Challenges & Misconceptions of Functional Safety in Process Industry

Dr. Thorsten Gantevoort

Head of Certification Body TÜV Rheinland A-FS

Safety Case Symposium 2019
Singapore
Mar 26 - 27, 2019

Agenda

Selected challenges in

- Specification of Safety Functions (SRS)
- Design and Engineering of SIS
- Functional Safety Management

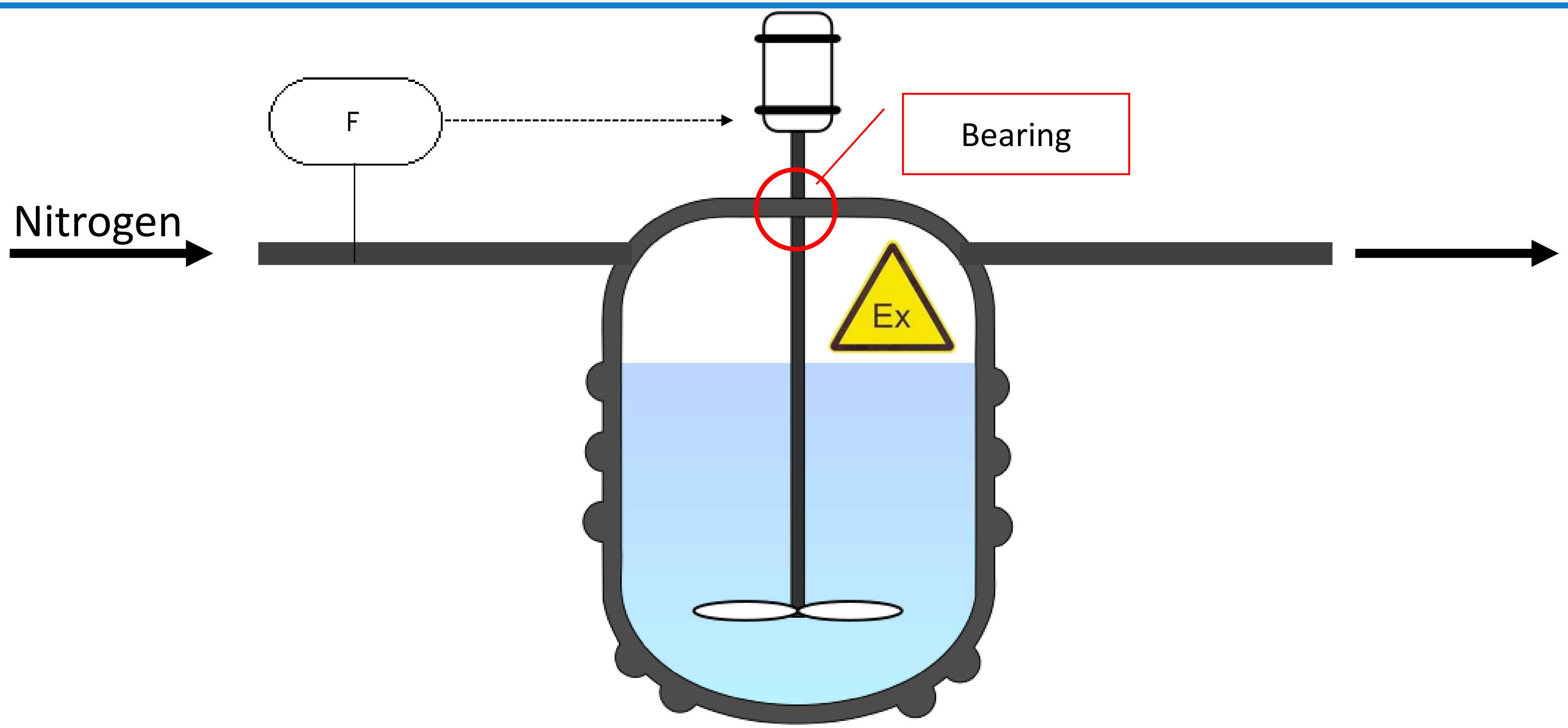
Introduction

- During more than 15 years of personal experience plus experience of our whole team we encountered many challenges during our assessment activities
- Many challenges were caused by lack of understanding Functional Safety (requirements)
- Ed. 2 od IEC 61511 provides more clarity and hopefully reduces misinterpretations
- IEC 61511-4 (draft) raises awareness for the most common misconceptions and misinterpretations

