

Functional Safety Management

KicMPi-bijeenkomst Safety Integrity Level (SIL)

Jan Luyts, BASF Antwerpen nv

Terneuzen, 25 januari 2018



EEN GEZOND BEDRIJF



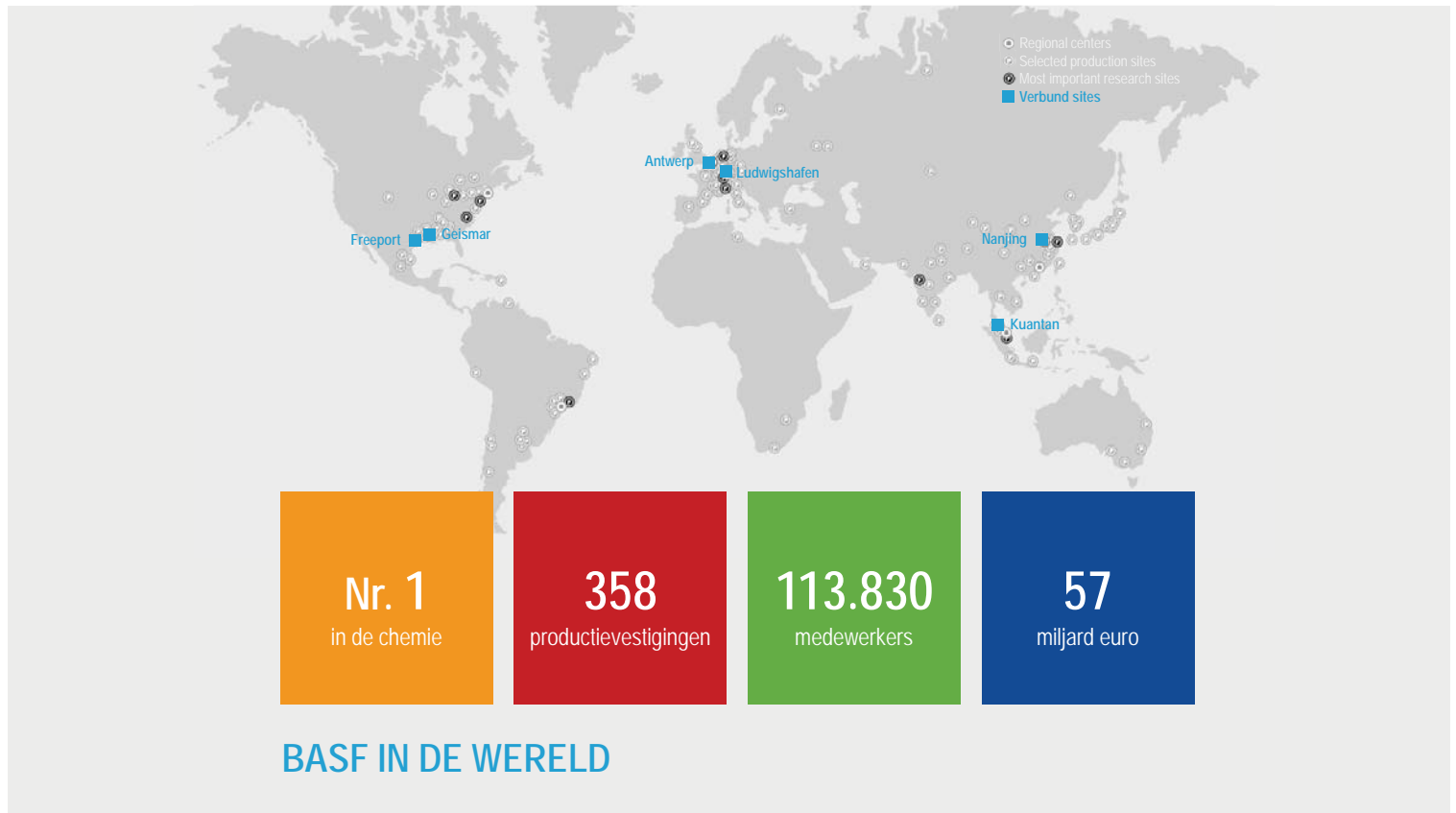
6
km²



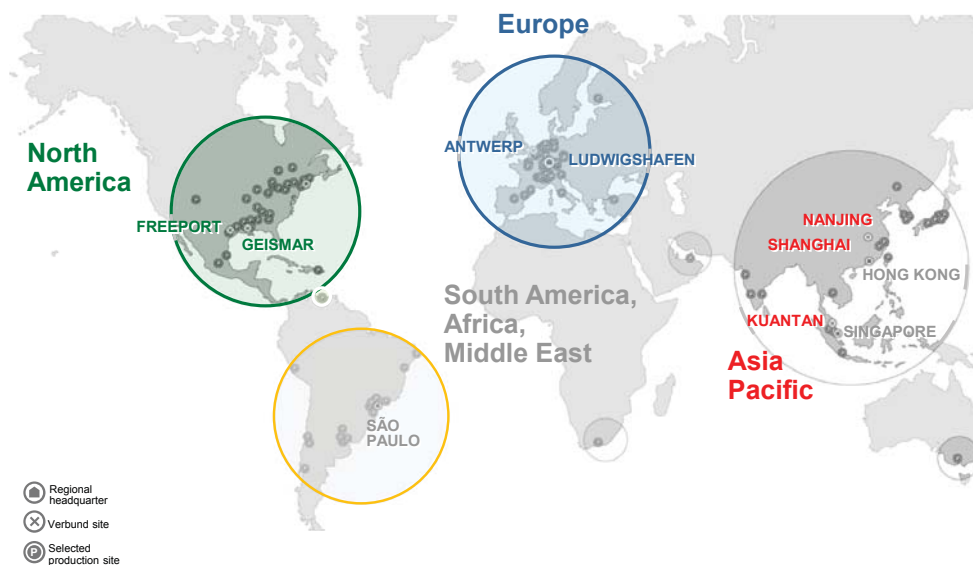
3.127
