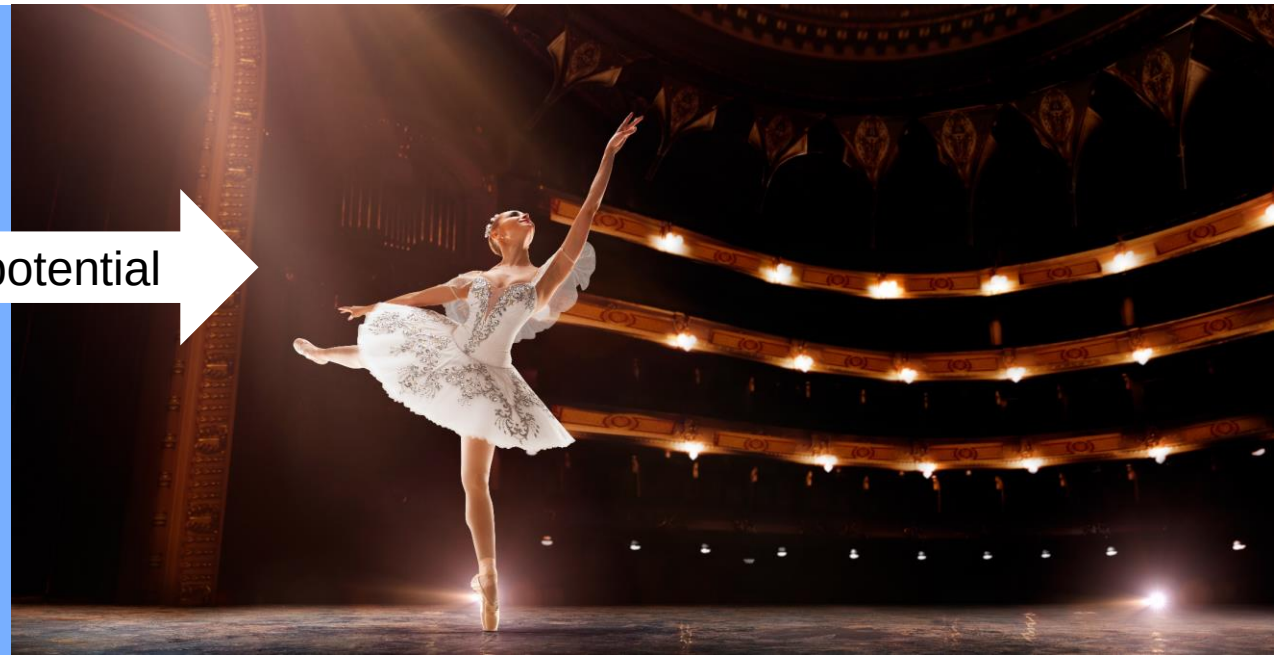
Human's risk processing **bottlenecks**
Digital twin's performance

Risk Assessment for Digital Twins

Express hazards based on parameters

➔ **Machine processable**

Use the full potential



Evolution in Risk Language (HSE)

