# Personnel Interlock systems

Andreas Rathjen
Personnel Interlock
DESY MPS

Hamburg, June 2025

HELMHOLTZ

DESY.

# Personnel Interlock Systems

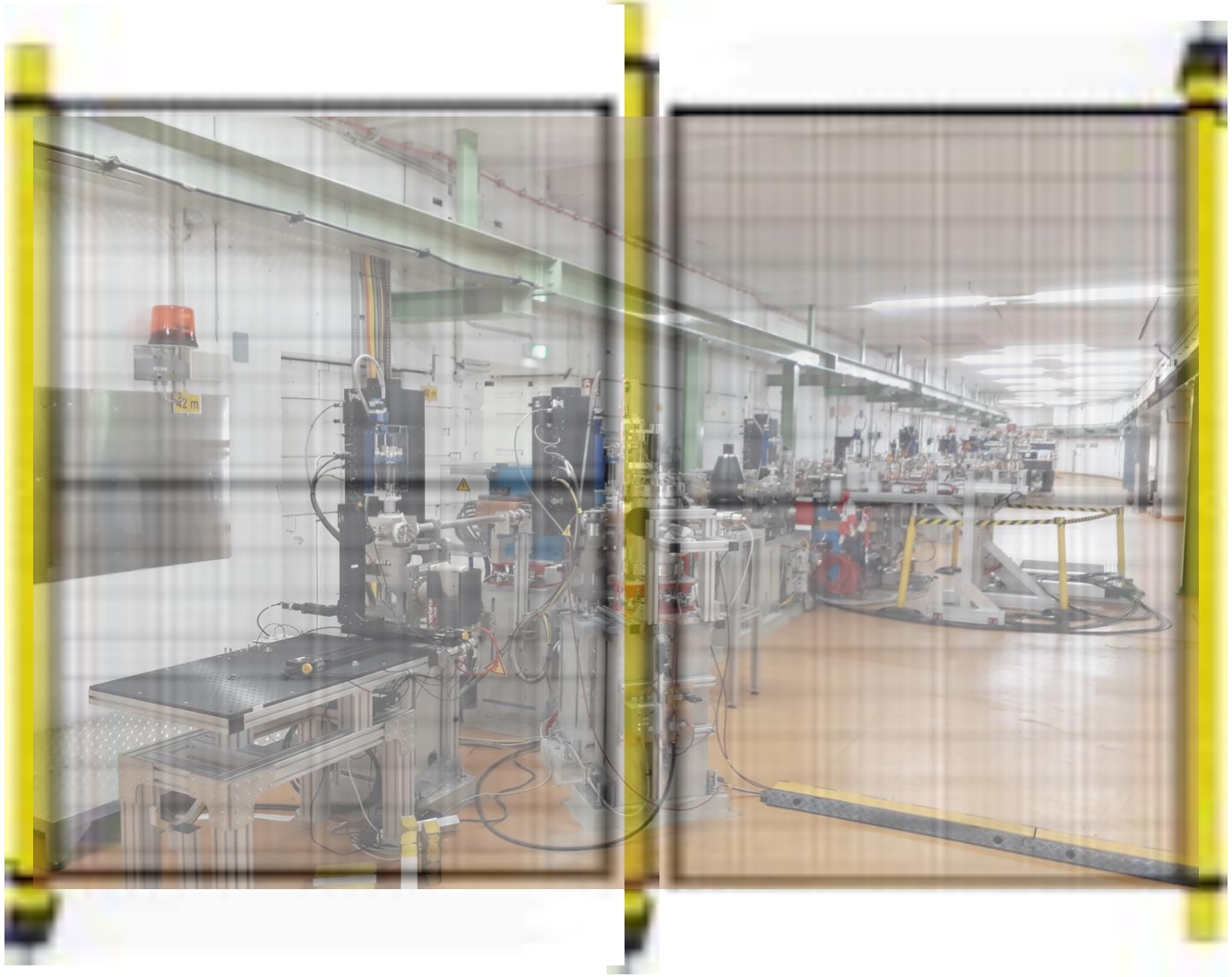
**Implementation of risk assessment requirements, especially for applications with a high safety level (SIL3 safety integrity level)**

## Introduction

- Risk assessment: identification of risks, estimation of the risks
- Hardware design of a suitable Functional Safety
- evaluation of the measure
- Fail-safe Software development
- Hard- and Software Code Review
- commissioning with functional test
- system acceptance
- acceptance of changes

# Risk Assessment

identification of risks

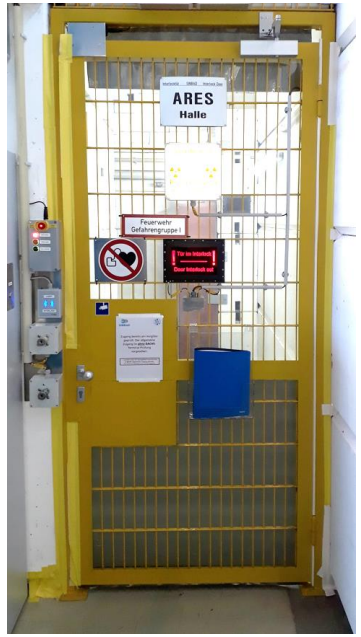


Best practice –

make it inherently safe!

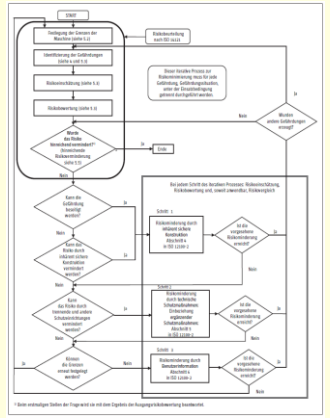
# Risk Assessment

## Standards




If inherent safety is not possible, the design of functional safety and an assessment of the residual risk is mandatory

ISO 12100 Safety of machinery – General principles for design – Risk assessment and risk reduction



Process of risk reduction

ISO 13849 Safety of machinery – Safety related parts of control systems

Performance Level a,b,c,d,e

PL

IEC/EN 62061 ”Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems”

Safety Integrity Level 1,2,3

SIL

application of harmonized standards can ensure compliance with legal requirements

