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

Introduction

Dr. Stefan Rath

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

Article in New York Times

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**."*

Motivation

- 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?

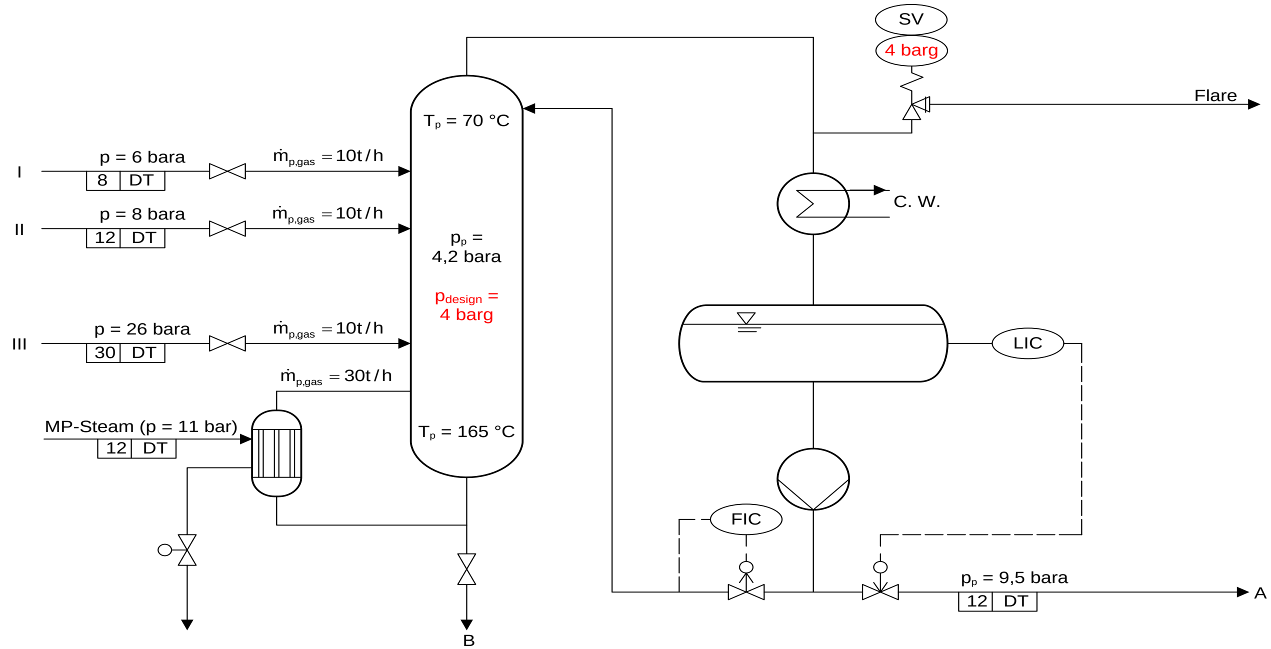
Cyber Attack on DCS

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



Cyber Attack on SIS

