



# Cyber attacks on process plants

possible consequences and mitigation with process safety tools

Dr. Stephan Burmberger, Dr. Stefan Rath  
European Conference on Plant & Process Safety  
Köln, 12.12.11.2019

Making our world more productive





### Dr. Stefan Rath

- Linde Engineering since 2000
- Department: Process- and Environmental Safety
- Group Lead “Risk studies and systematic Analyses”
  - HAZOP
  - HAZID
  - Quantitative Risk Analysis - QRA
  - Consequence Modelling (Dispersion, Fire, Explosion)
  - Rootcause Analyses
  - Technology Qualification Reviews
  - RAM
- Chairman of „ProcessNet“ working group “Risikomanagement”, Frankfurt, Germany



<https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>

*“a petrochemical company with a plant in Saudi Arabia was hit by a **new kind of cyberassault**. The attack was ...meant to sabotage the firm’s operations and **trigger an explosion**”*

*“The **only thing that prevented an explosion was a mistake in the attackers’ computer code**, the investigators said.”*

*“The **attack was a dangerous escalation in international hacking**, as faceless enemies demonstrated both the **drive and the ability to inflict serious physical damage**.”*



- Cyber Attacks on OT - Operational Technology (e.g. DCS, SIS) have been reported
- Improvements in operational technology minimize the probability of a successful cyber attack
- **BUT:**
  - Plants engineered today will still be in operation in 20, 30 or 40 years
  - Ongoing digitalisation

Quote: “... a DCS system will never be 100 % cyber secure”

Quote: “What is considered adequately protected against cyber attacks today might not be tomorrow”

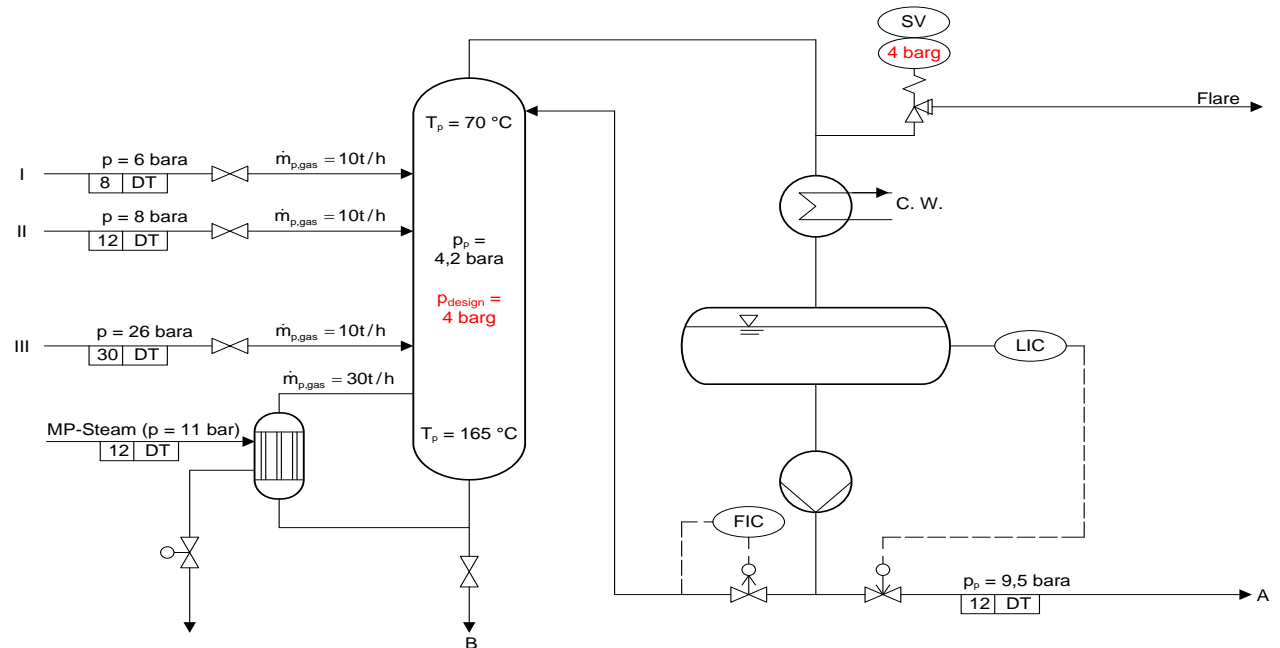
Quote: “The word of cyber safety can undergo significant changes within one day”

### Questions:

- What are possible consequences of successful cyber attacks on process plants?
- How can these consequences be mitigated?