medewerkers



ca. 5
miljard euro



BASF SIS Approach

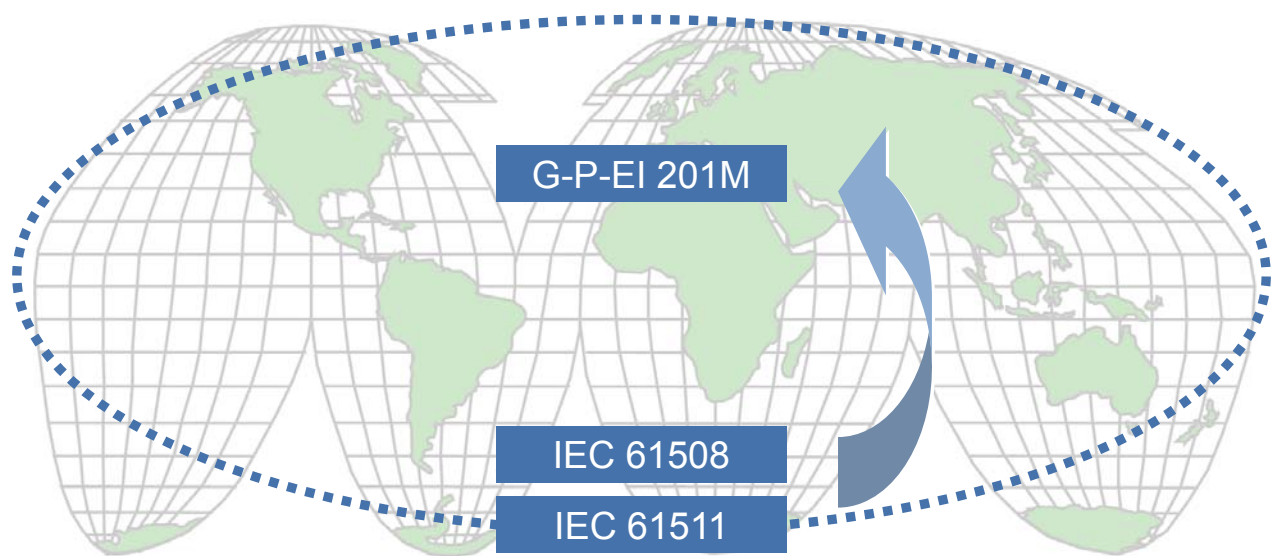


Data 2016
 > 100 Sites
 > 710 Plants
 > 18.800 SIF's
 > 84.500 Devices

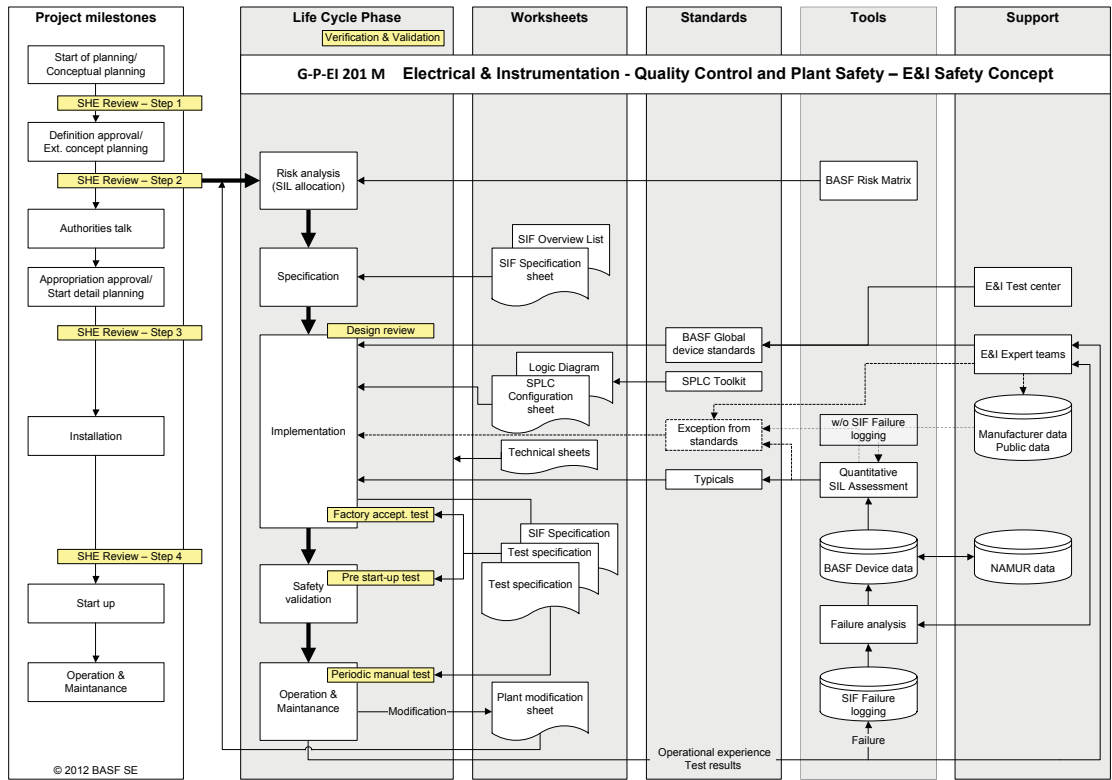
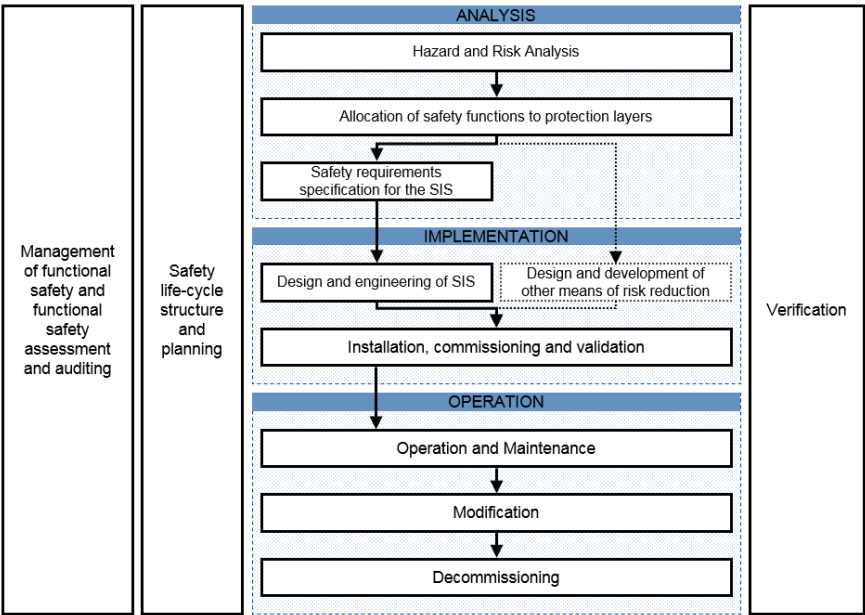
BASF SIS Approach