# Risk Assessment

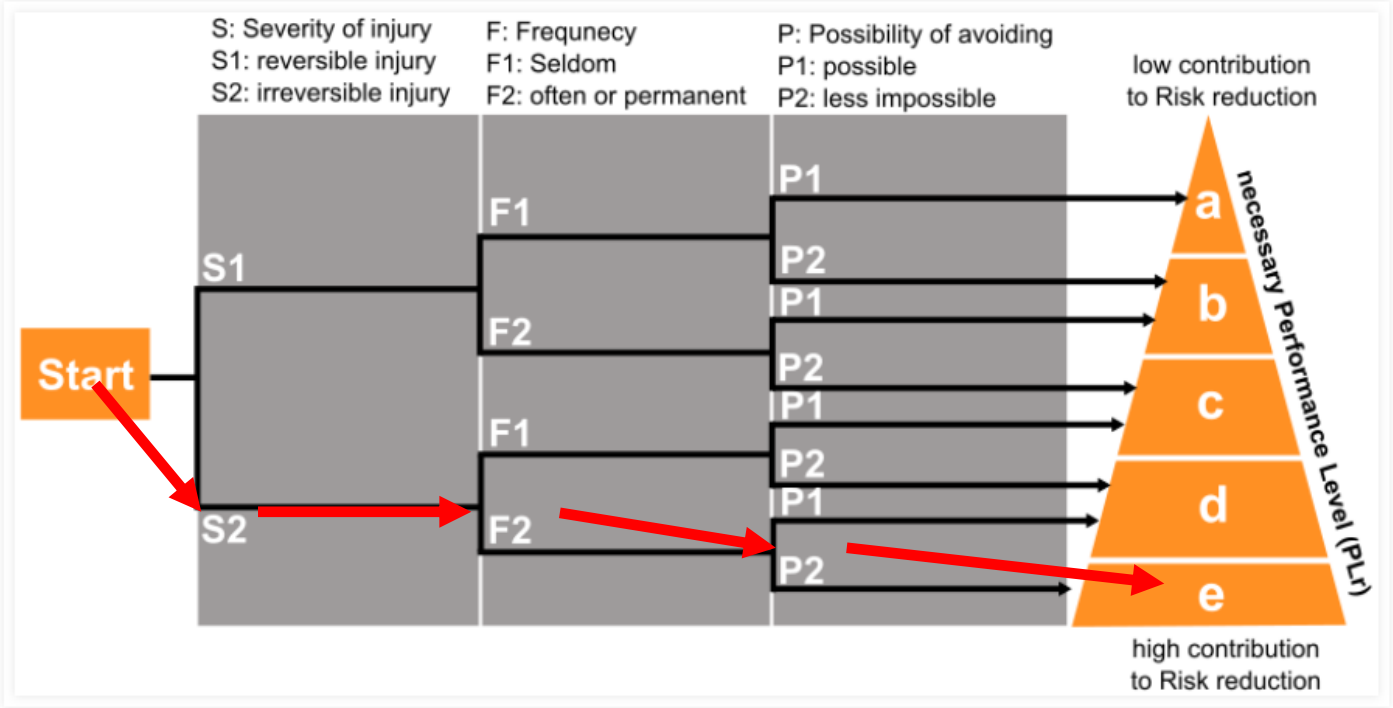
Relation between Performance Level and Safety Integrity Level

| ISO 13849 | Probability of a dangerous Failure per Hour (PFHd) | IEC/EN 62061 |
|---|---|---|
| PL | | SIL |
| a | ≥ $10^{-5}$ bis < $10^{-4}$ | - |
| b | ≥ 3 x $10^{-6}$ bis < $10^{-5}$ | 1 |
| c | ≥ $10^{-6}$ bis < 3 x $10^{-6}$ | 1 |
| d | ≥ $10^{-7}$ bis < $10^{-6}$ | 2 |
| e | ≥ $10^{-8}$ bis < $10^{-7}$ | 3 |

# Risk Assessment

Estimation of the risks

## Risk Graph

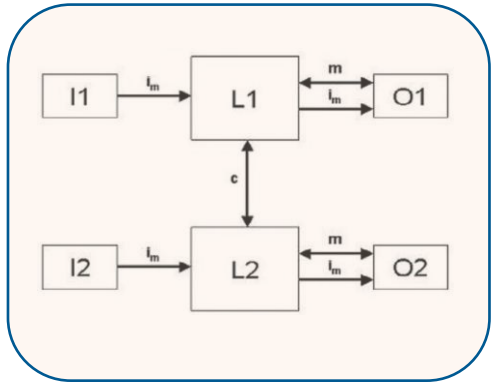



Standard ISO 13849 Safety of machinery – Safety related parts of control systems

# Design of a suitable Functional Safety

## two channel safety architecture

Example for Performance Level e – Solution in accordance with standard ISO13849




crosscheck and diagnostic – architecture: safety category 4

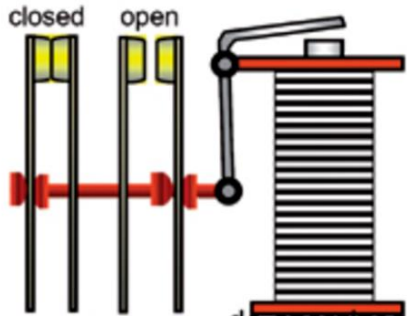
Failsafe PLC with input/output - interface

Door safety switch

Power contactor

Diagnostic

with EDM-
External Device Monitoring
(force guided contacts)



# Design of a suitable Functional Safety

## Function test for detecting fault accumulations and undetected faults

New requirement in the standard: Diagnostic coverage interval at least monthly for PLe

In a redundant system, an accumulation of faults over time could lead to a loss of the safety function.

To avoid undetected faults, safety circuits with non-electronic technology must be triggered regularly.

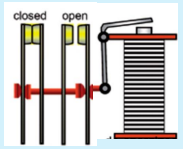
If a functional test is required to detect a possible accumulation of faults or an undetected fault before the next request, it must be performed within the following test intervals:

At least monthly for PLe (SIL3)
At least every 12 months for PLd (SIL2)

# Design of a suitable Functional Safety

→ Monthly testing is often not practicable
(e.g. open a interlock door between the regular maintenance)

## non-electronic devices





- Power contactors
- Mechanical switches
- Safety relay
- Key switch

## Example key exchange system (DOLD)

## Quote from the manual: Siemens-SIRIUS 3SK1 Safety Relay

**WARNING**

**3SK1..1 and 3SK1..3 safety relays (devices with contacting outputs):**

In continuous operation, the key safety values apply where the function test interval (state change of the outputs) for SIL2 ≤ 1 year and for SIL3 ≤ 1 month.

**Safety Related Data**

| Data suitable for the PFHd summation method according to EN ISO13849-1: 2016 | | | | |
|---|---|---|---|---|
| Category | 2 | 3 | 3 | 4 |
| PL | d | d | e | e |
| $PFH_D$ | 2.12199E-09 | 1.36918E-09 | 1.08914E-09 | 1.50183E-10 |
| Diagnostics Coverage ratio DC | 60 % | 60 % | 90 % | 99 % |
| Test interval | 1 / year | 1 / year | 1 / month | 1 / month |

# Design of a suitable Functional Safety

## OSSD - „Output Switching Signal Device

This electronical switch detect short-circuits and cross-circuits up to PLe in accordance with EN ISO 13849

Faults also detected in the actuated state via electronic diagnostics


**Switch with a “high” diagnostic coverage (DC)**
**This device avoid a monthly testing by rare safety requests in case of a PLe application**