## Situation

- Attack successful → transfer of process control
- Safety concepts are based on single failure principle (ref. to API 521)
- Hacker can cause targeted multi-jeopardy scenarios (e.g. rectification column, flare control valves, etc.)
  - Not covered by safety concepts
  - Damage of equipment, LOC, release of fluids (toxic, flammable), fire, explosion, etc, possible





## Situation:

- Attack successful → Loss of basic safety functions  
→ Damage of equipment, LOC, etc.
- More comprehensive cyber security measures can be applied for the SIS than for the DCS:
  - Isolation of SIS from other systems
  - Limited access to SIS
  - Implementation of OT cyber security measures

## Judgement?

- SIS sufficiently secure against cyber attacks?  
→ application of SIS for protection against cyber attacks on DCS possible
- SIS NOT sufficiently secure against cyber attacks?  
→ in high risk areas additional protection measures for SIS required

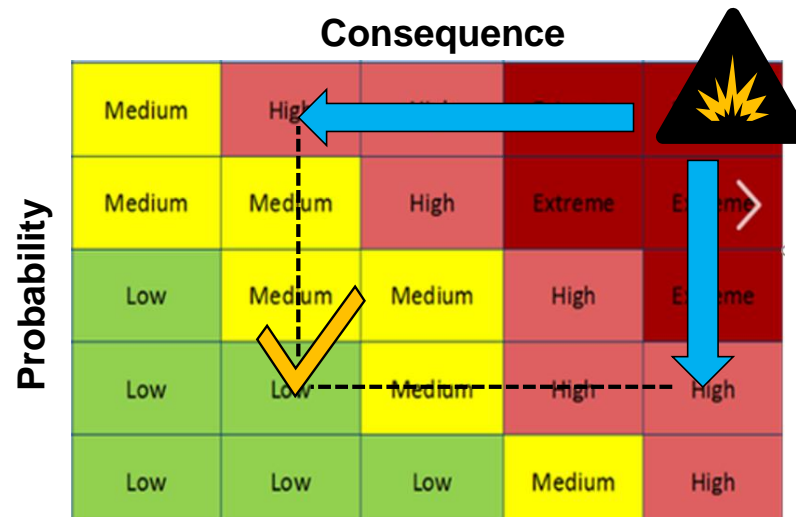
## Aim: Reduction of the Risk



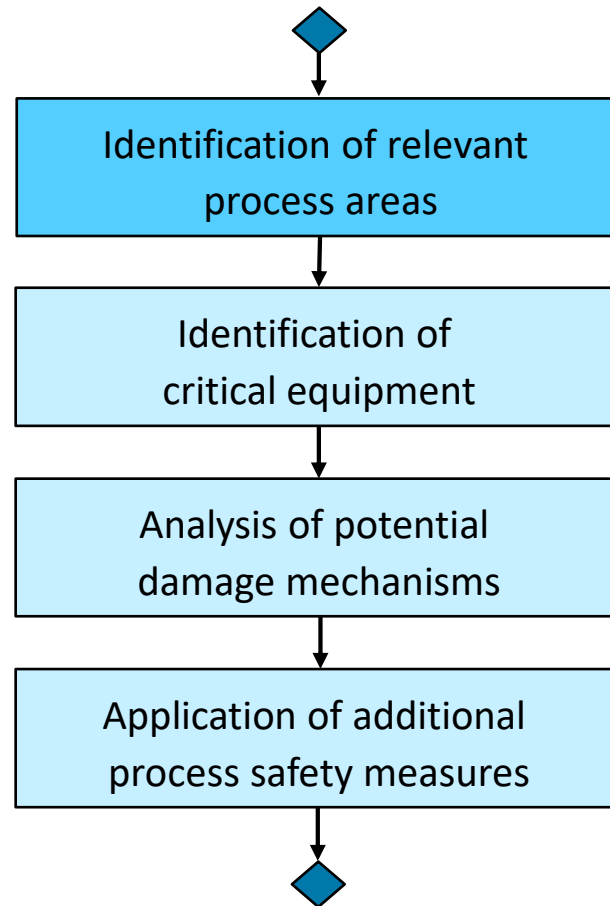
OT / IT Measures reduce the **PROBABILITY** of successful cyber attacks