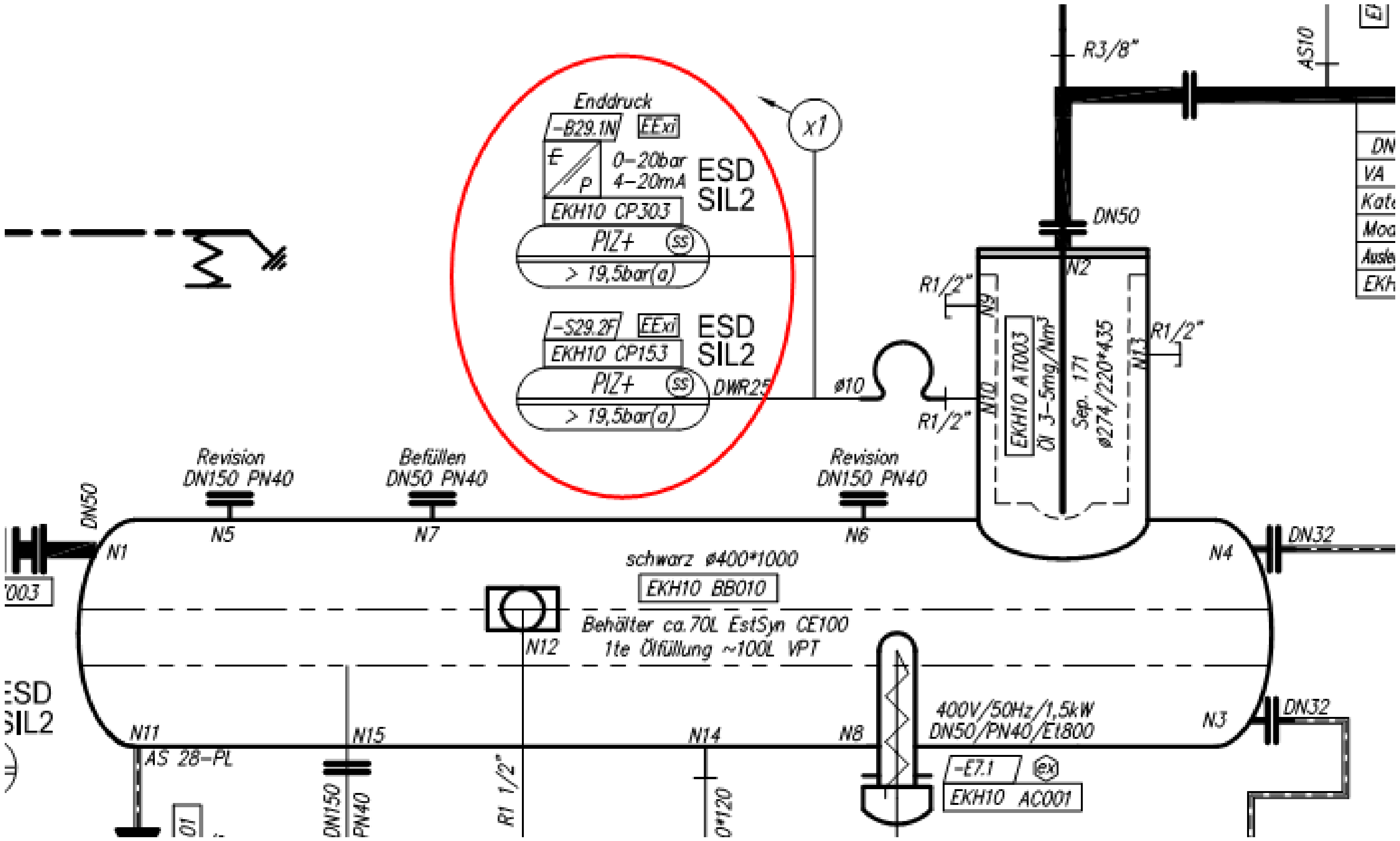
Safety Requirements Specification - SRS

- Every SIF needs a clear and traceable requirement specification as a basis for the development of the SIS.
- SRS defines:
  - Performance requirements (incl. bypass, testing, device criteria, response time …)
  - Functionality and reliability / safety integrity
- SRS shall be:
  - Clear, precise, unambiguous, traceable and complete
  - Used for transposing requirements into SIS HW design and application program development
  - Used for SIS validation purposes, the preparation of procedures for SIS operation, maintenance, proof testing and operator response on SIF failure etc.