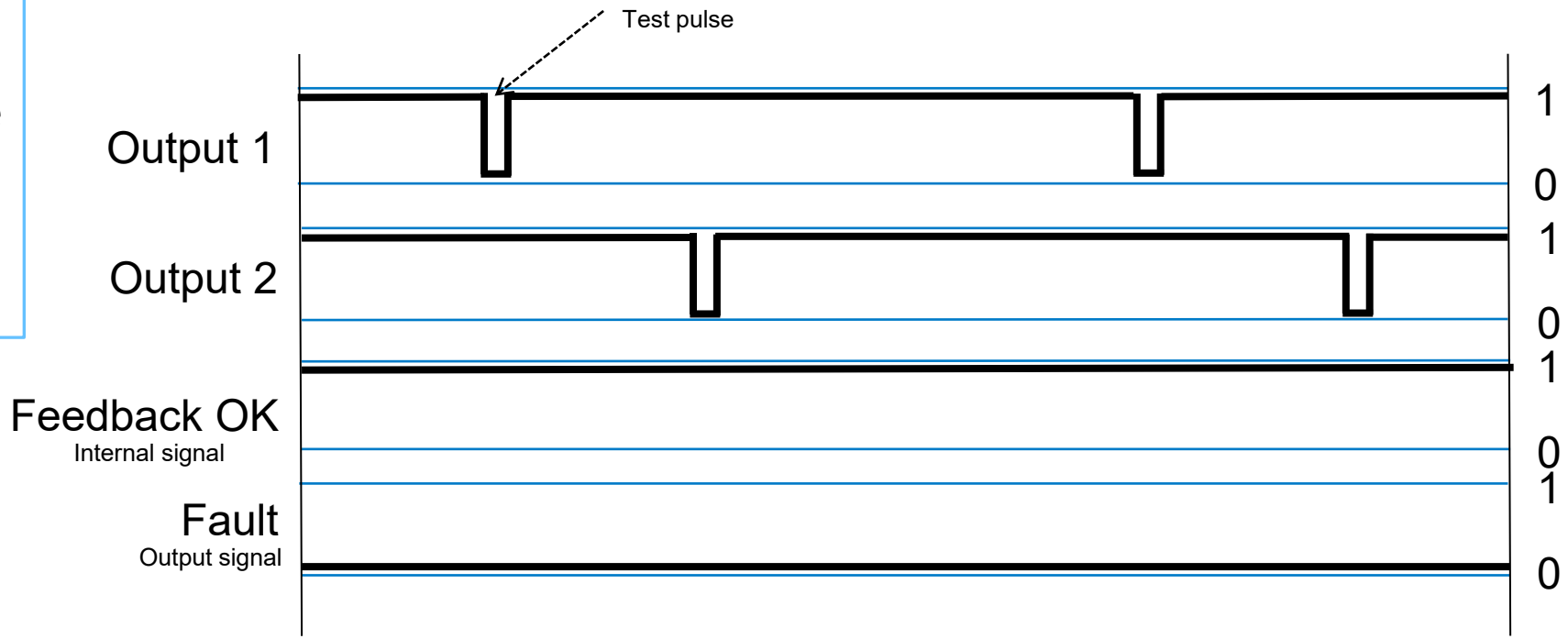
## Classical safety switch

An electro-mechanical switch fulfills at most PLd according to the standard ISO13849

**OSSD - „Output Switching Signal Device**

Two OSSD outputs are switched off with a time delay. During the pause time of the output, a built-in input is activated and read back.

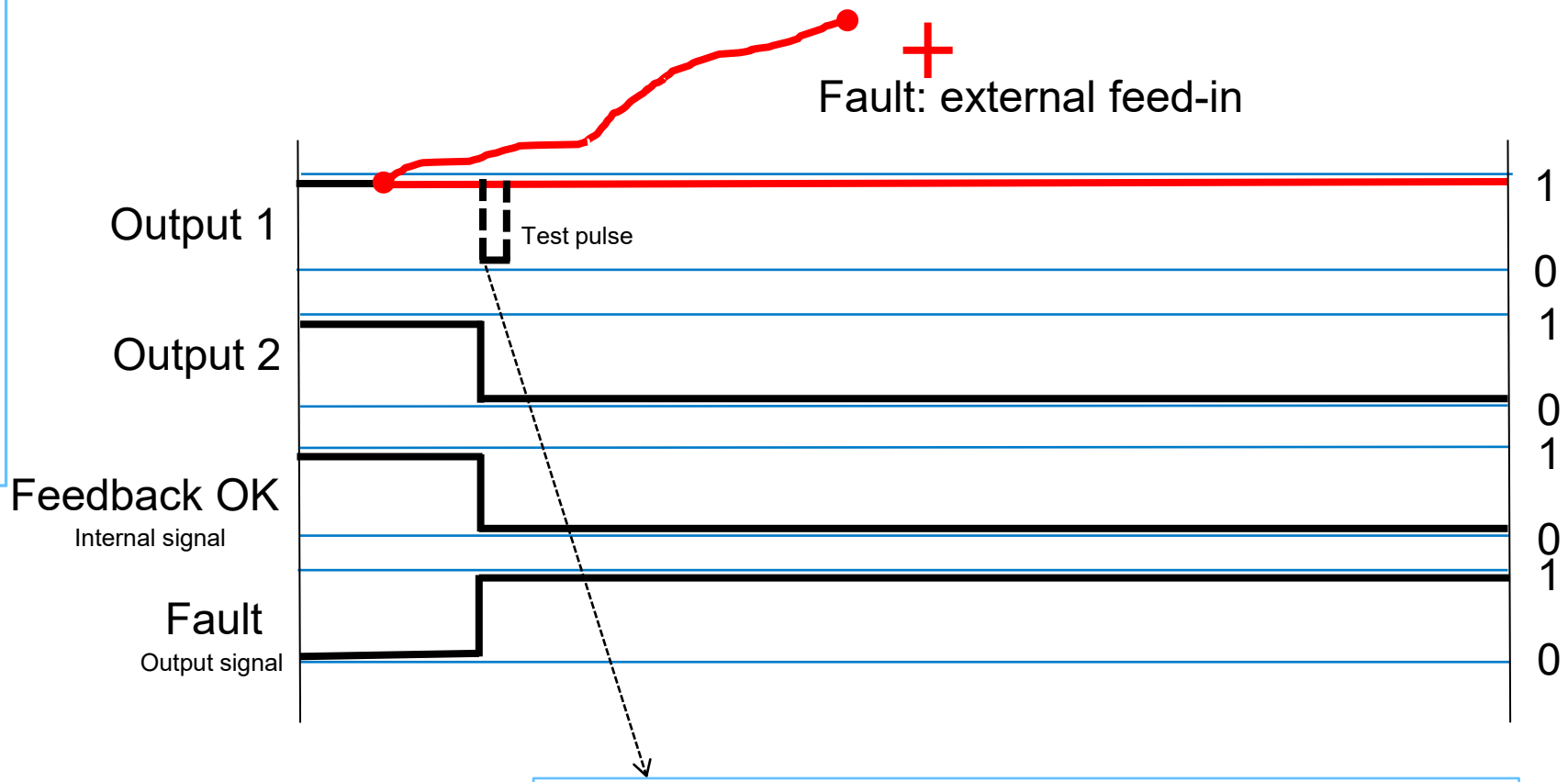
## Example for: OSSD - „Output Switching Signal Device



**OSSD - „Output Switching Signal Device**

If 24 V is present at the input after the output is switched off, an error is detected by the sensor and the OSSD outputs switch off safely.

**Example for: OSSD - „Output Switching Signal Device**




correct feedback-signal is missing:
- sensor switches both outputs immediately
- sensor generates error message

# Evaluation of the measure

The PFHd (Probability of a dangerous failure by hour) value can be calculated manually or with a software tool (e.g. Sistema).

Therefore is the technical data of the safety components necessary.

The PFHd must be compared with the requirement of the risk assessment.

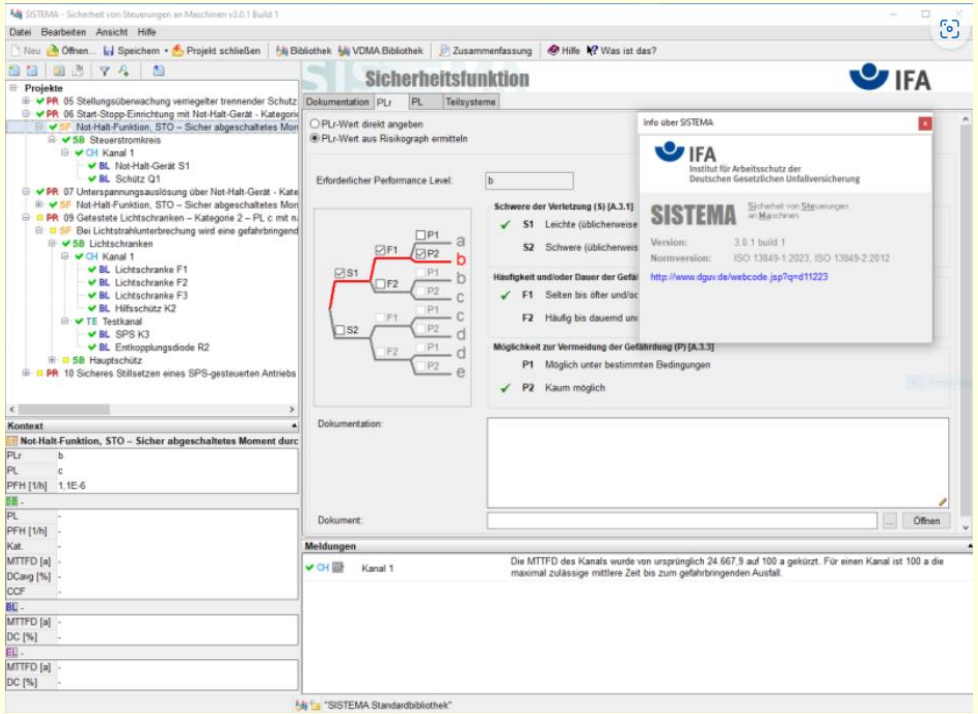
If the required Performance Level (PLr) is not reached, the design must be improved.