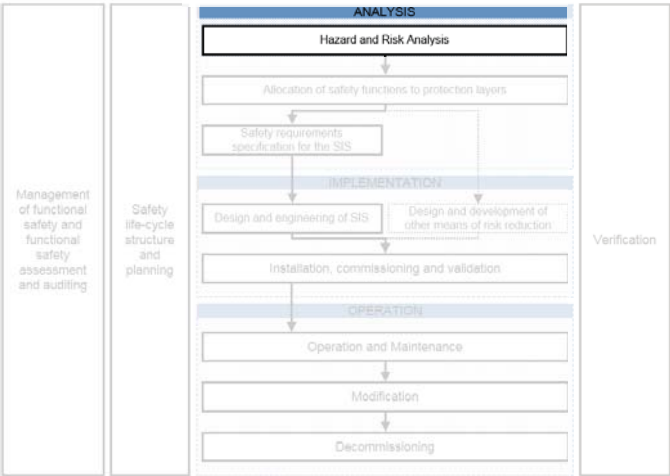
BASF SIS Approach



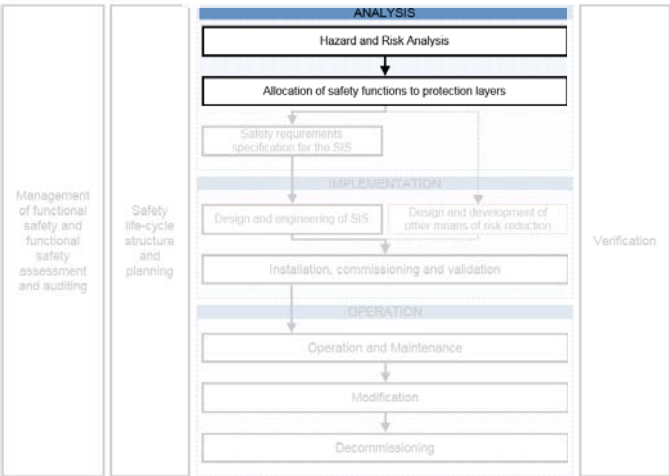
Management of Functional Safety & Life Cycle Requirements



Hazard and Risk Analysis



Allocation of safety functions



Risk Matrix				
Probability	Severity			
	S ₁	S ₂	S ₃	S ₄
P ₂	A	B	D	E
P ₁	A/B*	B	E	E
P ₂	B	C	F	F
P ₁	C	D	F	F
P ₄	E	F	F	F

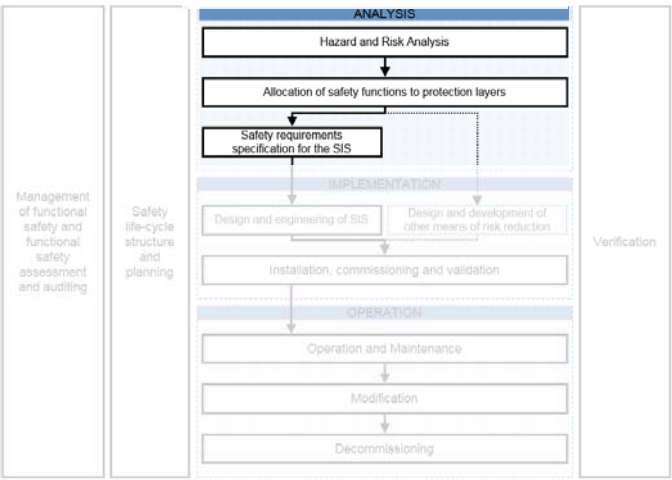
Probability:
P₄ Happened a couple of times (once per year or more often)
P₃ Happened once (Approx. once in 10 years)
P₂ Almost happened, near miss (Approx. once in 100 years)
P₁ Never happened, but is thinkable (Approx. once in 1,000 years)
P₀ Not plausible (less than once per 10,000 years)

Severity: (Health Effects)
S₁ On site: Potential for one or more fatalities
S₂ On site: Potential for one or more serious injuries (non-reversible)
S₃ On site: Potential for one or more lost time injuries
S₄ On site: Potential for minor injuries, or irritation

Risk Class	Risk Level	Minimum Requirements
A	Extreme, totally unacceptable risk	Process or design change preferred
B	Very large, unacceptable risk	Process / design change, or one protective measure of SIL 3 equivalent (PSV, SIS, etc.)
C	Large, unacceptable risk	Process / design change, or one protective measure of SIL 2 equivalent (PSV, SIS, etc.)
D	Medium, acceptable risk, which should be further reduced	One monitoring device of high quality with documented testing
E	Small, acceptable risk, which may be further reduced	One monitoring device
F	Very small, acceptable risk	None