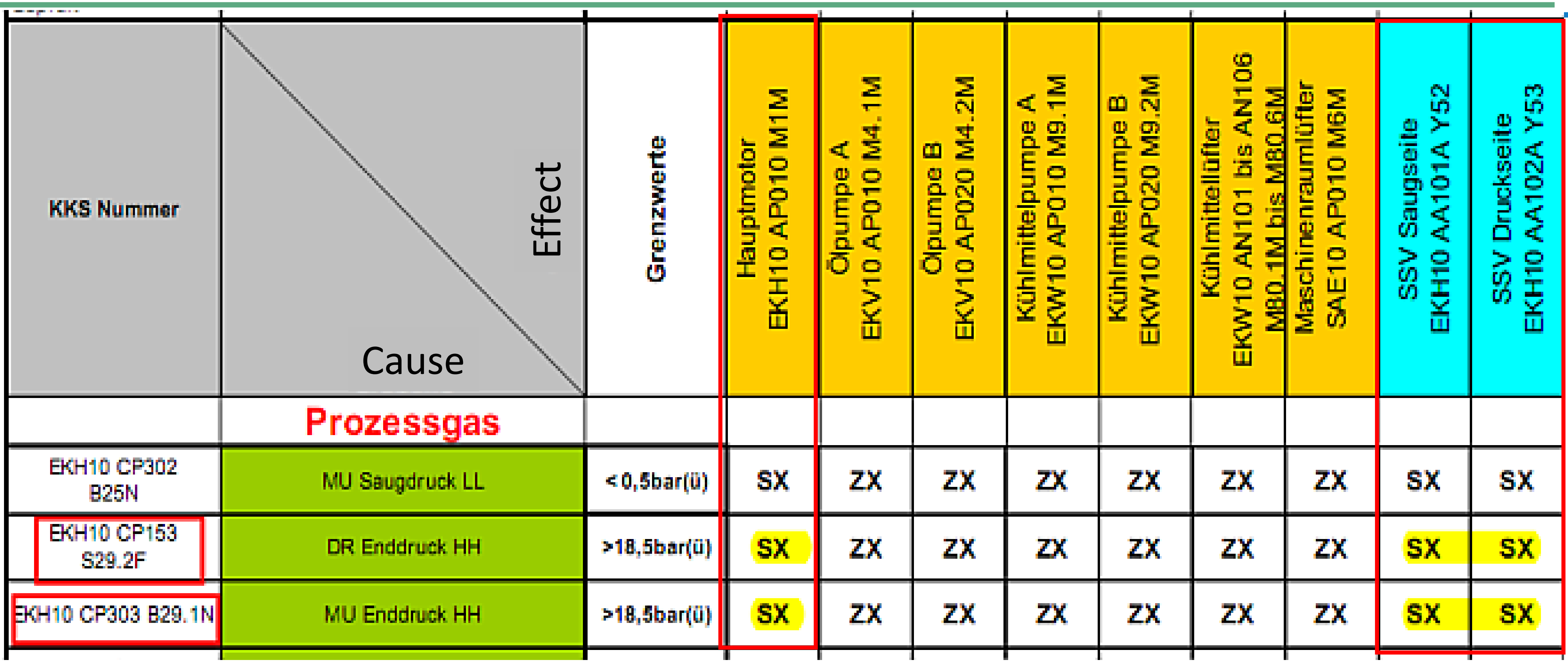
SRS Challenge – Example Explosion Protection