Evaluation Tool SISTEMA
Data input:

- technical data (B10d-, MTTFd-,...)
- safety architecture
- diagnostic coverage
- …

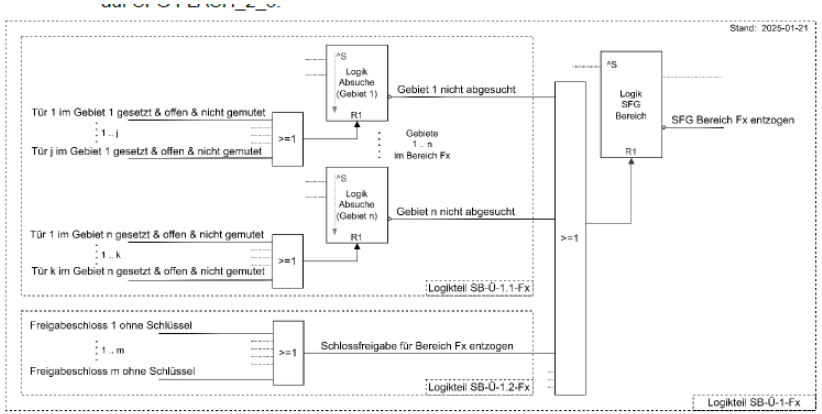
IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