Specific safety measures reduce the **CONSEQUENCES** of successful cyber attacks

Combination of both reduces the **Risk**



## Possible Approach





## Identification of relevant process areas

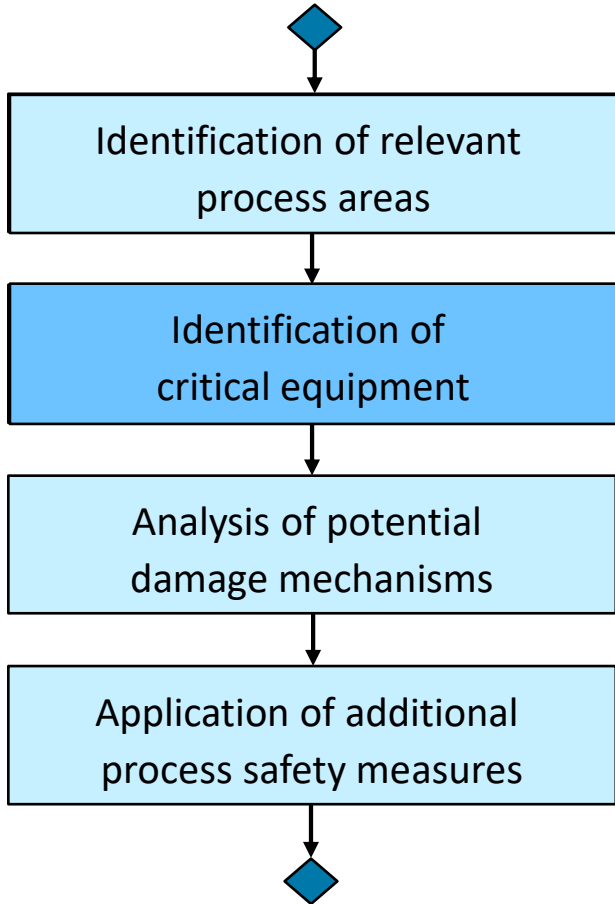


- Process areas containing high amount of hazardous materials acc. to z.B. SEVESO III

| <b>Dangerous Substances acc. to Seveso Directive III</b>               | <b>Upper Tier<br/>[t]</b> |
|------------------------------------------------------------------------|---------------------------|
| <b>flammable gases</b>                                                 | <b>50</b>                 |
| <b>flammable Liquids Class A (flash point <math>\leq 60</math> °C)</b> | <b>50</b>                 |
| <b>flammable Liquids Class B (temperature above boiling Point)</b>     | <b>200</b>                |
| <b>Flammable Liquids Class C (not covered in Class A and B)</b>        | <b>50.000</b>             |
| <b>Oxygen</b>                                                          | <b>2.000</b>              |
| <b>Chlorine</b>                                                        | <b>25</b>                 |
| <b>Hydrogen</b>                                                        | <b>50</b>                 |
| <b>liquefied flammable gases and LPG</b>                               | <b>200</b>                |