SRS Challenge – Example Pressure Tank

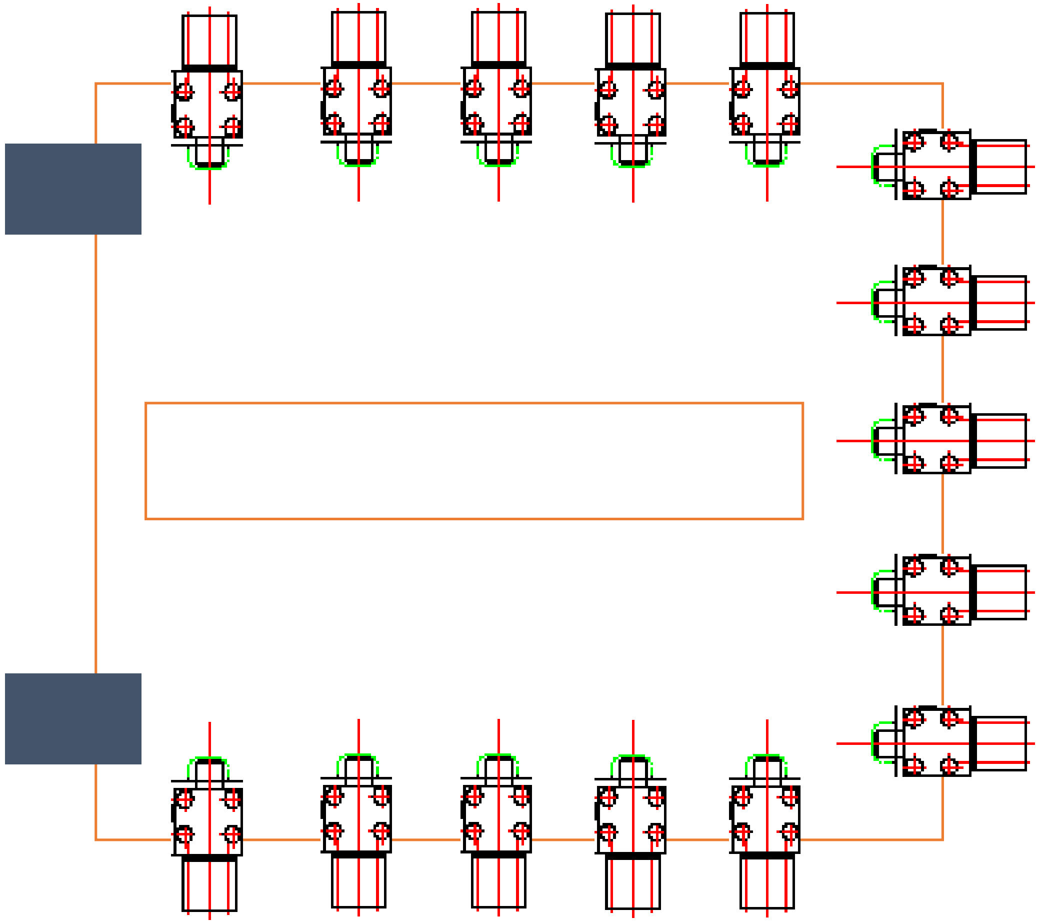


SRS Challenge – Example Pressure Tank



KKS Nummer	Effect Cause	Grenzwerte	Hauptmotor EKH10 AP010 M1M	Ölpumpe A EKV10 AP010 M4.1M	Ölpumpe B EKV10 AP020 M4.2M	Kühlmittelpumpe A EKW10 AP010 M9.1M	Kühlmittelpumpe B EKW10 AP020 M9.2M	Kühlmittellüfter EKW10 AN101 bis AN106 M80.1M bis M80.6M	Maschinenraumlüfter SAE10 AP010 M6M	SSV Saugseite EKH10 AA101A Y52	SSV Druckseite EKH10 AA102A Y53
	Prozessgas										
EKH10 CP302 B25N	MU Saugdruck LL	< 0,5bar(ü)	SX	ZX	ZX	ZX	ZX	ZX	ZX	SX	SX
EKH10 CP153 S29.2F	DR Enddruck HH	>18,5bar(ü)	SX	ZX	ZX	ZX	ZX	ZX	ZX	SX	SX
EKH10 CP303 B29.1N	MU Enddruck HH	>18,5bar(ü)	SX	ZX	ZX	ZX	ZX	ZX	ZX	SX	SX

SRS Challenge – Example Safe Locking of Door



Design and Engineering

- Designing SIS shall address controlling effects of random hardware failures and avoiding / controlling systematic failures:
  - Appropriate Device Selection (prior use or in acc. with IEC 61508)
  - Ensure min. redundancy (HFT), either in acc. with IEC 61511 or IEC 61508
  - Design architecture and application program acc. SRS, do V&V (see also next topic)
  - Ensure independence between SIS and BPCS (HW & AP) so that the overall risk reduction performance is achieved