SISTEMA Sicherheit von Steuerungen an Maschinen



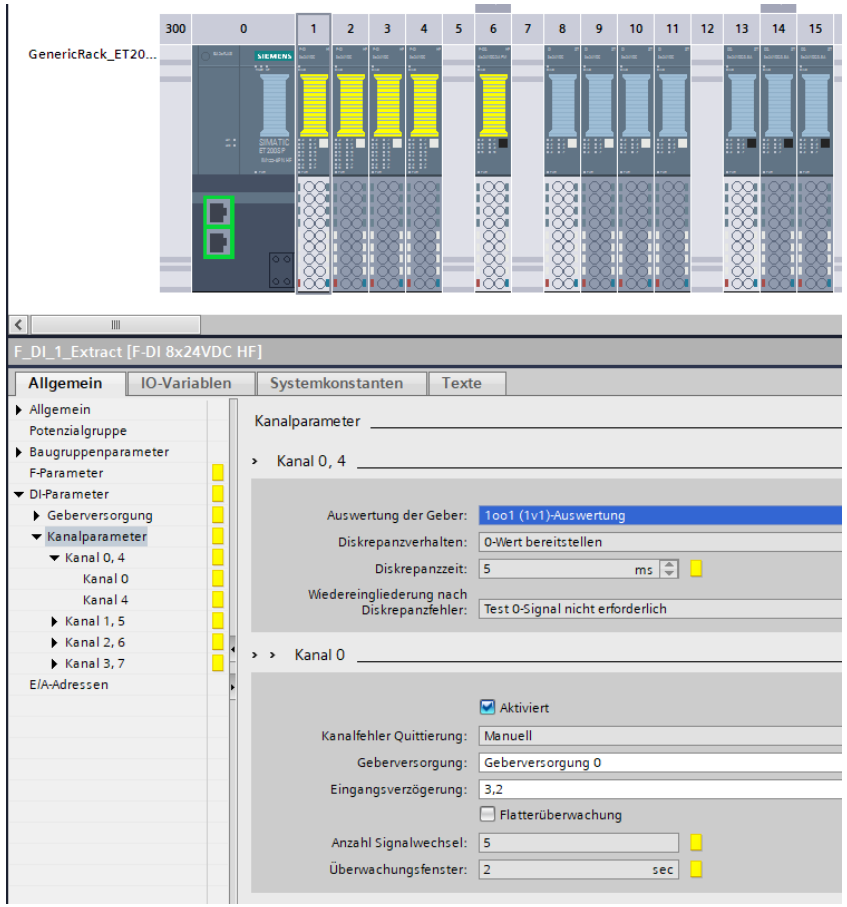

| Modulatorfreigabe | |
|---|---|
| PLr | d |
| PL | e |
| PFHD [1/h] | 1,6E-8 |

# Fail-safe Software development

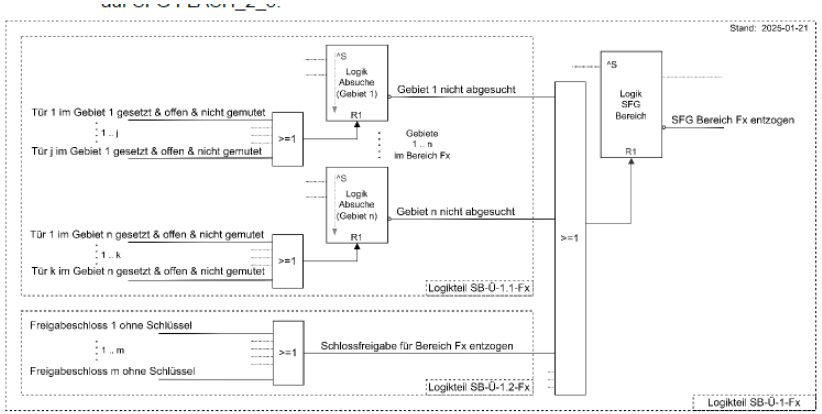



The PLC hardware must be created in accordance with the safety specification

## PLC Hardware

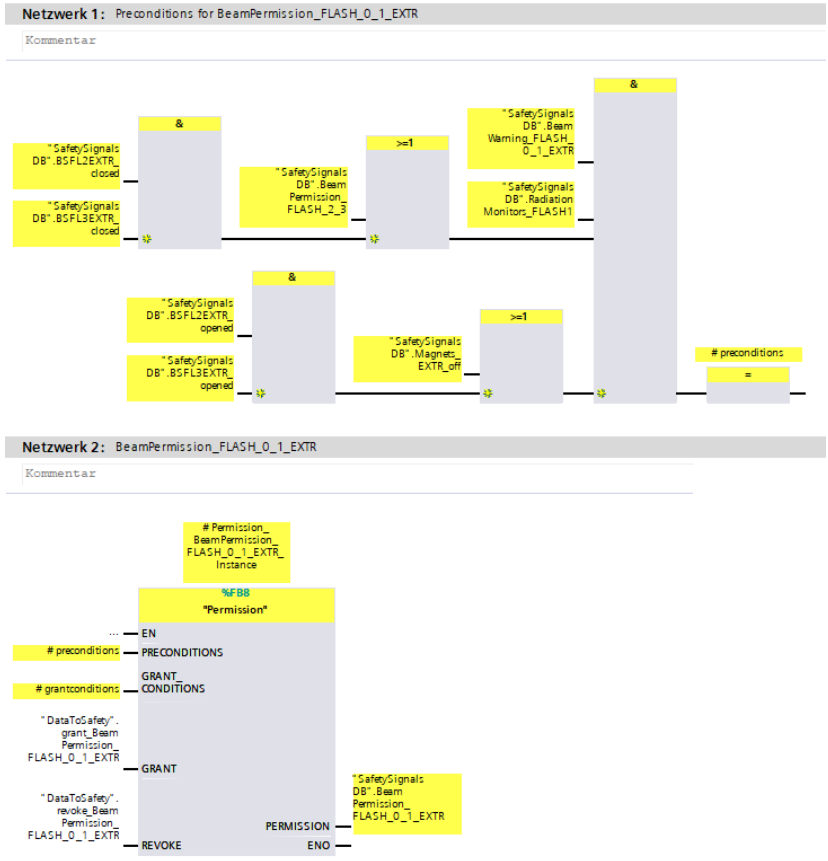


# Fail-safe Software development



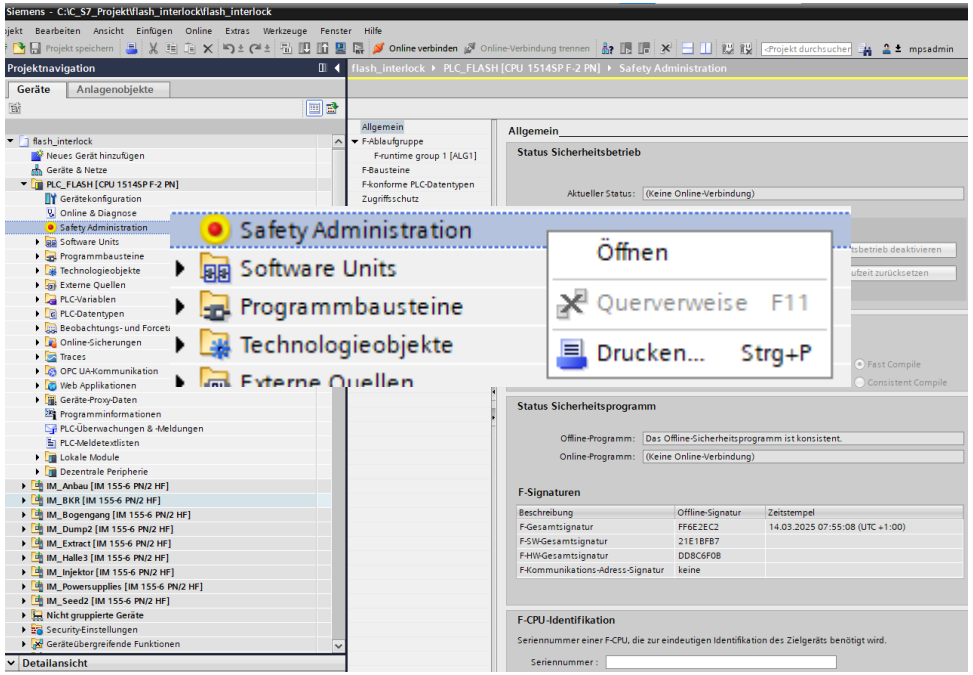

The PLC software must be created in accordance with the safety specification

## PLC Software



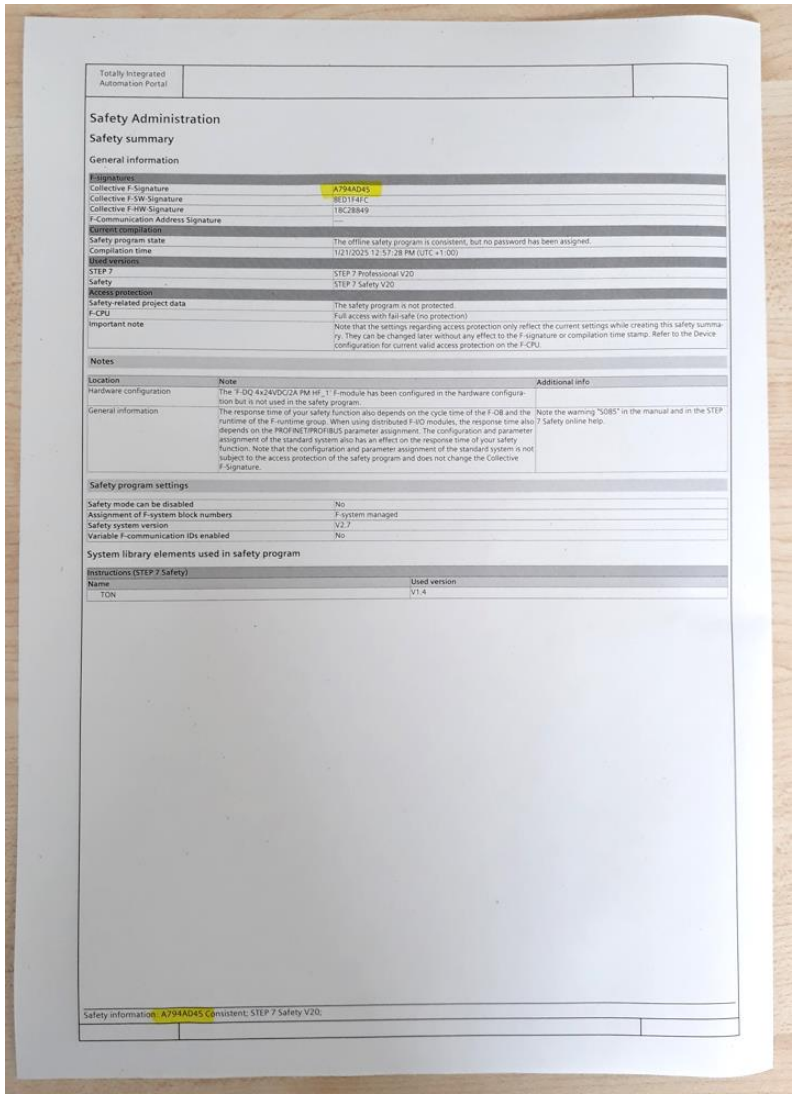
# Software Documentation

## Siemens - programming tool TIA



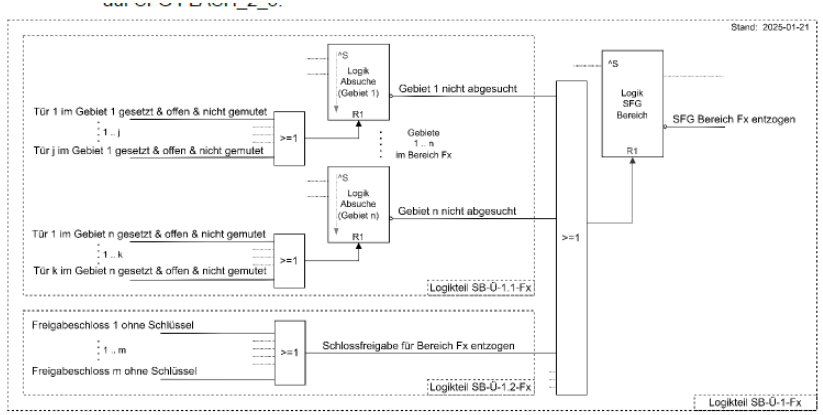

Print a safety summary by using the programming tool