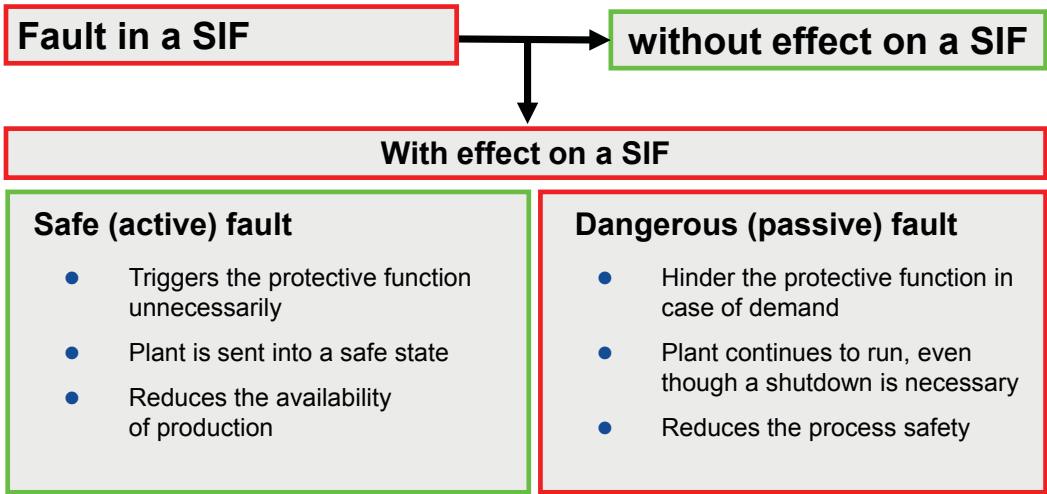


Safety Requirements Specifications



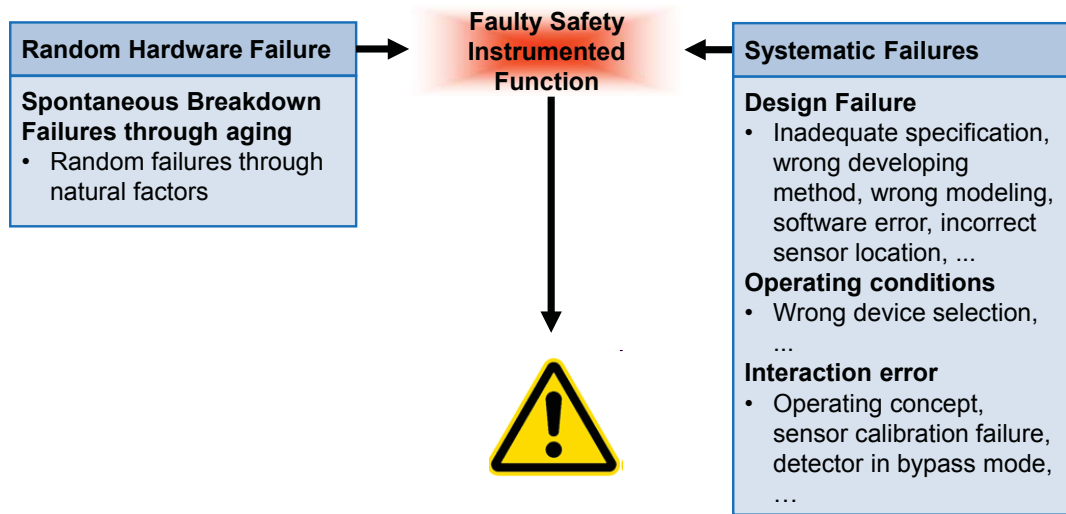
Safety Requirements Specifications

Faults within Instrumented Installations

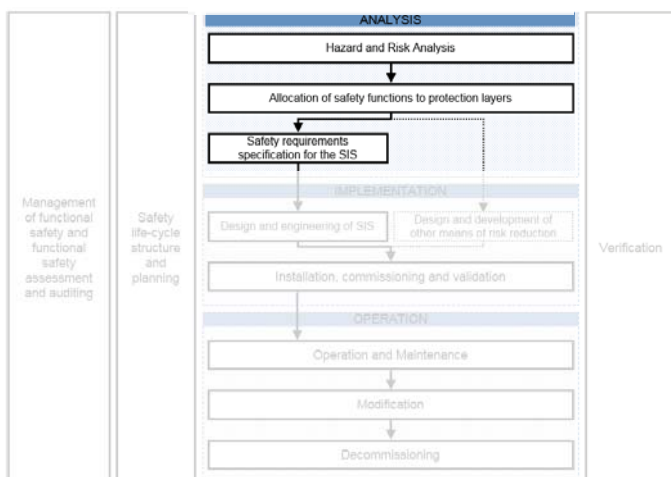


Safety Requirements Specifications

Faults within Instrumented Installations



Safety Requirements Specifications




Basics Design Rules for SIF:

- ▶ SIF's should be as simple as possible
- ▶ SIF's shall not be carried out in the BPCS (e.g. "standard" DCS)
- ▶ A breakdown based on a dangerous fault in a SIF is not tolerable
- ▶ A dangerous fault may not lead to a hazardous condition
- ▶ Trip functions may not automatically be reset after the process variable has returned to its normal value again
- ▶ Whenever feasible, devices shall be used which have the capability to go to a predetermined safe state in the event of a specific malfunction
- ▶ Analog values shall be used whenever possible
- ▶ Measures should be taken to increase the online diagnostic coverage, e.g. through A-B-channel-comparison for analog signals, signal plausibility checks or other means
- ▶ SIF's and the components which are part of a SIS (e.g. transmitter, power supply, I/O card of a logic solver) shall be clearly marked

→ Good Engineering Practices

Safety Requirements Specifications

- General plant information
- Requirements from Technology and Operation
 - ▶ SIF Description
 - ▶ Requirements from Risk Assessment
 - ▶ Safety-relevant process values and their trip limits
 - ▶ Safety-relevant Process outputs and dedicated actions
 - ▶ Operational requirements
 - Manual actions or
 - Time of uninterrupted operation
 - Repair time
 - ...