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

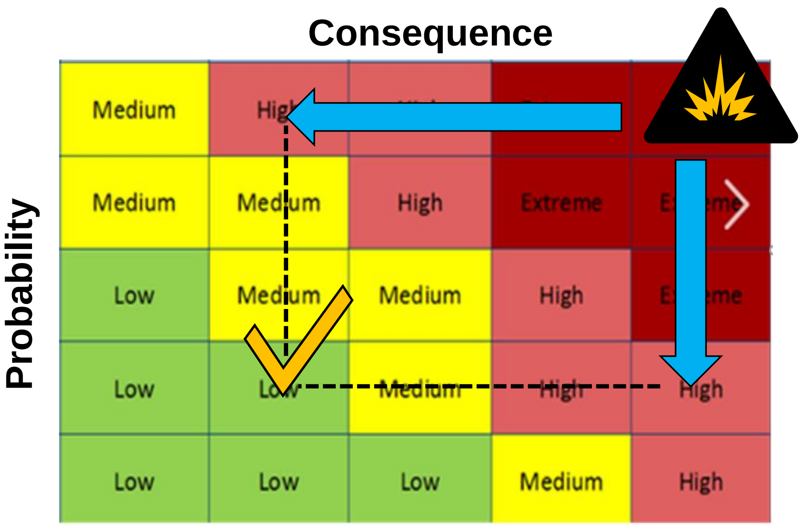
Aim: Reduction of the Risk

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

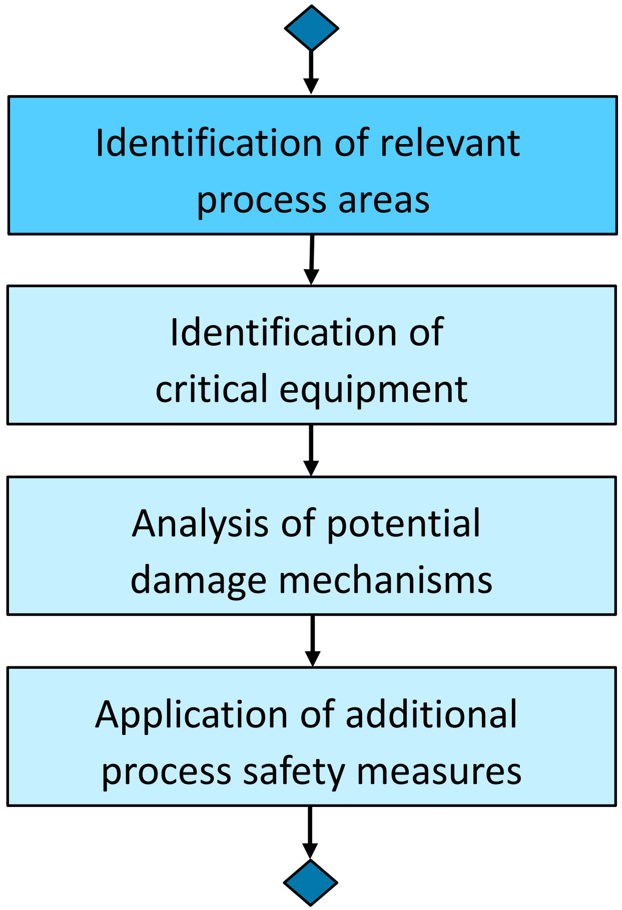
Specific safety measures reduce the **CONSEQUENCES** of successful cyber attacks

Combination of both reduces the

Risk



Possible Approach



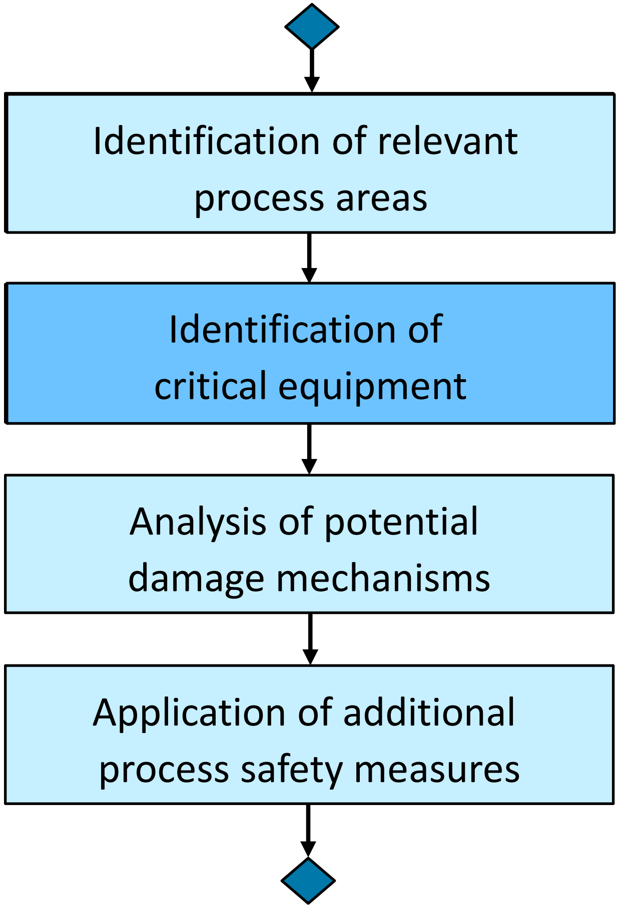
Identification of relevant process areas