## Paper print



# Hard- and Software Code-Review

## Verification

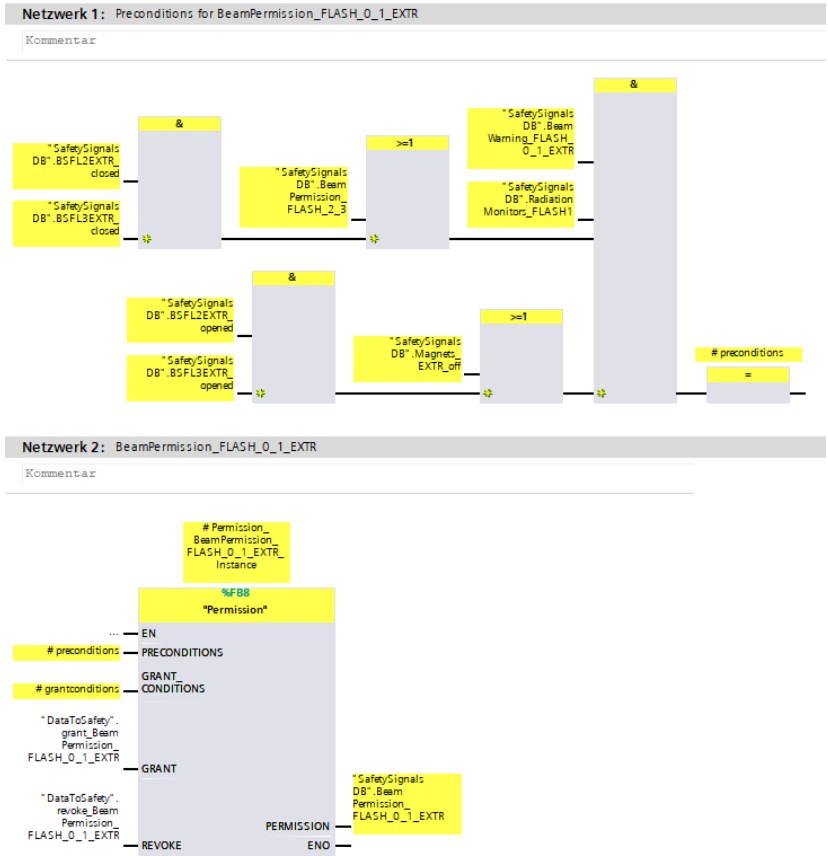



Testing the Safety-Specification against the PLC-Software

<u>Code review</u>

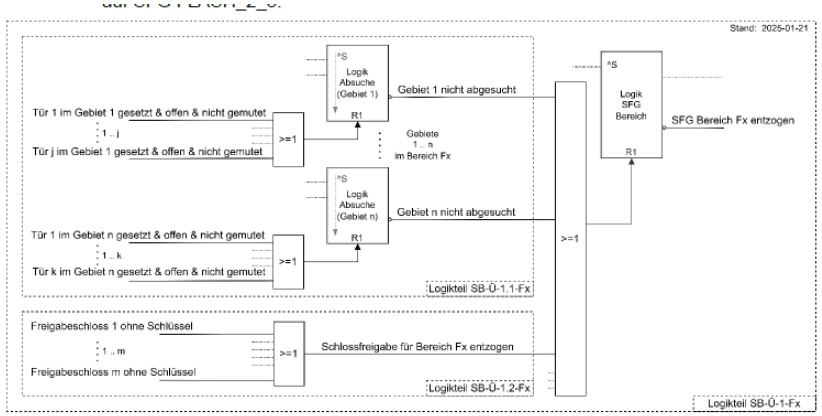
Key questions to clarify:
Is the function complete realized?
Is the logic correct?
Are the software (time-) parameters suitable?

## PLC Software



# Hard- and Software Code-Review

## Verification

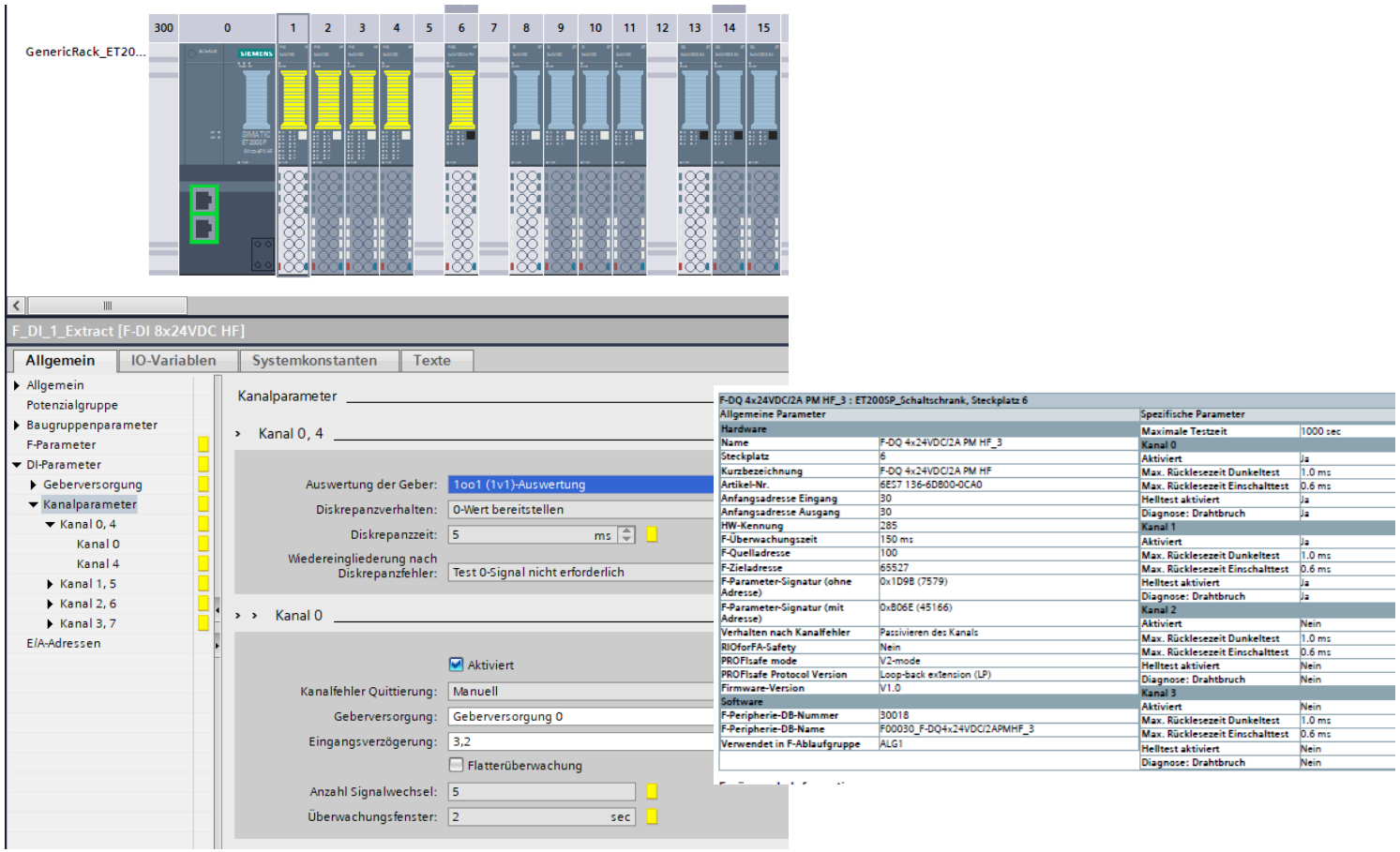



Testing the Safety-Specification against the PLC-Hardware

### Code review

Key questions to clarify:
Is the Hardware correctly designed (electrical data)?
Is the Hardware correctly configured (addresses)?
Are the Hardware parameters suitable (time-,wire-… monitoring)?