Design and Engineering

Challenges

- Focus on SIL calculation leads to insufficient attention of systematic aspects, like using prior use devices of similar operating environment
- Incorrect use of reliability data from safety manuals, data sheets leads to too optimistic results
- Incorrect use of devices (i.e. use of ETT devices instead of DTT)
- Incorrect use of HFT table 6 (only appropriate, if clauses 11.5-11.9 are fulfilled, like confirming that the device is suitable for the environment)

ETT: Energize To Trip
DTT: De-Energize To Trip

Application Program (AP) Development

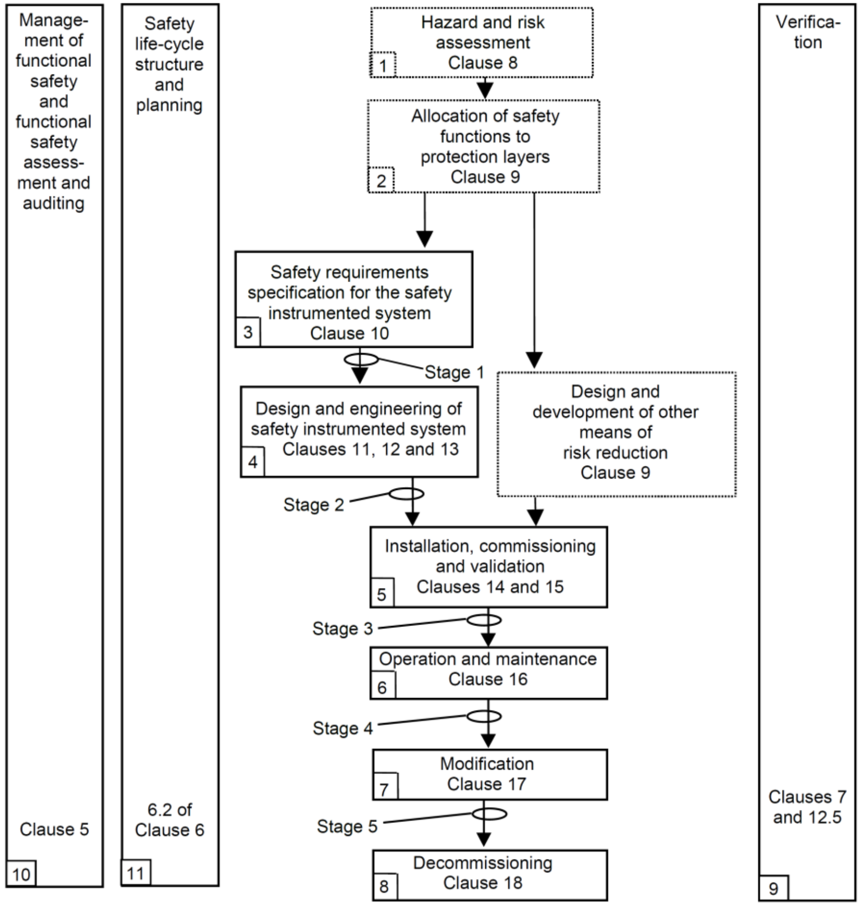
- Application Programming relates to systematic aspects, no random hardware failures. Measures for fault avoidance shall be applied.
- AP normally has no “real” redundancy, i.e. single failures can lead to dangerous loss of the SIF
- Challenges:
  - No different rigour requirements for SIL 1 as for SIL 3 (compared to IEC 61508), target always SIL 3 compliant AP
  - Verification of a SIS is not limited to a check of the hardware or simple function tests (AP / configuration verification is required, which might be much more complex like dynamic vs static behaviour analysis, proof of absence of dangerous variable combinations)

Functional Safety Management

- Management of functional safety addresses systematic failures, mostly caused by humans, that are not quantifiable.
- Requires measures for fault avoidance through processes and procedures.
- Challenges:
  - No different rigour requirements for SIL 1 as for SIL 3 (compared to IEC 61508)
  - Avoidance of “checklist mentality” instead if living processes
  - Covering the whole safety lifecycle
  - Competency Management
  - Applying performance monitoring
  - Covering Existing Systems

Challenge - Covering the whole safety lifecycle

- SIS shall be designed for FSM of the whole safety lifecycle, it shall be managed over time.
- All activities in the safety lifecycle are impacted by upstream and downstream activities.
- The iterative nature of H&RA, SRS development, and SIS design needs to be considered.
- The project disciplines need to be trained such, that necessary interactions will not be overlooked.