- Hazards to third party population

## Possible Approach



- Process areas to be assessed

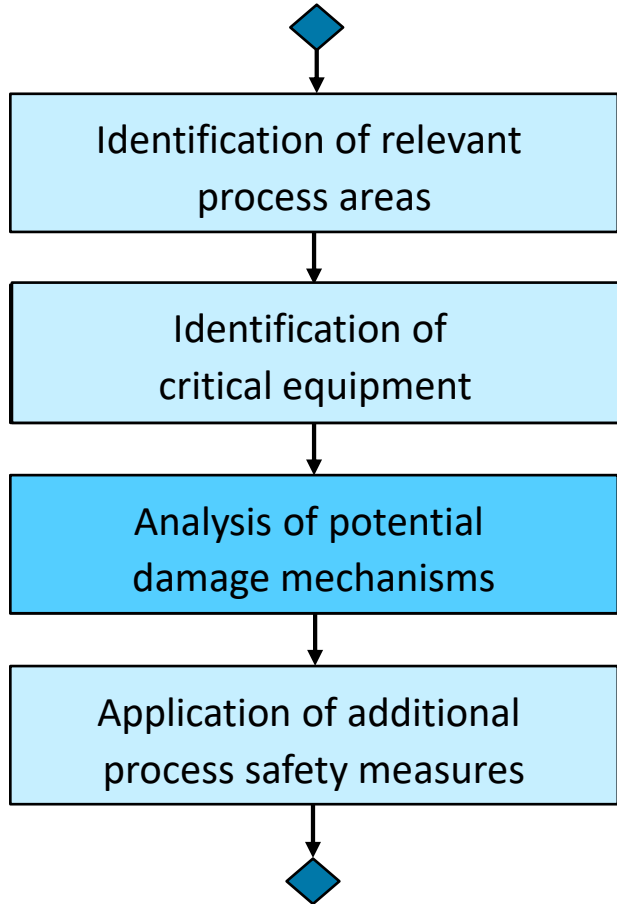
# Identification of critical equipment



- Which equipment would cause most disastrous consequences in case of damage?
  - hazardous materials processed / stored (flammable, toxic, radioactive, ...)
  - size of equipment / mass of hazardous materials
  - process conditions (pressure, liquefied gases,...)
  - vulnerable vicinity
  - safety critical equipment (flare system,...)



## Possible Approach



- Process areas to be assessed
- Critical equipment to be protected

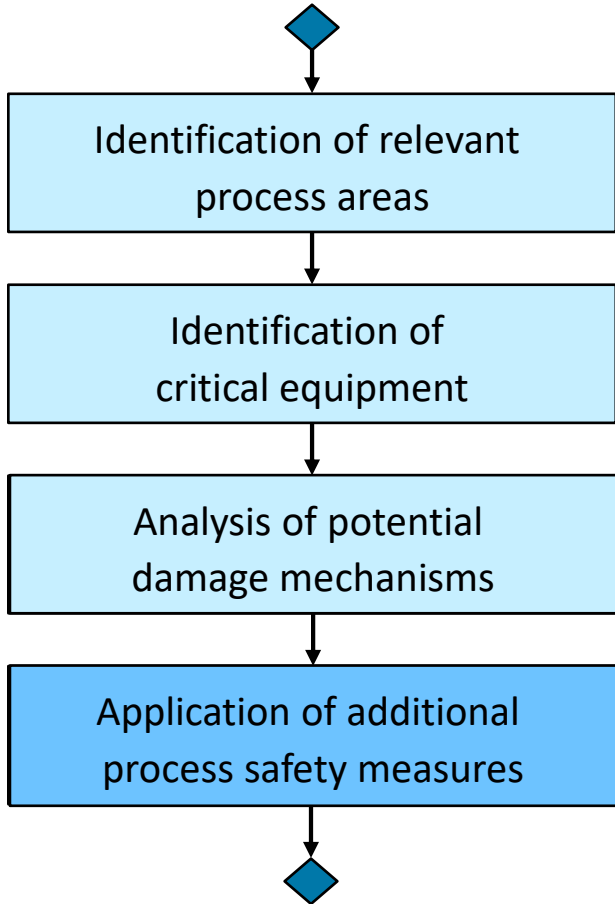
## Analysis – which additional measures are required?



- How can the critical equipment be damaged?
  - attack on DCS → targeted induced multi-jeopardy scenarios (→ assessment of the PID)
  - attack on SIS → manipulation of SIS (→ assessment of SIFs)
  - damage by domino effects (e.g. explosion of steam-boiler close to critical equipment, ...)  
(→ assessment of plot plan)
  - other manipulations (e.g. wrong sequence steps, ...)