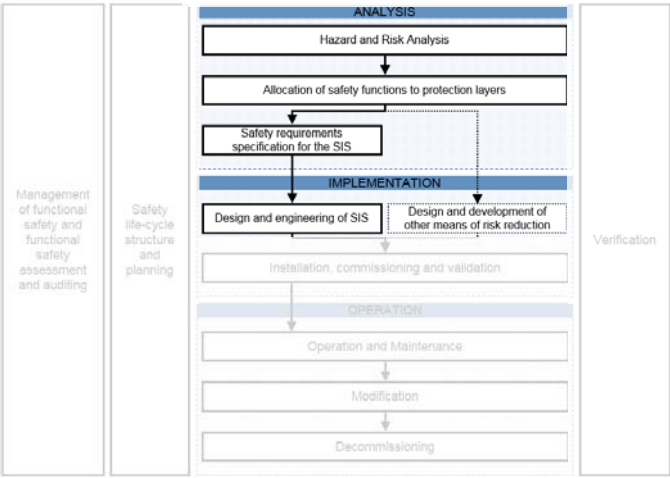
 BASF The Chemical Company		Specification & Review Form for Safety Instrumented Function U2 <small>Page 1 of 2</small>		
Item	Rev	Rev Description	Approved Signature	Date
Plant / Location U2 Description Complete Event and possible Effects		U2.1. No. Rev. Revision		
U2.2. Safety Function				
U2.3. Safe State of the Function				
U2.4. Normal Operating Range and Safe Low/High Limits				
Requirements from Risk Assessment				
U2.5. Risk from: BOP, No. Safe States U2.6. No. Safety Functions, U2.7. No. SIFs U2.8. No. Safety Functions, U2.9. No. SIFs U2.10. No. Safety Functions, U2.11. No. SIFs U2.12. No. Safety Functions, U2.13. No. SIFs		Approved U2.4 U2.5 U2.6 U2.7 U2.8 U2.9 U2.10 U2.11 U2.12 U2.13		
U2.14. No. Safety Functions, U2.15. No. SIFs U2.16. No. Safety Functions, U2.17. No. SIFs U2.18. No. Safety Functions, U2.19. No. SIFs U2.20. No. Safety Functions, U2.21. No. SIFs		U2.22 U2.23 U2.24 U2.25 U2.26 U2.27 U2.28 U2.29 U2.30 U2.31 U2.32 U2.33 U2.34 U2.35 U2.36 U2.37 U2.38 U2.39 U2.40 U2.41 U2.42 U2.43 U2.44 U2.45 U2.46 U2.47 U2.48 U2.49 U2.50 U2.51 U2.52 U2.53 U2.54 U2.55 U2.56 U2.57 U2.58 U2.59 U2.60 U2.61 U2.62 U2.63 U2.64 U2.65 U2.66 U2.67 U2.68 U2.69 U2.70 U2.71 U2.72 U2.73 U2.74 U2.75 U2.76 U2.77 U2.78 U2.79 U2.80 U2.81 U2.82 U2.83 U2.84 U2.85 U2.86 U2.87 U2.88 U2.89 U2.90 U2.91 U2.92 U2.93 U2.94 U2.95 U2.96 U2.97 U2.98 U2.99 U2.100		
U2.101 U2.102 U2.103 U2.104 U2.105 U2.106 U2.107 U2.108 U2.109 U2.110 U2.111 U2.112 U2.113 U2.114 U2.115 U2.116 U2.117 U2.118 U2.119 U2.120 U2.121 U2.122 U2.123 U2.124 U2.125 U2.126 U2.127 U2.128 U2.129 U2.130 U2.131 U2.132 U2.133 U2.134 U2.135 U2.136 U2.137 U2.138 U2.139 U2.140 U2.141 U2.142 U2.143 U2.144 U2.145 U2.146 U2.147 U2.148 U2.149 U2.150 U2.151 U2.152 U2.153 U2.154 U2.155 U2.156 U2.157 U2.158 U2.159 U2.160 U2.161 U2.162 U2.163 U2.164 U2.165 U2.166 U2.167 U2.168 U2.169 U2.170 U2.171 U2.172 U2.173 U2.174 U2.175 U2.176 U2.177 U2.178 U2.179 U2.180 U2.181 U2.182 U2.183 U2.184 U2.185 U2.186 U2.187 U2.188 U2.189 U2.190 U2.191 U2.192 U2.193 U2.194 U2.195 U2.196 U2.197 U2.198 U2.199 U2.200				
U2.201 U2.202 U2.203 U2.204 U2.205 U2.206 U2.207 U2.208 U2.209 U2.210 U2.211 U2.212 U2.213 U2.214 U2.215 U2.216 U2.217 U2.218 U2.219 U2.220 U2.221 U2.222 U2.223 U2.224 U2.225 U2.226 U2.227 U2.228 U2.229 U2.230 U2.231 U2.232 U2.233 U2.234 U2.235 U2.236 U2.237 U2.238 U2.239 U2.240 U2.241 U2.242 U2.243 U2.244 U2.245 U2.246 U2.247 U2.248 U2.249 U2.250 U2.251 U2.252 U2.253 U2.254 U2.255 U2.256 U2.257 U2.258 U2.259 U2.260 U2.261 U2.262 U2.263 U2.264 U2.265 U2.266 U2.267 U2.268 U2.269 U2.270 U2.271 U2.272 U2.273 U2.274 U2.275 U2.276 U2.277 U2.278 U2.279 U2.280 U2.281 U2.282 U2.283 U2.284 U2.285 U2.286 U2.287 U2.288 U2.289 U2.290 U2.291 U2.292 U2.293 U2.294 U2.295 U2.296 U2.297 U2.298 U2.				

Safety Requirements Specifications

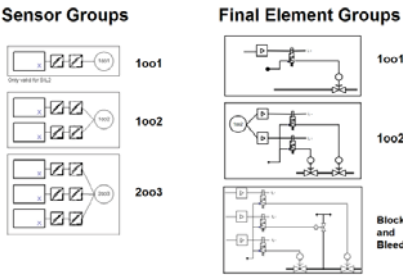
- Requirements from Process control / E&I
 - ▶ Detailed function
 - ▶ Requirements for diagnostics
 - ▶ Interfaces
 - ▶ Special requirements for sensors and/or final elements based on environmental conditions or requested reliability/accuracy
- Regional requirements
- Roles and Responsibilities
 - Technology: Persons deeply involved in the process and participating or knowing the results of the safety review
 - E&I: Persons participating or knowing the results of the safety review
 - Responsibility for completeness and correctness of the SIF requirements including change order based on the Safety review
 - Four-eye-principle

[illegible]

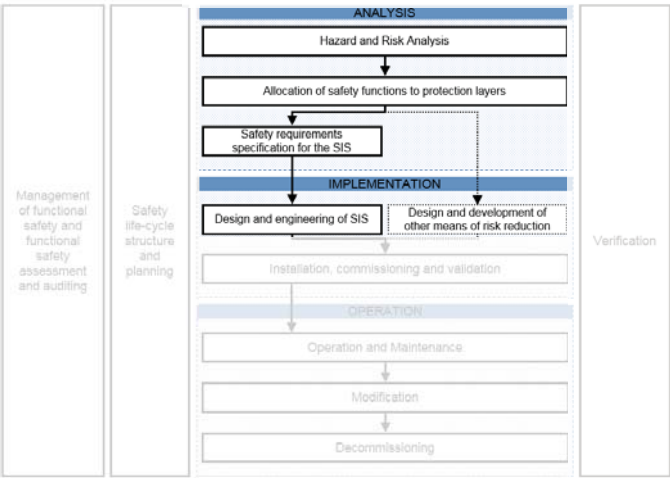
Design and engineering of SIS



Sensor and Final Element groups

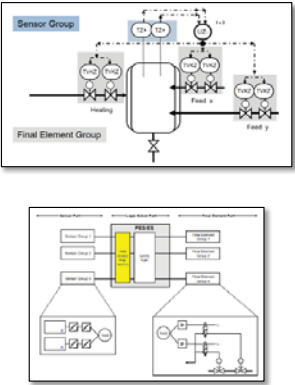


Design and engineering of SIS



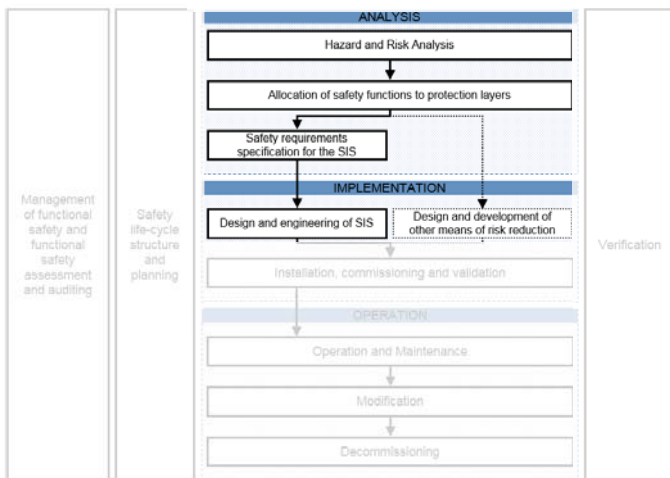
SIF Standard Hardware Structures:

Typicals:



Limits of Standard HW Structures have to be taken in to account

Design and engineering of SIS



- Only field devices or logic solvers that comply with BASF's "Global Standard List (GSL) for Instrumentation" shall be used for new Safety Instrumented Functions
- Devices not on the GSL shall only be used if
 - ▶ it can be shown that the device is proven in use in a chemical plant environment for at least one year prior to date of delivery to BASF without any dangerous failure and
 - ▶ the regional working group responsible (e.g. in BASF SE: CoE Instrumentation, BASF Corporation I&C COE, etc) for that type of device has agreed and a risk analysis was performed
- SPLC's working as a logic solver shall only be used for SIS if they are certified by an independent organization (e.g. TUV)

Design and engineering of SIS BASF Standard Device

- Test in acc. to IEC 770 and NE95 in the E&I equipment test center
 - ▶ Check of specification (desired functions of the device)
 - ▶ Check of influencing factors (U, T, p, EMC, ...)
 - ▶ Load/stress tests (e.g. ball valves or switching amplifiers 100,000 switching's, pressure sensors 500,000 load changes)
- Workshop check
- Operational experience (acc. NE130)
 - ▶ Period of one to two years
 - ▶ Evaluation of handling, parameterization, failures

Design and engineering of SIS BASF Global Standard Device List

- Standardization of equipment and installation materials is an essential means in improving E&I planning, engineering, installation and maintenance activities.
- Key advantages
 - ▶ Costs
 - ▶ Stocking of spare parts
 - ▶ Quality assurance
 - ▶ Availability
 - ▶ Use in safety instrumented systems
 - ▶ Central documentation



Design and engineering of SIS Global Standard Device List for Logic Solvers

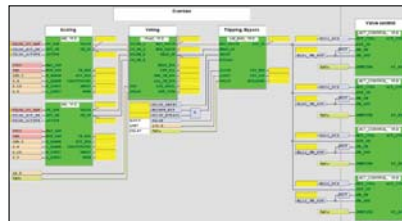
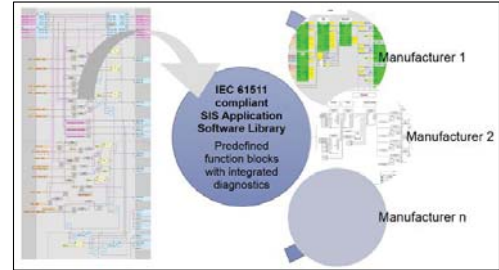
- SPLC's or hardwired systems shall only be used for SIS if they are IEC 61508 certified by an independent organization (e.g. TÜV) and listed on the BASF Standard device list!



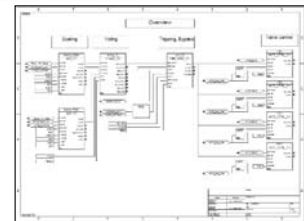
Design and engineering of SIS Application software

■ BASF Standard Software Structures

- ▶ BASF SPLC-Toolkit for application software
 - Optimized for use with BASF standard hardware structures
- ▶ Parameterization instead of programming
 - Safety and Economic Efficiency



HIMA

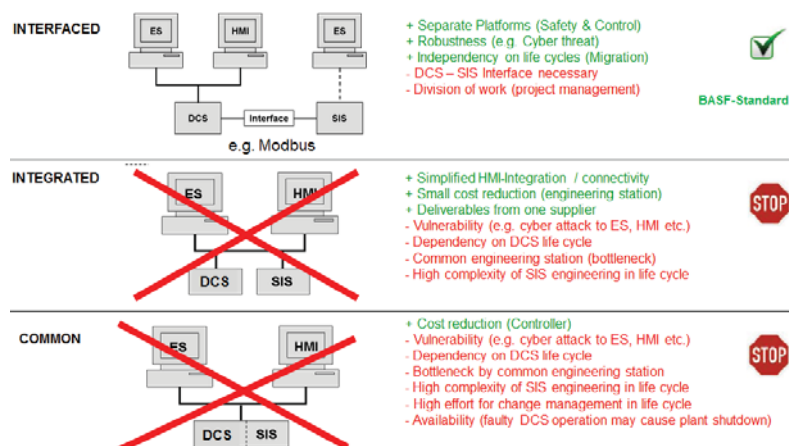


Triconex



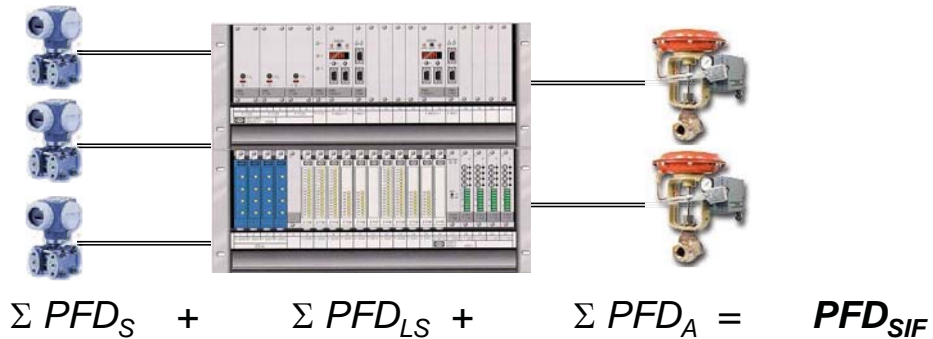
Design and engineering of SIS Safety and Economic Efficiency

■ Levels of Integration (DCS / SIS)