Management of functional safety and functional safety assessment and auditing
Clause 5
10

Safety life-cycle structure and planning
6.2 of Clause 6
11

1 Hazard and risk assessment Clause 8

2 Allocation of safety functions to protection layers Clause 9

3 Safety requirements specification for the safety instrumented system Clause 10

Stage 1

4 Design and engineering of safety instrumented system Clauses 11, 12 and 13

Design and development of other means of risk reduction Clause 9

Stage 2

5 Installation, commissioning and validation Clauses 14 and 15

Stage 3

6 Operation and maintenance Clause 16

Stage 4

7 Modification Clause 17

Stage 5

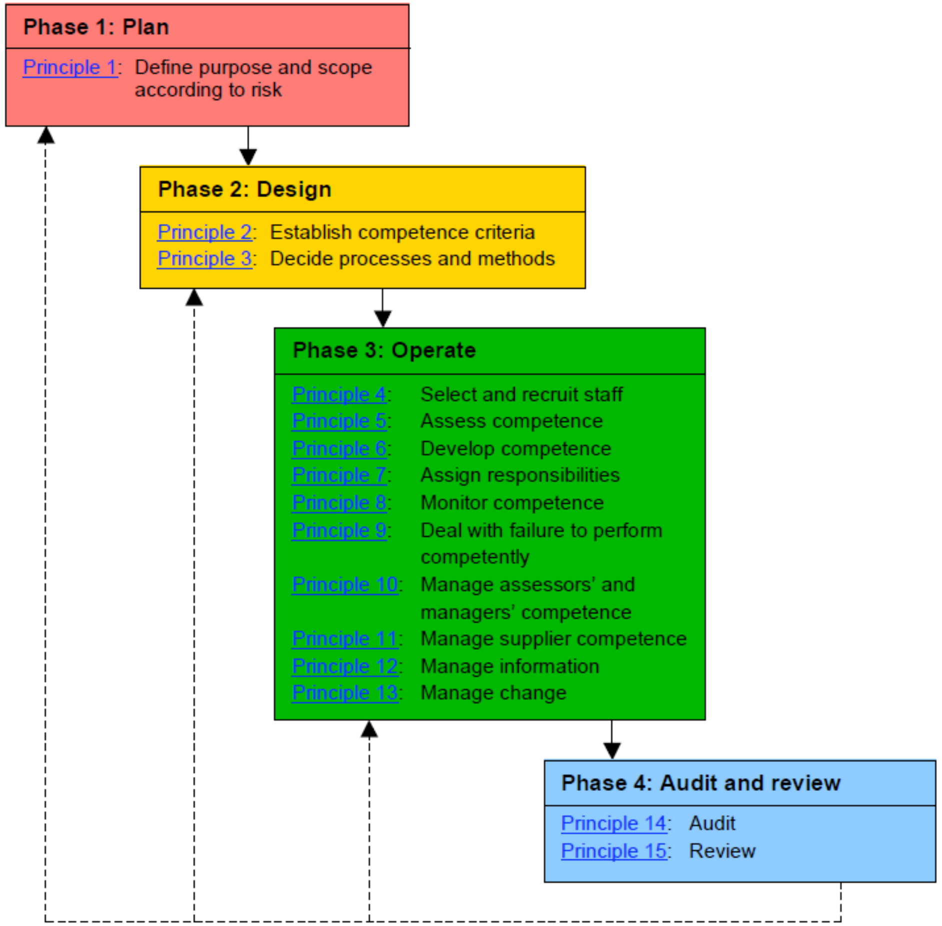
8 Decommissioning Clause 18

Verification
Clauses 7 and 12.5
9

Challenge - Competency Management

- Competency (Management) is a key requirement for Functional Safety.
- Competency is a combination of knowledge, experience, attributes and related to the individual role / task (assessor, auditor, designer etc.)
- Competency will degrade over time without refresher trainings and practical experience → competency is not a lifetime constant.
- Identification of safety critical roles (whole safety lifecycle) and activities need to be done.
- Competency Management if often lacking, especially for external service providers.