## Possible Approach

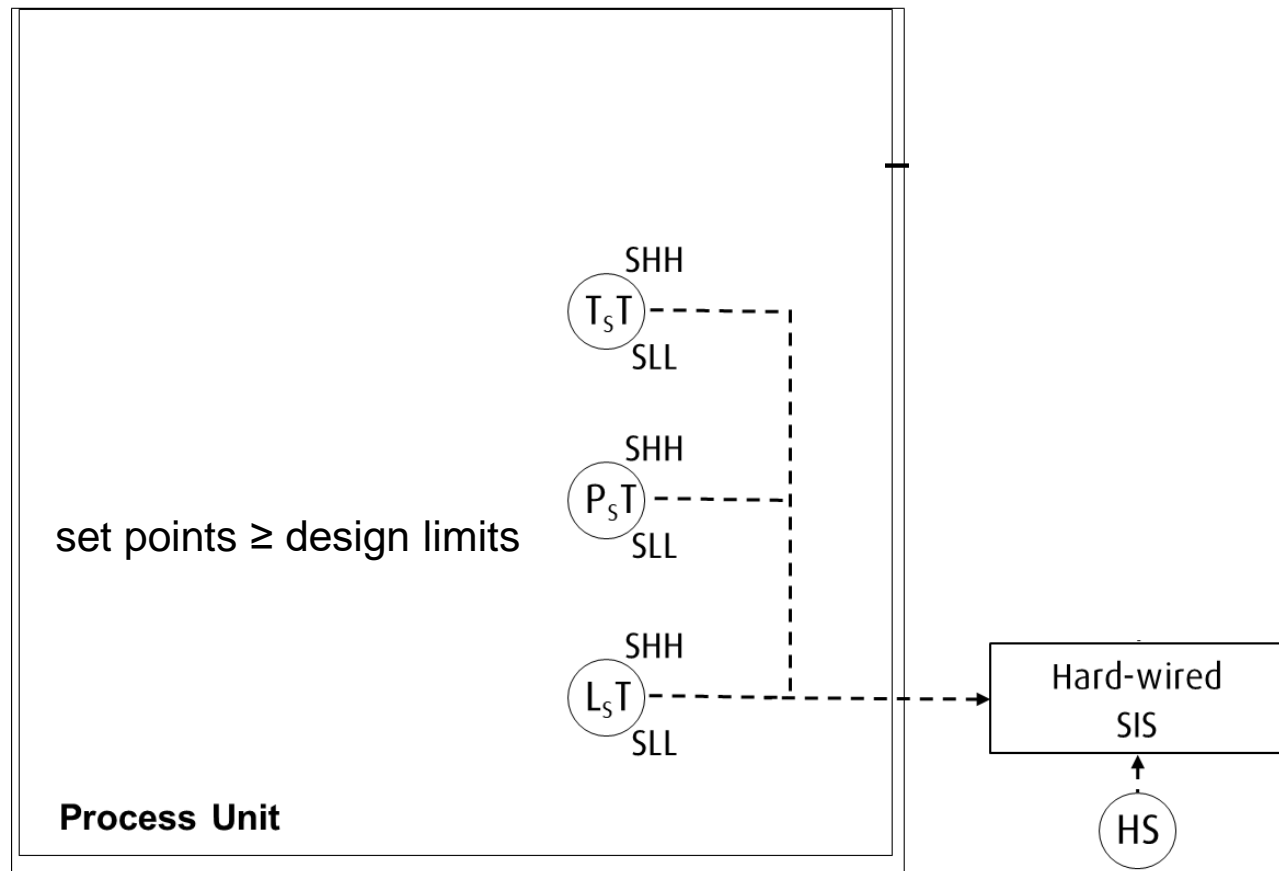


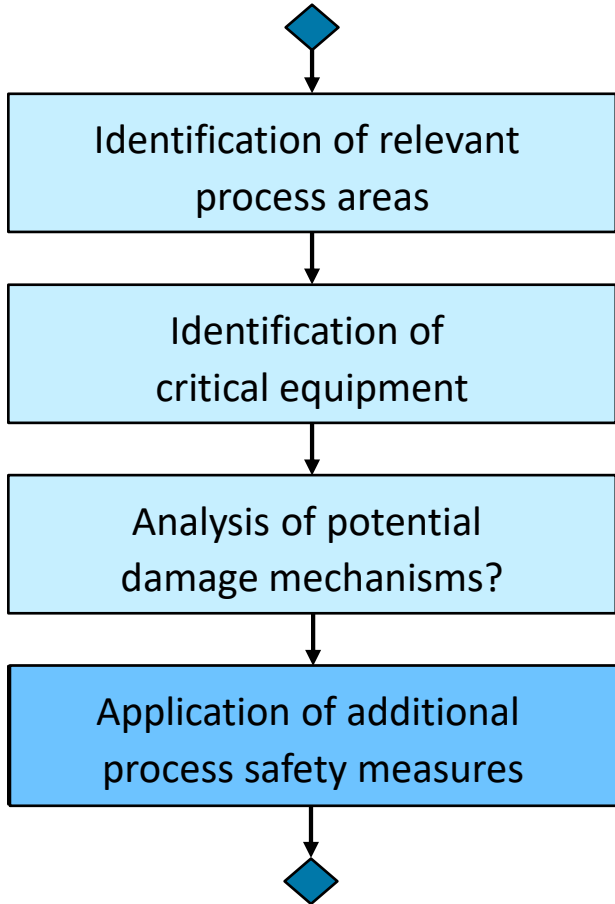
- Process areas to be assessed
- Critical equipment to be protected
- Damage mechanisms to be prevented

# Application of additional process safety measures



- Change of design (PSV sizing, mechanical design conditions, material selection, ....)
- Additional SIF (measure for protection of DCS)
- Hard-wired SIF
- Dedicated Cyber-Attack Protection Trip





- Process areas to be assessed
- Critical equipment to be protected