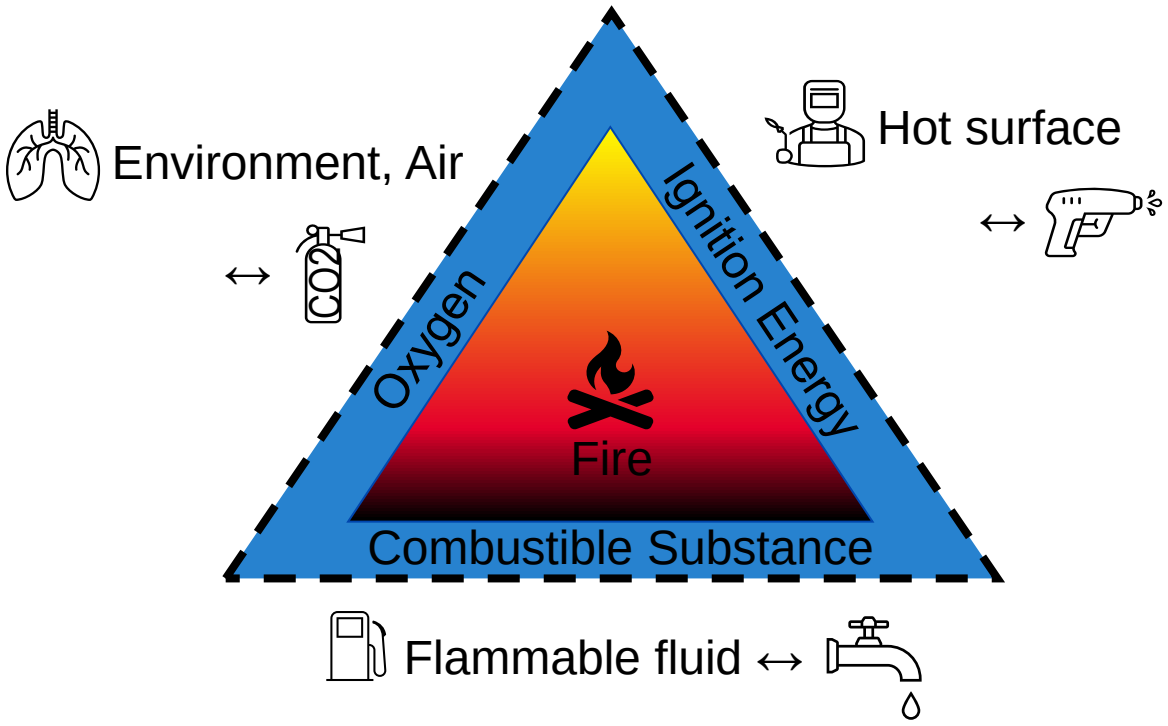
Hazards don't care about assessment standards and industry branches

- People are injured or killed by an unacceptable amount of energy transfer
- Hazards can be described by physical parameters

The current risk language is a simplification for human needs

Digital twins allows us to break through these historical boundaries

Hazard Rule example:




```
If(  "Oxygen" AND
     "Combustible_Substance" AND
     "Ignition_Energy")
then
     "Fire_Hazard"
```

HAZOP translated into iaHAZOP

Static HAZOP

Guideword	Description	S	P	Risk	Measure
Backflow	Backflow of flammable mixture into the storage tank	6	1	$R = f(S,P)$ = 6	Operation monitoring and shut-off valve with SIL

Human Risk Language

translation

iaHAZOP

Failure mode → **Triggers** → **Hazard Rule** → **Risk Calculation** → **Safety Rule**

The **failure modes are processed by the program** using simulation data and logical functions

The effects and the recognizability of the **hazard are** represented in so-called **Hazard Rules**

Dynamic risk calculation

Protective measures are mapped as **countermeasures** in so-called **Safety Rules**