Challenge - Competency Management - Example



Phase 1: Plan

Principle 1: Define purpose and scope according to risk

Phase 2: Design

Principle 2: Establish competence criteria

Principle 3: Decide processes and methods

Phase 3: Operate

Principle 4: Select and recruit staff

Principle 5: Assess competence

Principle 6: Develop competence

Principle 7: Assign responsibilities

Principle 8: Monitor competence

Principle 9: Deal with failure to perform competently

Principle 10: Manage assessors' and managers' competence

Principle 11: Manage supplier competence

Principle 12: Manage information

Principle 13: Manage change

Phase 4: Audit and review

Principle 14: Audit

Principle 15: Review

Source: HSE - Managing competence for safety-related systems;
Part 2: Supplementary material
© Crown copyright 2007

Safety Case Symposium 2019
Singapore
Mar 26 - 27, 2019

Challenge - Applying performance monitoring

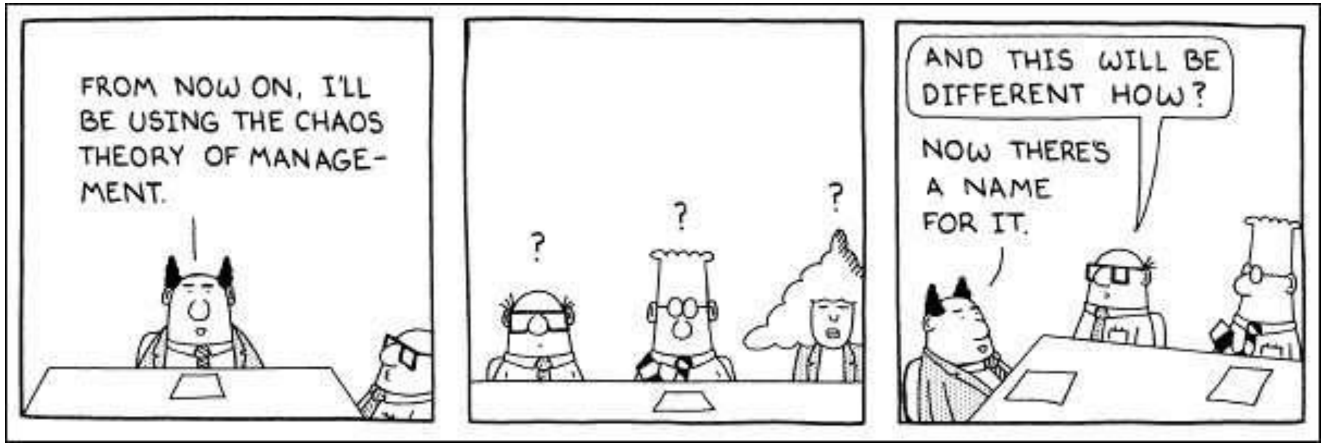
- For SIS design often overly optimistic data, not applicable to operating environment of the SIS, is used.
- Variations in process, operations, maintenance, etc. over time can result in poor system performance and inadequate risk reduction.
- Avoidance / detection measure is to collect performance data on an ongoing basis and to periodically assess for conformance to H&RA and SRS requirements (i.e. periodically perform FSA stage 4)
- Especially at small plant operators no collection of performance data is available

Challenge - Covering Existing Systems

- Existing systems can reduce overall risk reduction / be hazardous as they might not be treated acc. to Functional Safety aspects at the time of putting into operation
- Challenges:
  - Existing systems are part of the current Functional Safety Management System and cannot be treated as “old, nothing needs to be done”.
  - At least a risk assessment and evaluation of risk reduction measures shall be performed for these systems.
  - As part of the FSM, all modifications to existing systems shall be performed acc. to the requirements of the FSM (i.e. clause 17, modification).

Summary

- Experience within TÜV Rheinland fits to the described misinterpretations/misconceptions in IEC 61511-4 (Draft)
- Correct and complete specification of the SIF (SRS) is a key aspect for Functional Safety
- Most challenges lie in correct application of FSM


FROM NOW ON, I'LL BE USING THE CHAOS THEORY OF MANAGEMENT.
?
?
?
AND THIS WILL BE DIFFERENT HOW?
NOW THERE'S A NAME FOR IT.

Challenges & Misconceptions of Functional Safety in Process Industry

Thank you!

Dr. Thorsten Gantevoort

Head of Certification Body TÜV Rheinland A-FS

Safety Case
Symposium 2019
Singapore
Mar 26 - 27, 2019
www.SafetyCaseSymposium.com