## PLC Hardware




F-DQ 4x24VDC/2A PM HF_3 : ET200SP_Schaltschrank, Steckplatz 6

| Allgemeine Parameter | | Spezifische Parameter | |
|---|---|---|---|
| Hardware | | Maximale Testzeit | 1000 sec |
| Name | F-DQ 4x24VDC/2A PM HF_3 | Kanal 0 | |
| Steckplatz | 6 | Aktiviert | Ja |
| Kurzbezeichnung | F-DQ 4x24VDC/2A PM HF | Max. Rücklesezeit Dunkeltest | 1.0 ms |
| Artikel-Nr. | 6ES7 136-6DB00-0CA0 | Max. Rücklesezeit Einschalttest | 0.6 ms |
| Anfangsadresse Eingang | 30 | Helltest aktiviert | Ja |
| Anfangsadresse Ausgang | 30 | Diagnose: Drahtbruch | Ja |
| HW-Kennung | 285 | Kanal 1 | |
| F-Überwachungszeit | 150 ms | Aktiviert | Ja |
| F-Quelladresse | 100 | Max. Rücklesezeit Dunkeltest | 1.0 ms |
| F-Zieladresse | 65527 | Max. Rücklesezeit Einschalttest | 0.6 ms |
| F-Parameter-Signatur (ohne Adresse) | 0x1D9B (7579) | Helltest aktiviert | Ja |
| | | Diagnose: Drahtbruch | Ja |
| F-Parameter-Signatur (mit Adresse) | 0xB06E (45166) | Kanal 2 | |
| | | Aktiviert | Nein |
| Verhalten nach Kanalfehler | Passivieren des Kanals | Max. Rücklesezeit Dunkeltest | 1.0 ms |
| RIOforFA-Safety | Nein | Max. Rücklesezeit Einschalttest | 0.6 ms |
| PROFIsafe mode | V2-mode | Helltest aktiviert | Nein |
| PROFIsafe Protocol Version | Loop-back extension (LP) | Diagnose: Drahtbruch | Nein |
| Firmware-Version | V1.0 | Kanal 3 | |
| Software | | Aktiviert | Nein |
| F-Peripherie-DB-Nummer | 30018 | Max. Rücklesezeit Dunkeltest | 1.0 ms |
| F-Peripherie-DB-Name | F00030_F-DQ4x24VDC/2APMHF_3 | Max. Rücklesezeit Einschalttest | 0.6 ms |
| Verwendet in F-Ablaufgruppe | ALG1 | Helltest aktiviert | Nein |
| | | Diagnose: Drahtbruch | Nein |

# commissioning with functional test

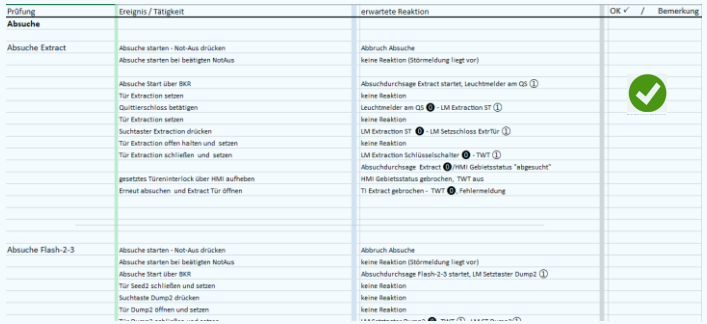
A comprehensive checklist must be created according to the I/O list and the safety specifications.

Check that the documentation of the safety-devices, the hard-and software fits together.
Start commissioning.

- I/O-test - check Input- and Output signals and the related devices
- Check the Hardware parameters and configuration by manual triggered faults (e.g. discrepancy fault)
- Push sensors and switches and check the correct reaction

Use the possibility´s of your development equipment:
Tags of the safety program can be monitored at any time

## Checklist



| Prüfung | Ereignis / Tätigkeit | erwartete Reaktion | OK ✓ / Bemerkung |
|---|---|---|---|
| **Absuche** | | | |
| Absuche Extract | Absuche starten - Not-Aus drücken | Abbruch Absuche | |
| | Absuche starten bei betätigten NotAus | keine Reaktion (Störmeldung liegt vor) | |
| | Absuche Start über BKR | Absuchdurchsage Extract startet, Leuchtmelder am QS ① | |
| | Tür Extraction setzen | keine Reaktion | |
| | Quittierschloss betätigen | Leuchtmelder am QS ❶ - LM Extraction ST ① | |
| | Tür Extraction setzen | keine Reaktion | |
| | Suchtaster Extraction drücken | LM Extraction ST ❶ - LM Setzschloss Extr'tür ① | |
| | Tür Extraction offen halten und setzen | keine Reaktion | |
| | Tür Extraction schließen und setzen | LM Extraction Schlüsselschalter ❶ - TWT ① | |
| | | Absuchdurchsage Extract ❶/HMI Gebietsstatus "abgesucht" | |
| | gesetztes Türeninterlock über HMI aufheben | HMI Gebietsstatus gebrochen, TWT aus | |
| | Erneut absuchen und Extract Tür öffnen | TI Extract gebrochen - TWT ❶, Fehlermeldung | |
| Absuche Flash-2-3 | Absuche starten - Not-Aus drücken | Abbruch Absuche | |
| | Absuche starten bei betätigten NotAus | keine Reaktion (Störmeldung liegt vor) | |
| | Absuche Start über BKR | Absuchdurchsage Flash-2-3 startet, LM Setztaster Dump2 ① | |
| | Tür Seed2 schließen und setzen | keine Reaktion | |
| | Suchteste Dump2 drücken | keine Reaktion | |
| | Tür Dump2 öffnen und setzen | keine Reaktion | |

The checklist must be completed without any errors detected, otherwise you have to fix the problem and start again from “the beginning”

# System acceptance

## Independent expert

As a general rule, the acceptance of a Failsafe-System is performed by an independent expert. The independence required of the expert must be defined in the safety plan and depends on the required PL/SIL.

| Degrees of independence IEC61508 | SIL1 (PLc) | SIL2 (PLd) | SIL3 (PLe) |
|---|---|---|---|
| independent person | recommended | recommended | not sufficient |
| independent department | | recommended (new technology) | recommended |
| independent organization | | | recommended (new technology) |

# System acceptance

If all these steps have been carried out, an independent expert must be consulted now at the latest

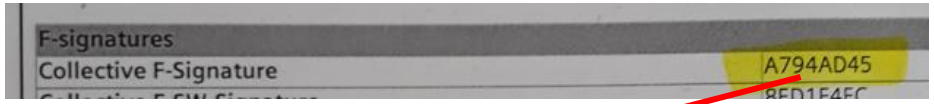
| | |
|---|---|
| Verification & Validation | Completeness and correctness of the safety program including hardware configuration (including testing)<br>Completeness and correctness of the safety equipment |
| Function test | In practice: check the whole functional safety and confirm that it works |
| Documentation | Completeness and correctness of the risk assessment, safety summary, circuit diagram, safety evaluation |
| Version check | Once you have checked all properties of the offline safety program you must ensure that the safety program is identical on the F-CPU on which it is supposed to be run.<br>Check the installation – Are the intended devices installed? |

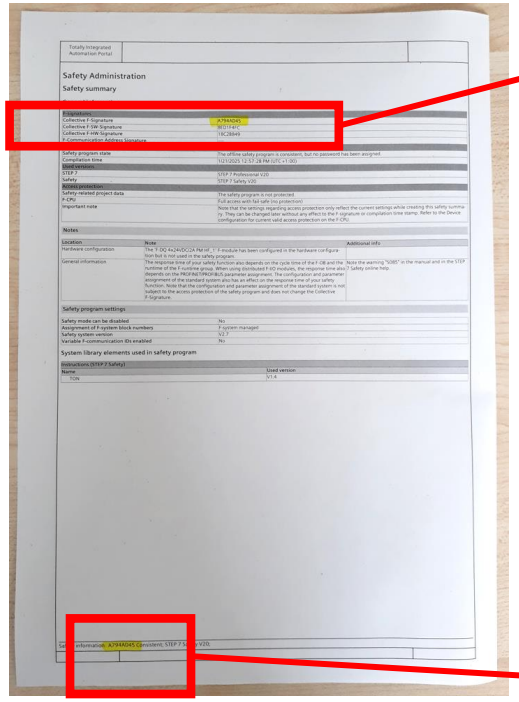
# System acceptance



PLC – display

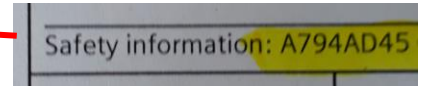
## Version Check




The safety summary signature must be the same which is shown in the PLC!