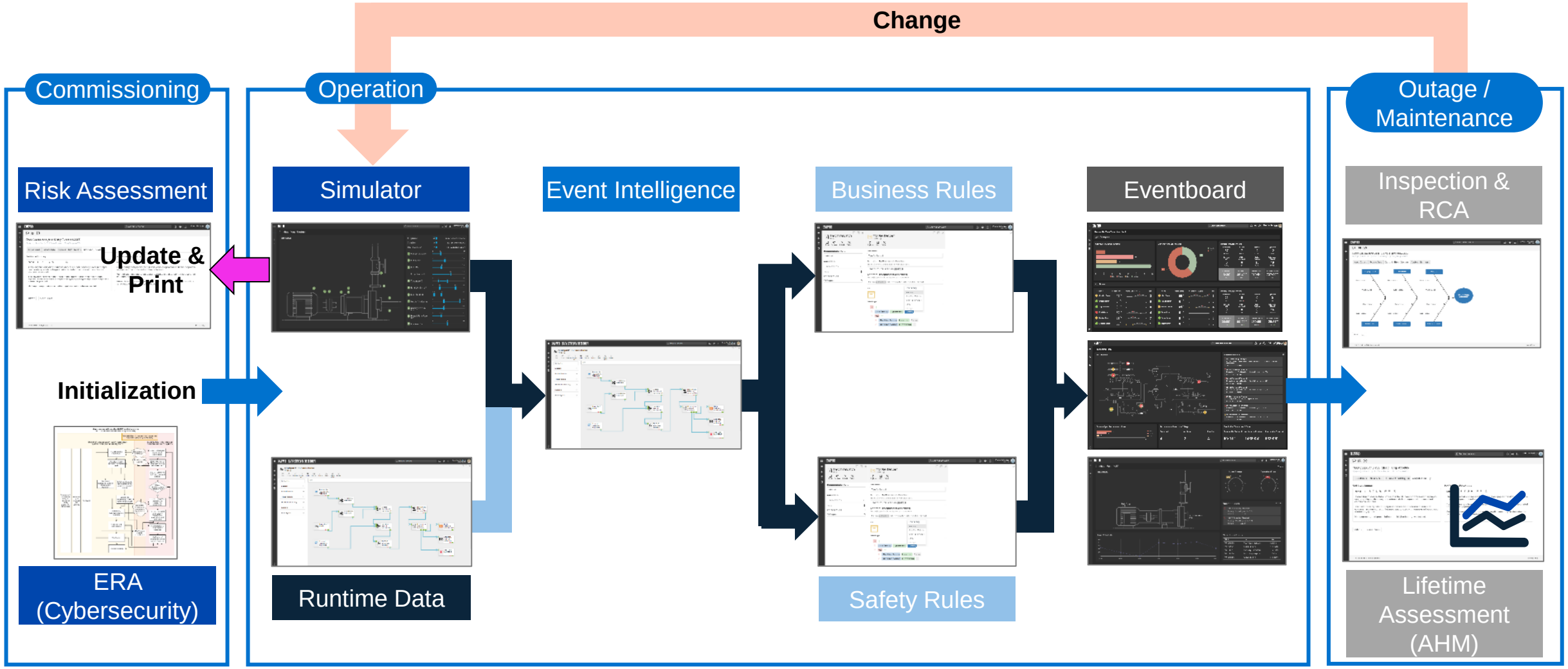
Model / Digital Twin

Software processable Risk Language