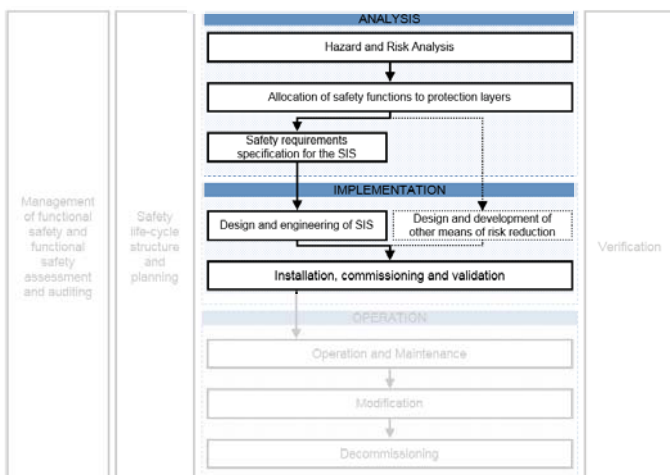
Design and engineering of SIS

PFD of a Safety Instrumented Function

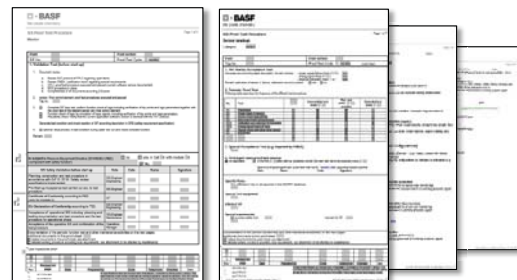


Standard hardware structures (Typicals) that have been verified for SIL2 and SIL3 hardware safety integrity requirements.

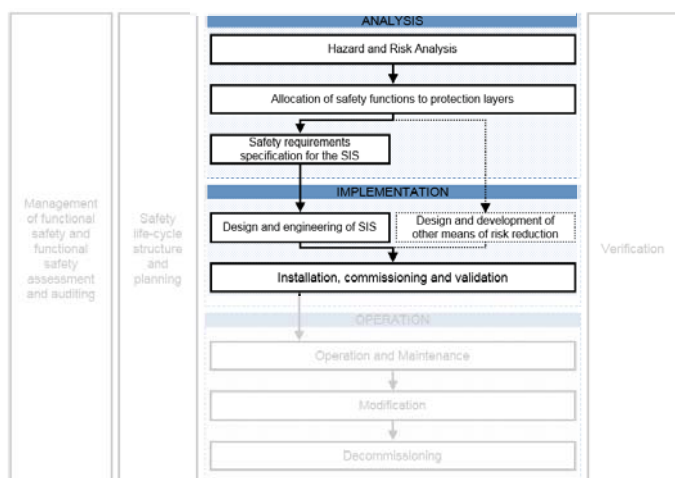
Installation, commissioning and validation



- Installation
- FAT (Factory Acceptance Test)
- SAT (Site Acceptance Test)
- PSAT (Pre Startup Test)
- ▶ Staggered Test or Function-oriented Test (Pipe to Pipe)



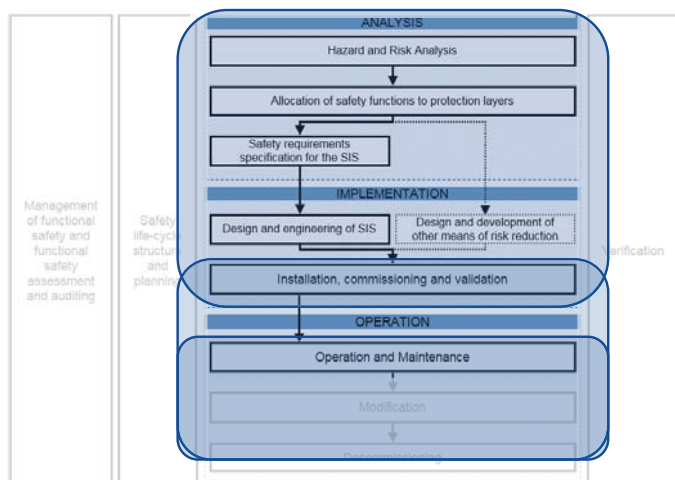
Installation, commissioning and validation



■ SHE Step 4 Review

- ▶ Validation that the SIS was built, installed and tested according SRS
- ▶ Test procedure(s) for the regular proof test are in place
- ▶ Safety Review recommendations that apply to the SIS have resolved or implemented
- ▶ Employee training has been completed
- ▶ Documentation has been fully completed
- ▶ Test results are documented, signed by BASF SIS Engineer and Plant Manager

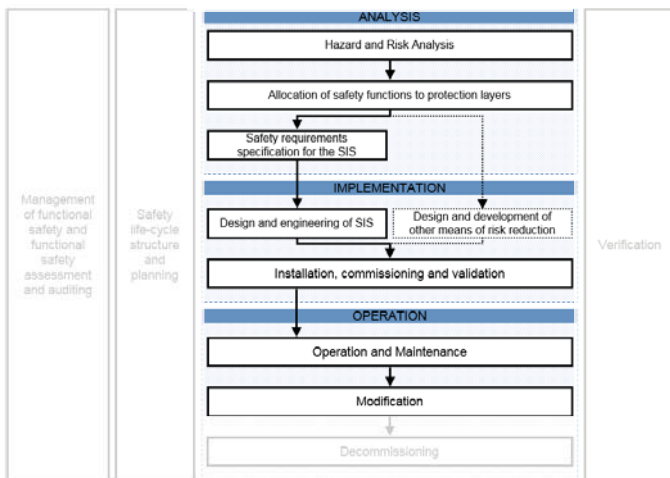
Operation and Maintenance



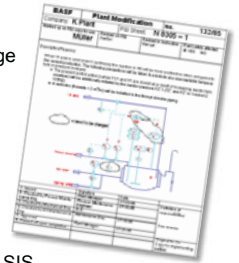
- Operation
- Periodic proof test
- Maintenance
- Test after repair
- Test after modification

[illegible][illegible]