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

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

- Hazards to third party population

Possible Approach

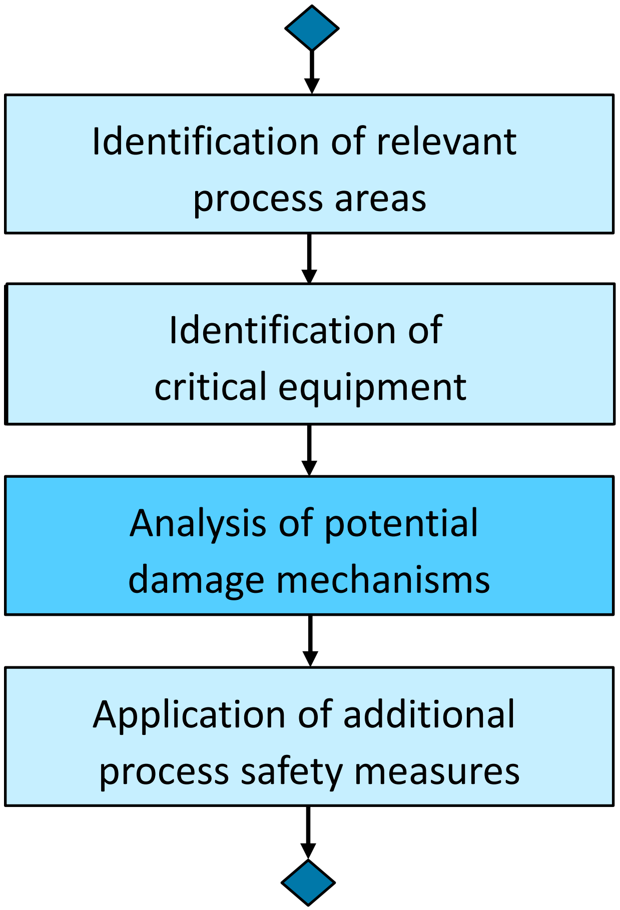


- Process areas to be assessed

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

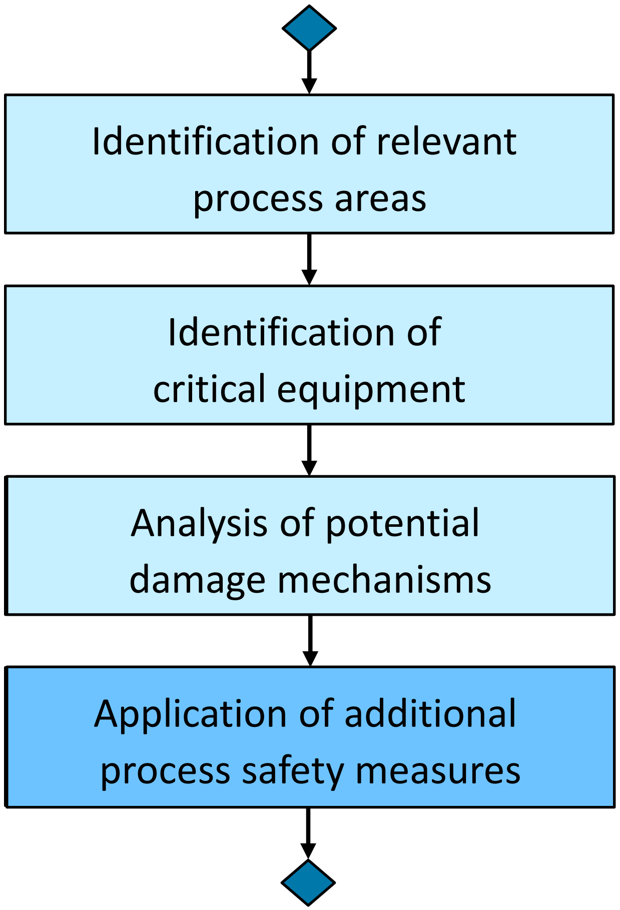


- Process areas to be assessed
- Critical equipment to be protected

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, ...)