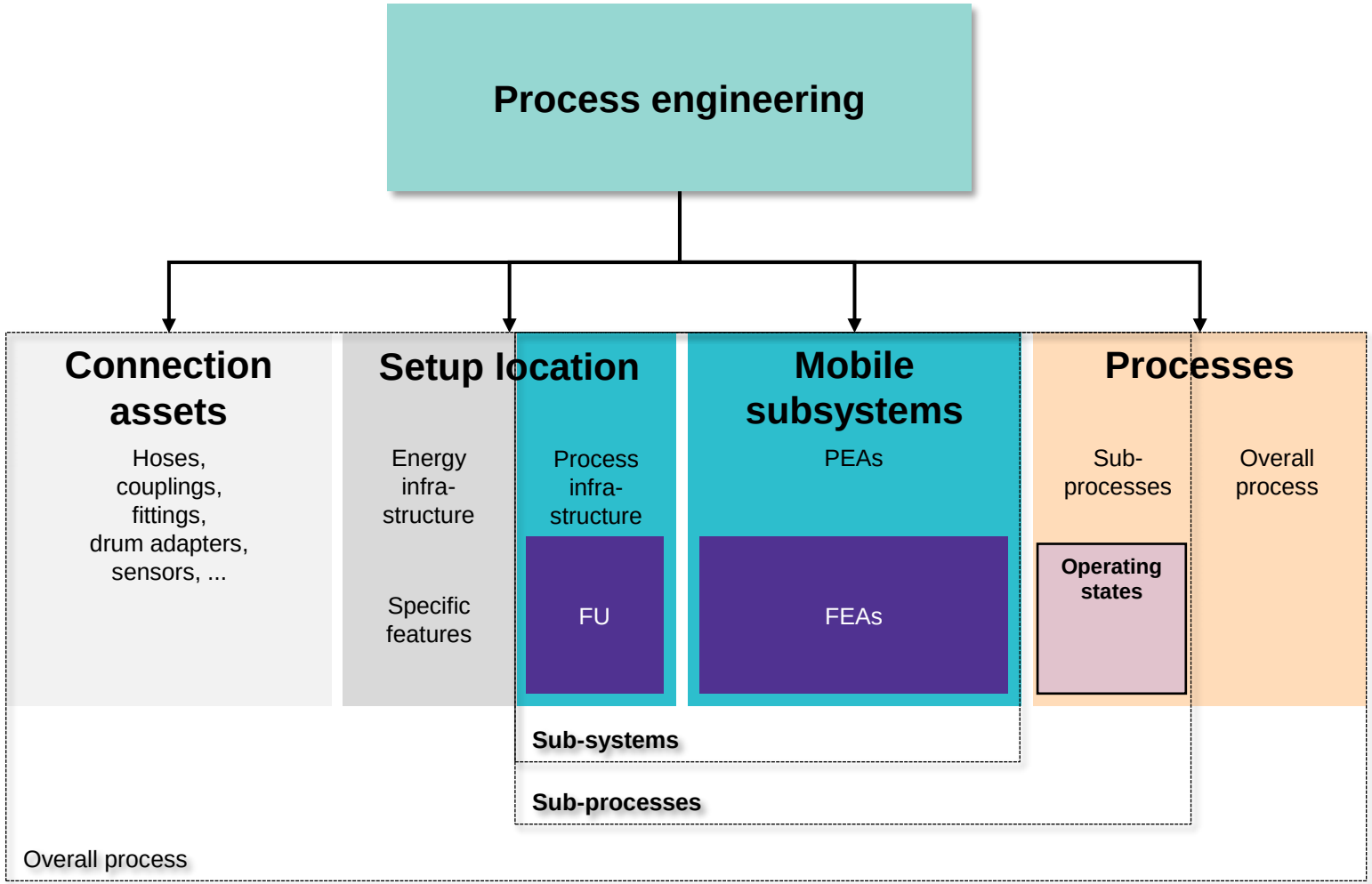
iaHAZOP (Based on the Digital Twin) = **System FMEA**