- Damage mechanisms to be prevented
- Process safety measures to be implemented to prevent catastrophic outcomes

**Is this too expensive?**





### DCS

Example: Analysis of the main process unit of a natural gas plant (57 PID pages)

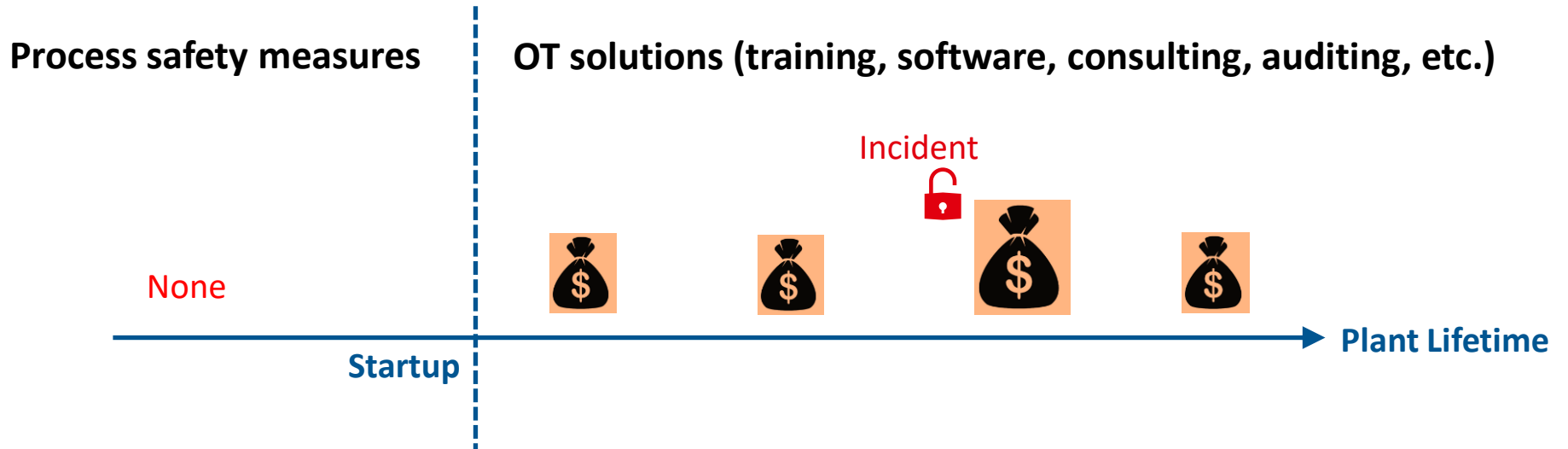
- 3 times: extension of existing SIS (activation of additional, existing valves)
- 5 times: additional solenoid valves or SIF required (estimated cost < 35.000,-Euro)

### SIS

Example: Analysis of a natural gas plant (120 SIL Loops)