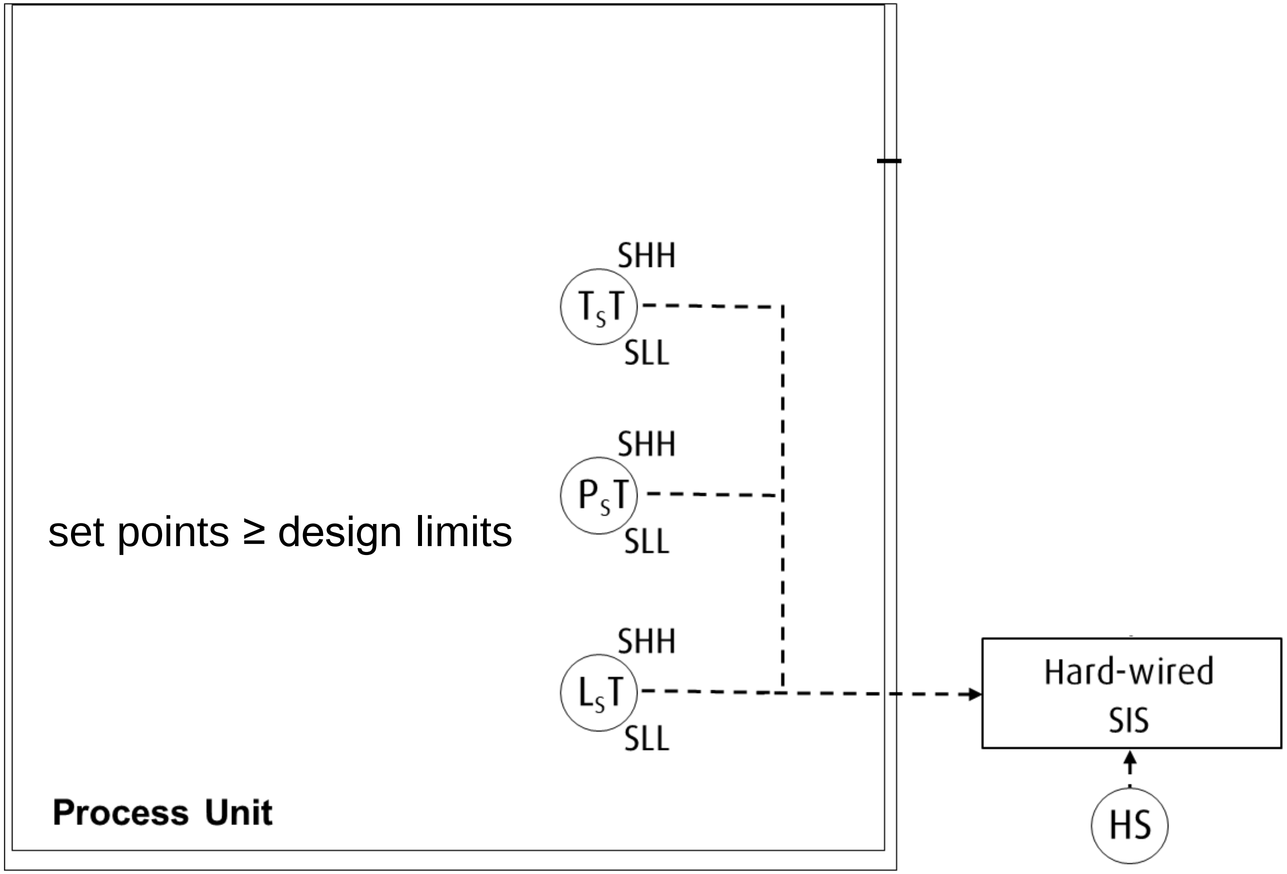
Possible Approach



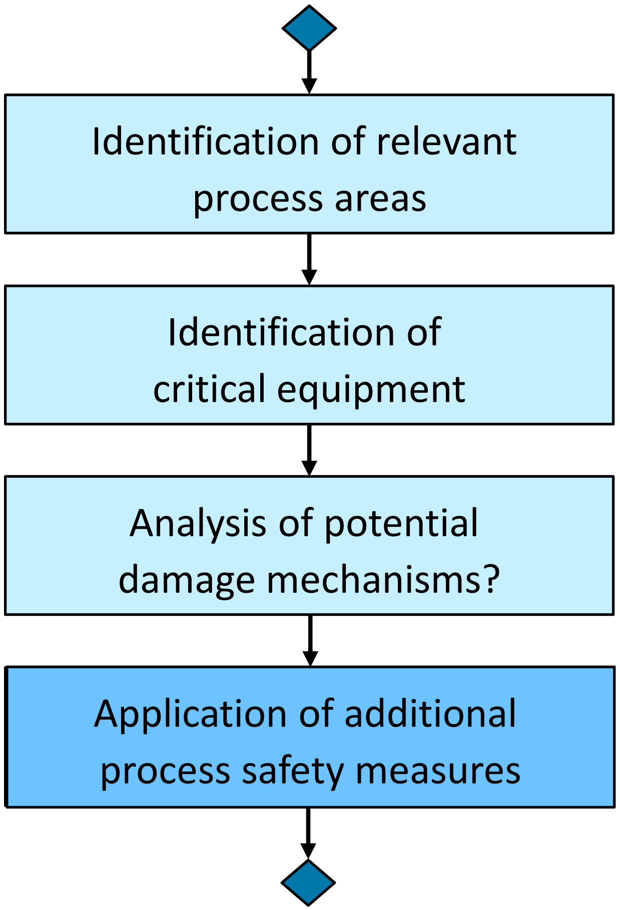
- Process areas to be assessed
- Critical equipment to be protected
- Damage mechanisms to be prevented

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



Possible Approach



- 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?

Estimation – Effort for additional measures