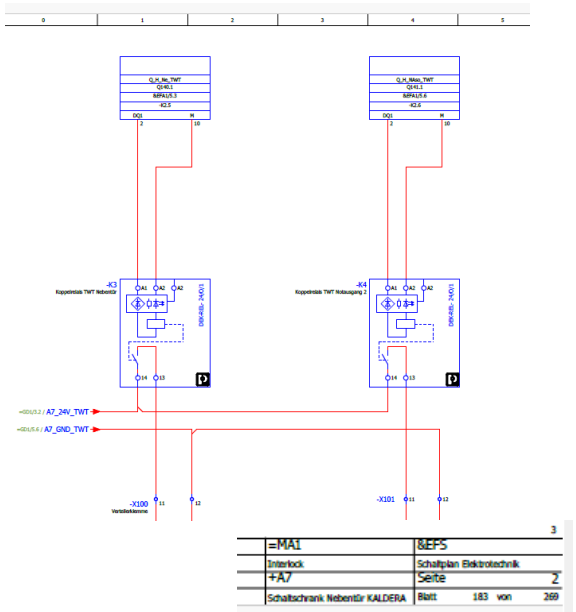
(PLC-display or check the referred safety data block online)




Summary (paper print)

# System acceptance

## Check the actually installed equipment




circuit diagram with equipment list

The documented and evaluated devices must be installed and no other!

| | | | | |
|---|---|---|---|---|
| 6ES7526-2BF00-0AB0 | 1 | ET 200MP, F-DQ 8X24VDC 2A PPM | 6ES7526-2BF00-0AB0 | SIE |
| 6ES7521-1BH10-0AA0 | 3 | S7-1500, DI 16X24VDC BA | 6ES7521-1BH10-0AA0 | SIE |
| 6ES7522-1BH10-0AA0 | 2 | S7-1500, DQ 16X24VDC/0.5A BA | 6ES7522-1BH10-0AA0 | SIE |
| 3SK1111-1AB30 | 3 | SIRIUS SICHERHEITSSCHALTGERAET STD R3+1 | 3SK1111-1AB30 | SIE |

# System acceptance

Validation & Verification 

Documentation 

Function test 

Version check 

---

Functional safety fully audited 

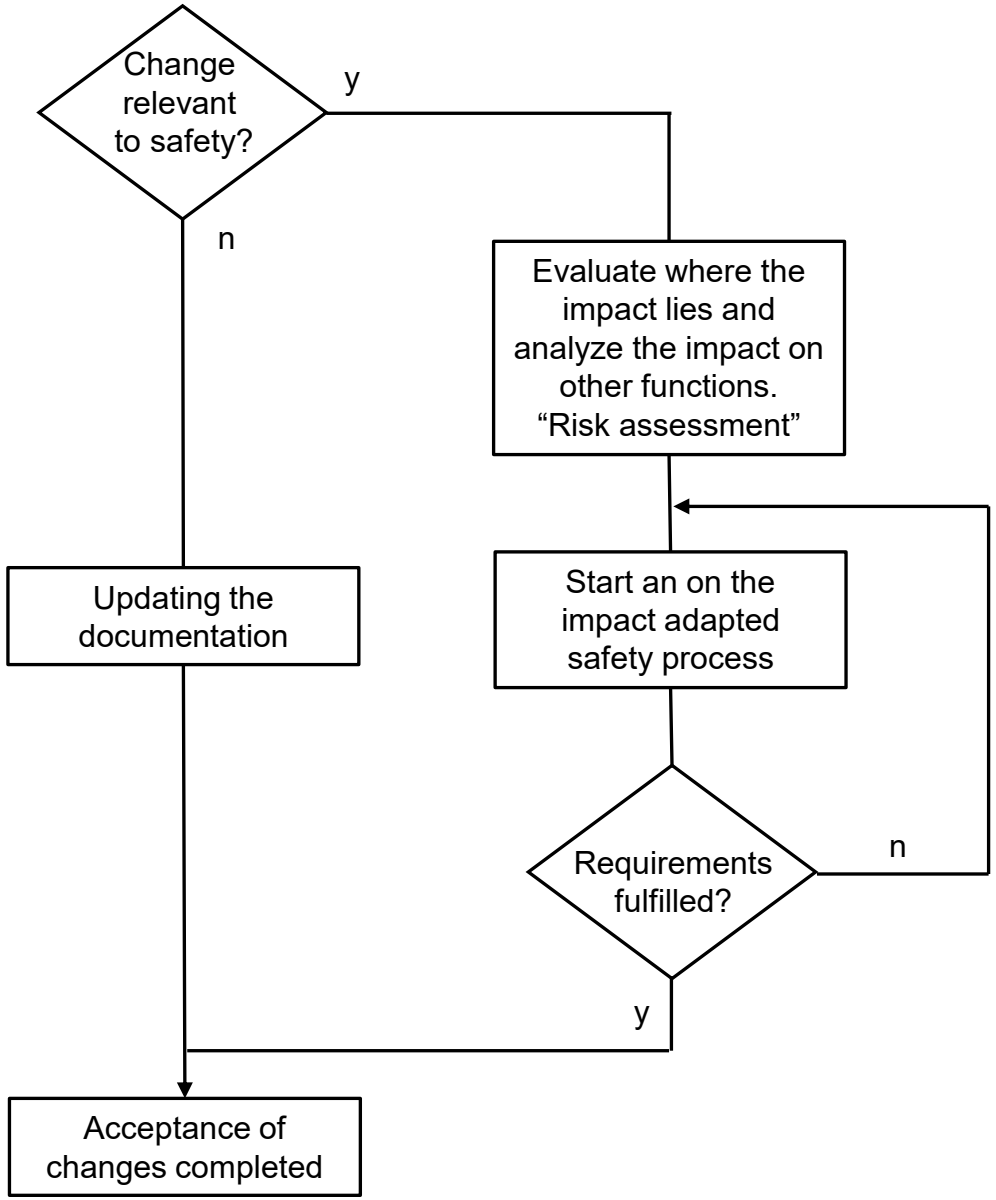
# Acceptance of changes

## Impact analysis

**Acceptance of Changes**

In general, you can adopt the same approach for the acceptance of changes as the initial Acceptance

Check the entire safety-related project data for changes and determine the safety-related project data to be validated and approved as part of an impact analysis.



# Annual testing

Annual testing:

Create a checklist with the following topics and work through it

- Check Software-Signature: must be unchanged
- Check wires and components: must be undamaged, clean and dry
- Check the whole effect chain of all safety functions: Everything works like expected


PLC – display


If the signature remains unchanged, the PLC software and hardware parameters do not need to be checked again.

The logic must be the same, but does everything work as it should?

# Conclusion

- First, clarify whether an independent expert is helpful or even necessary
- Risks must be identified and assessed at the start of the project
- The application of harmonized standards can ensure compliance with legal requirements
- The use of standard solutions and certified components makes development and testing easier
- A suitable design with appropriate devices can reduce the interim manual checks using diagnostics
- A well thought-out implementation of functional safety saves time and money over the entire life cycle

# Thank you for your attention!

**Contact**

Deutsches Elektronen-
Synchrotron DESY

www.desy.de

Andreas Rathjen
Notkestraße 85
D-22607 Hamburg
Dept. DESY-MPS
andreas.rathjen@desy.de
+49 40 8998 2528