The results can also be translated back into the HAZOP system

Adaptive Safety during Runtime



Proof of Concept for Modular Plants



PEA: Process Equipment Assembly (VDI 2776)

FEA: Functional Equipment Assembly (VDI 2776)

FU: Functional Unit (IEC 61882)

Source: Merck Group

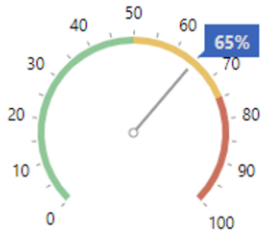
Haber Bosch Process - Hazard Scenarios

Thu Nov 30 2023 15:42:11 GMT-0600 (Central Standard Time) Reset

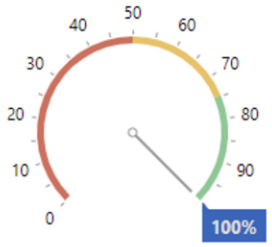
Hazard Rules

#	Title	Location	Status	Measures
1	Overpressure	Reactor		Redundant pressure sensing
2	Overpressure	Pre-Heater		Max. allowed working pressure
3	Material compatibility	All		Check for material compatibility
4	Burn at hot surface	All		Only trained works permitted
5	Back flow	-		NA

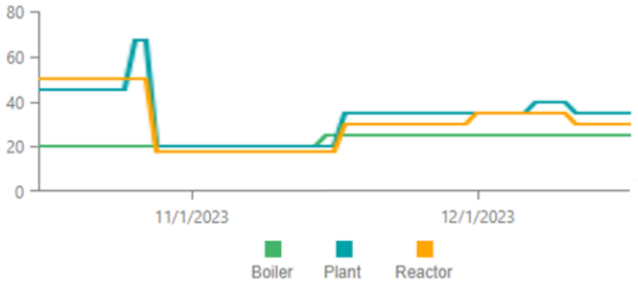
Current Risk Score



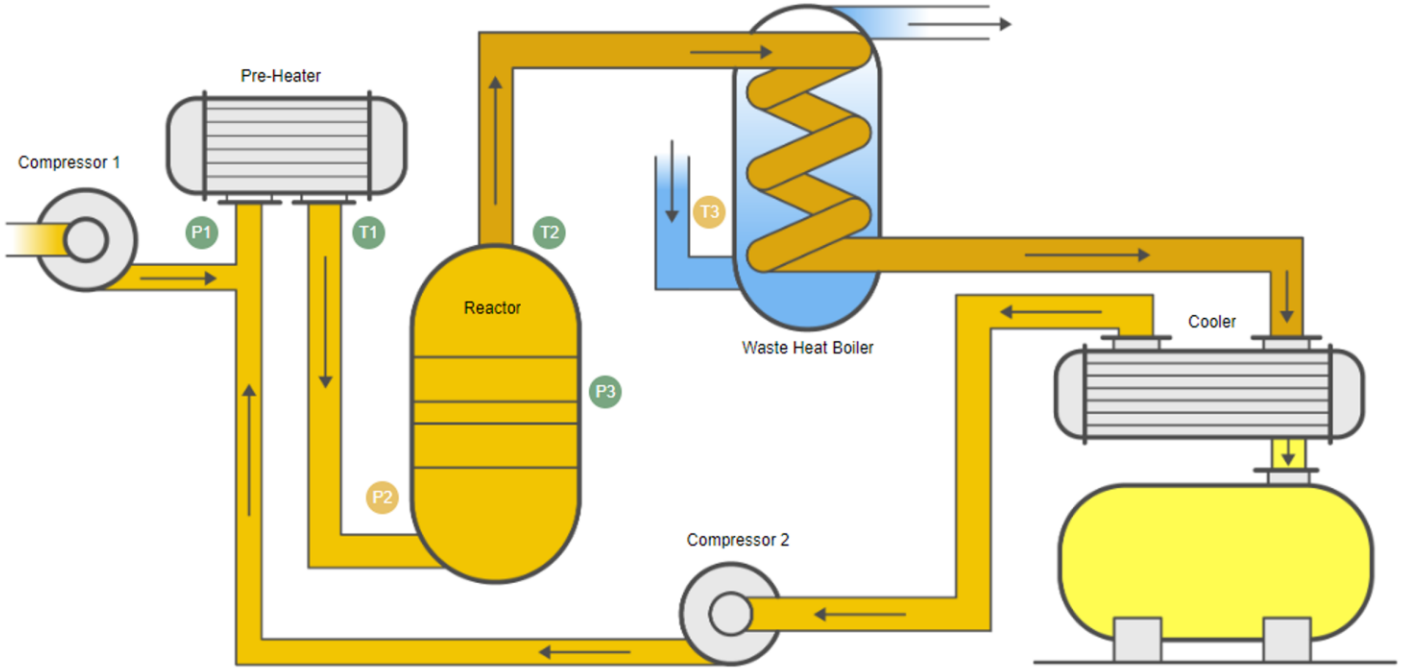
Current Productivity Score



Plant Risk Score Trend



Process Overview



Recommendations

Sensor P2 Error
Redundancy for hazard rule #1 only simulated
Nov 30, 2023 3:42 PM