- 23 SIL Loops classified as consequence „severe“
    - 15 protected with PSV already
    - 8 required additional protection
- additional protection required for approx. 7% of all SIF of the plant

# Money spent on Cyber Security





## The aim is **NOT** to

- question the process safety design according to the state of the art
- add extensive additional safety measures to all process plant installations

## The aim is to

- raise awareness of hazards by cyber attacks on process plants
- apply additional process safety measures in high risk process areas (these can be pragmatic)

## Outlook

- Discussion of possible approach with partners from process industry
- Application and testing of the approach for different process plants

## Further activities

- ProcessNet Working Group „Risk Management“ ([https://processnet.org/Fachgemeinschaften/Anlagen\\_+und+Prozesssicherheit/Risikomanagement.html](https://processnet.org/Fachgemeinschaften/Anlagen_+und+Prozesssicherheit/Risikomanagement.html))
- CeSIS - *Center for Safety Integrity and Security* (<https://cse-engineering.de/cesis/>)

# Cyber attacks on process plants possible consequences and mitigation with process safety tools



Linde Engineering  
Dr. Stefan Rath  
stefan.rath@linde.com  
www.linde.com





# Hardwired SIS– selected options



## Orbus Hardwired Safety Systems

### Proven solid state technology

The Orbus® range is based on well-proven solid state technology that is inherently exceptionally reliable. Typically this equipment is able to achieve very high levels of quantified safety integrity suitable for SIL 4 use. This range enable us to engineer systems that are pulse testable, fail-safe or combined. Additionally we are able to provide diverse systems for extremely onerous applications, as found within the Nuclear Industry.



Presentation Documents & Downloads

## Features

- Key Features include:**
- Safety Instrumented System specifically designed for applications which require the highest Safety Integrity Levels (SIL3 & SIL4)
  - Inherently Cyber Secure
  - Modular design allows users to create fault-tolerant, fail-safe or combined systems with very high availability, without compromising the superior safety performance
  - Extensively used in IEC61508 applications
  - Type tested via TÜV, BSI, GSI/PTB/IE & ENA
  - Provides diverse systems for rejection of common mode failures
  - Stable technology with proven use in a vast installed base with over 30 years of application in majority of process markets



- Control System
  - Distributed Control System (DCS)
- Safety Instrumented System (SIS)
  - SIS (Up to SIL 3) ProSafe-RS
  - Solid-state SIS (Up to SIL 4) ProSafe-SLS**
  - Software Based Solution Sustainable SIS
- SCADA System
- Process Control PLC/RTU
- Programmable Logic Controllers (PLC/PAC)
- Core Products Technology
- Controllers & Indicators
- Paper Quality Control System (QCS)
- Film/Sheet Thickness Gauge

Home / Products / Control System / Safety Instrumented System (SIS) / Solid-state SIS (Up to SIL 4) ProSafe-SLS

## ProSafe-SLS



Yokogawa is the world's most experienced safety and control firm. Our commitment to providing reliable, state of the art safety instrumented systems is rooted in a wealth of installations since 1962.

The solid-state, hard-wired ProSafe-SLS covers all requirements in process industries. The product line covers specific requirements for individual safety instrumented systems and offers all safety integrity levels (SIL 3-4) for the oil & gas, petrochemical, chemical, nuclear and conventional power industries.

ProSafe-SLS safety instrumented system is also fully integrated with Yokogawa's CENTUM VP process control system together with ProSafe-RS safety system as well as FAST/TOOLS SCADA software package.



## Planar4: Die SIL4-Steuerung für die höchste Sicherheitsstufe

Ob auf der Ölplattform oder bei der Erdgasförderung: In manchen Industriebereichen ist selbst der kleinste Kompromiss einer zu viel. Wo das Risikopotential so extrem hoch ist, benötigen Sie eine Sicherheitssteuerung, die immer fehlerfrei läuft und resistent gegen Cyberattacken ist. Mit dem Safety-System Planar4 von HIMA setzen Sie auf eine festverdrahtete Steuerung, die extrem robust und maximal belastbar ist. Natürlich entspricht sie den entsprechenden aktuell gültigen Normen. Und sie ist die einzige Steuerung, die für den Einsatz bis SIL 4 nach IEC 61508 Edition 2 (2010) zugelassen ist.