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)

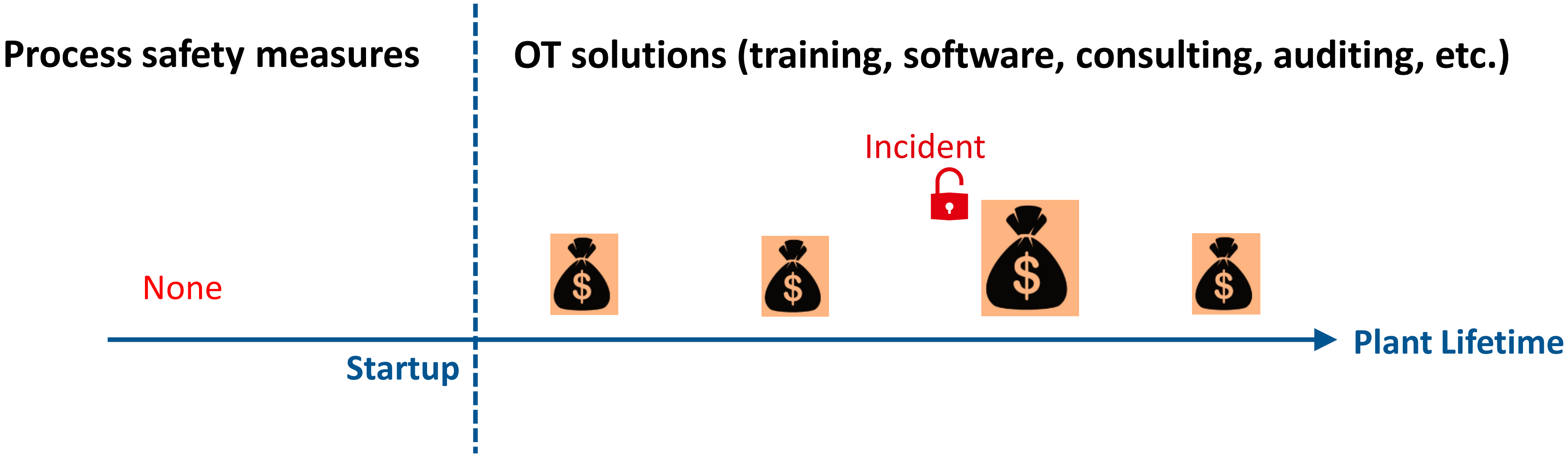
SIS

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



Summary

The aim is **NOT** to

- question the process safety design according to the state of the art
- add extensive additonal 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)
- 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