Scenario Modular/Adaptive Process

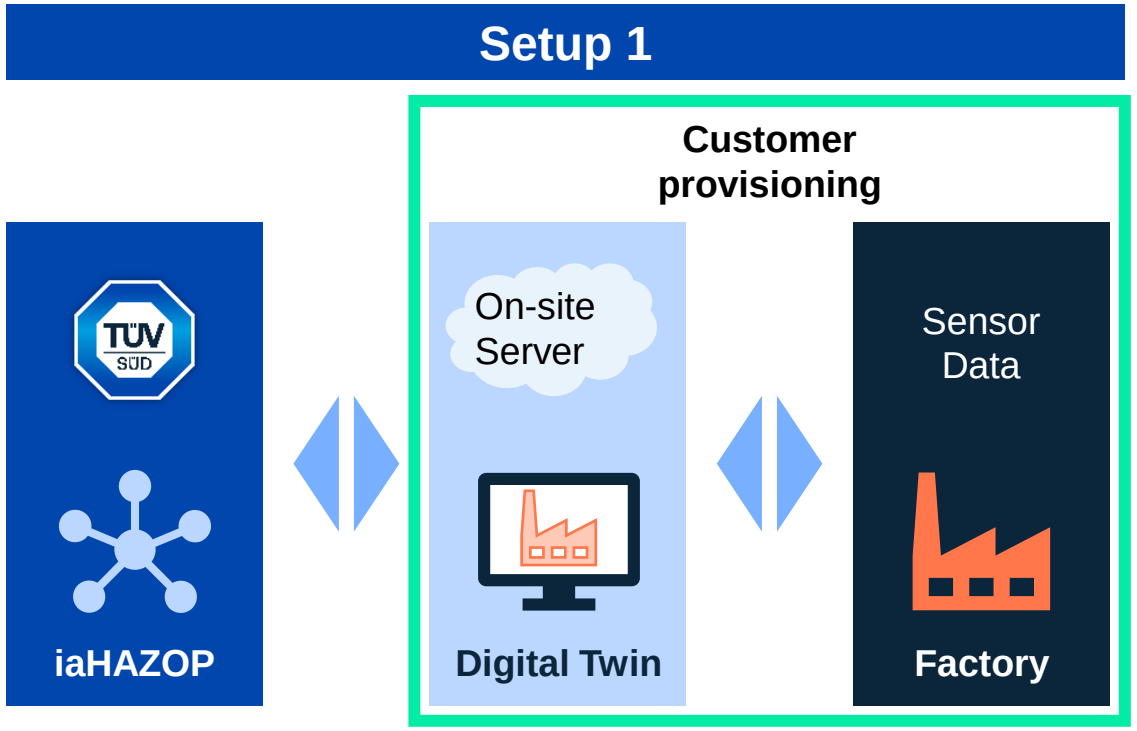
Trigger the Scenario OFF Not Running

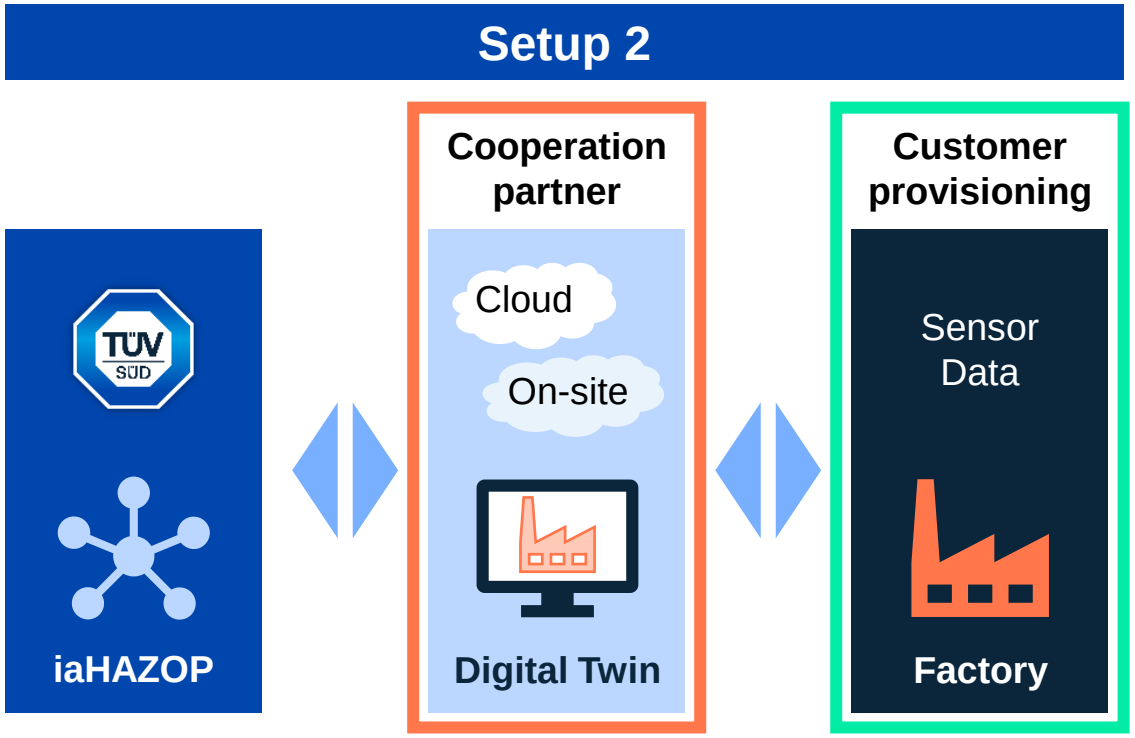
Project Setup

Realization:

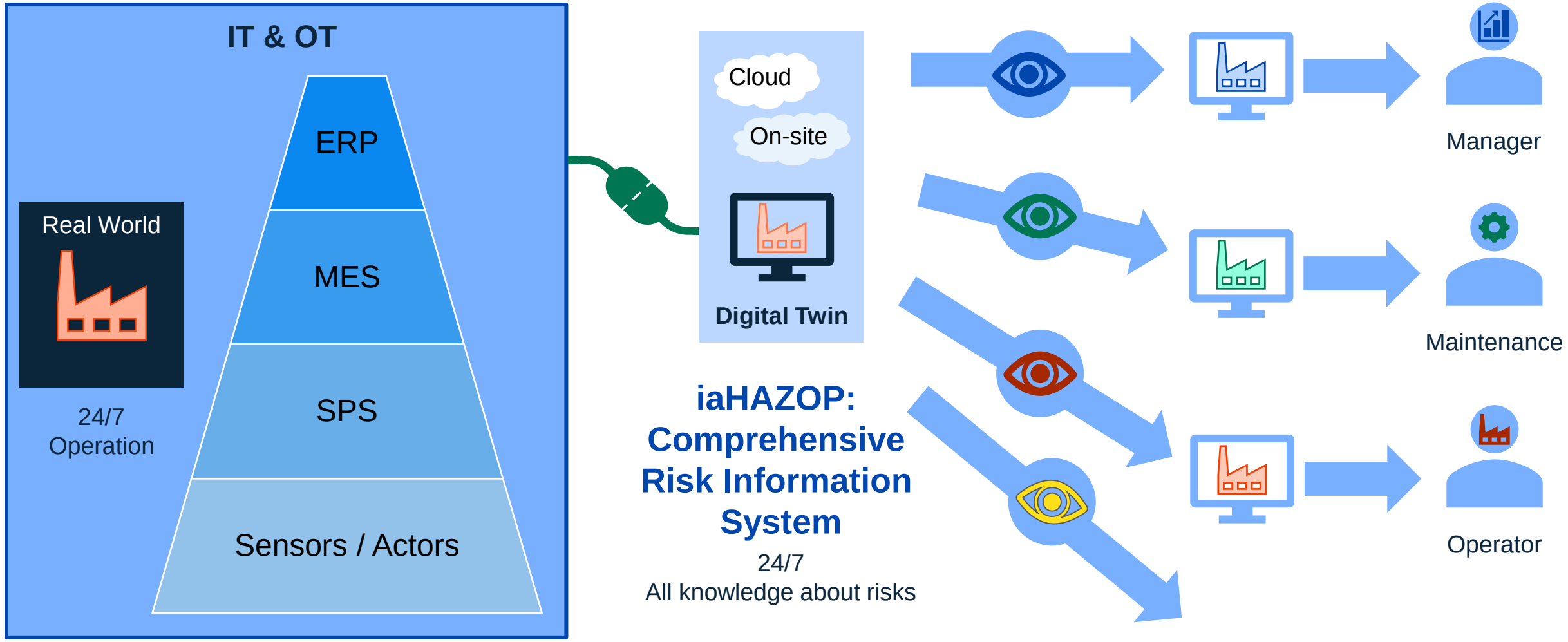
1. **System understanding and feasibility**
2. Pre-Setup of solution and **detailing of target picture**
3. **Setup of digital solution**
4. Operation – **Runtime Risk Management**

We formalize the language of risk and extract hazard rules





Architecture



iaHAZOP: Digital Twin based Risk Management

Benefits

- **Time to market**
  Plant Modifications
  → **Immediate update of risk assessment**

- **Up-time**
  Improved decision support and LMRA
  → **Less incidents**

- **Efficiency**
  Use of resources incl. high qualified staff

- **Faster**
  Fewer events grow into incidents or accidents
  → **Less liability events**

➔ Transform from reactive to **predictive risk management**

It’s time for the next level…

…now, together!

Contact:

Michael Pfeifer
Smart Safety Lead Architect
Certified SIRI-Assessor

E-mail:
michael.pfeifer@tuvsud.com
Phone:
+49 89 5791-3329

Alexander Kurdas
Digitalization Designer
Machine Safety Engineer

E-mail:
alexander.kurdas@tuvsud.com
Phone:
+49 89 5791-1005

Follow us on:

tuvsud.com
info@tuvsud.com
iahazop@tuvsud.com