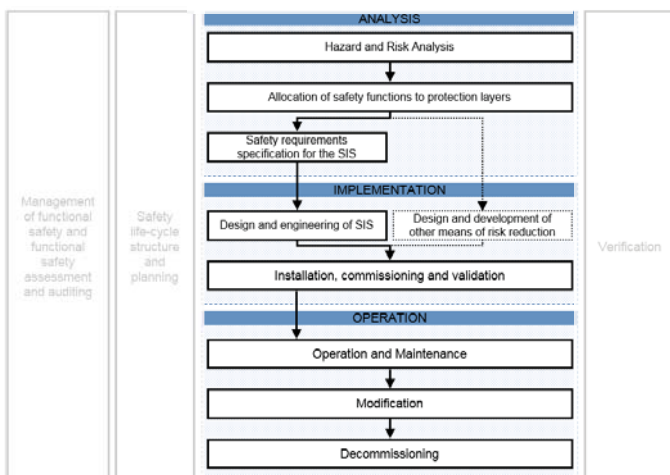
Modification



- Types of Modification
 - ▶ Plant modification / Trip point change / Parameter change
- Plant Modification Sheet Form
 - ▶ Description of the modification or change
 - ▶ Reason for the change
 - ▶ Identified hazards which may be affected
 - ▶ Analysis of the impact of the modification activity on the SIS
- Additional documentation
 - ▶ Hard- & software changes, new device data sheets, ...
- Test
 - ▶ As PSAT but only for the affected SIF part
 - ▶ If possible use of automatic application software comparison

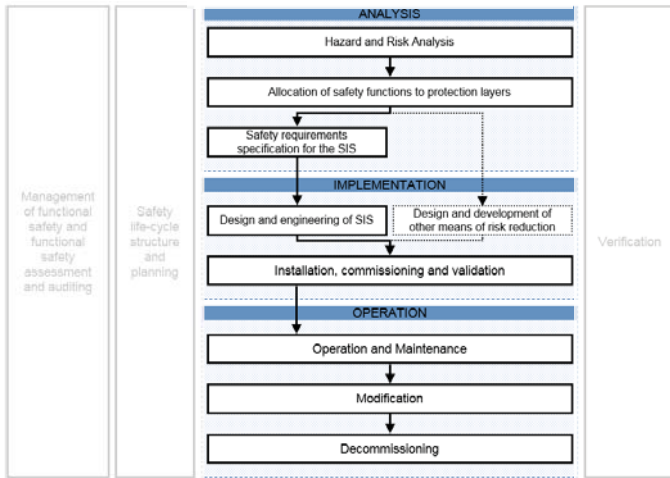


Decommissioning

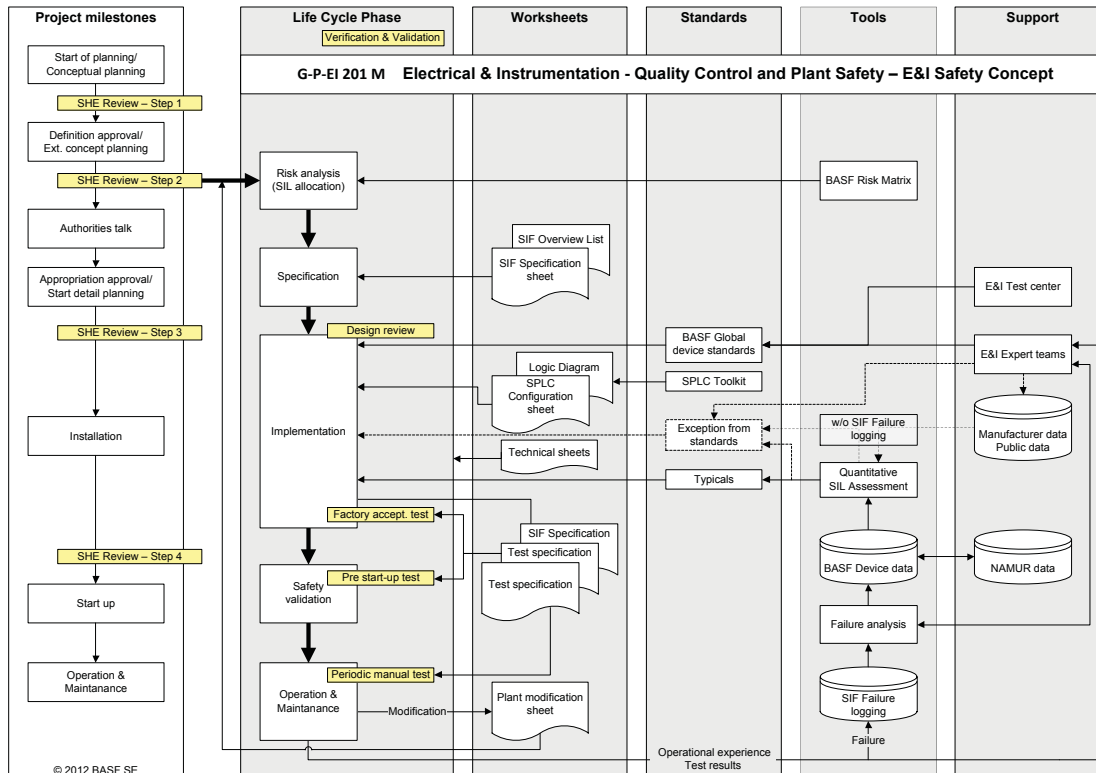


- Hazard analysis
 - ▶ Update of the hazard and risk assessment
 - ▶ Determination which subsequent safety life cycle phases shall need to be revisited
 - ▶ Functional safety during the execution of the decommissioning activities
 - ▶ The impact of decommissioning of a SIS on adjacent operating units and facility services
- The results shall be used to re-implement the relevant requirements including re-verification and re-validation.
- MOC procedure

Verification and Validation



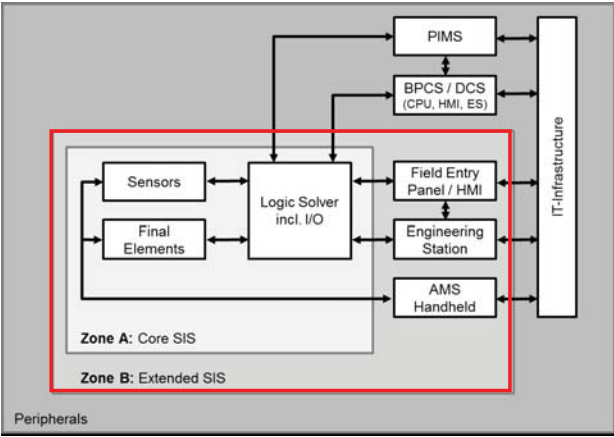
- Continuous inspection in every step of the safety life cycle → Verification
 - ▶ For-Eyes-Principle → a person that is independent from the current work step
 - ▶ Responsible: E&I Engineer, Lead Engineer, Asset and/or Maintenance Manager
- Functional Safety Assessment → Validation
 - ▶ Technical expert
 - ▶ Surveyor
 - ▶ Authorities
 - ▶ ...



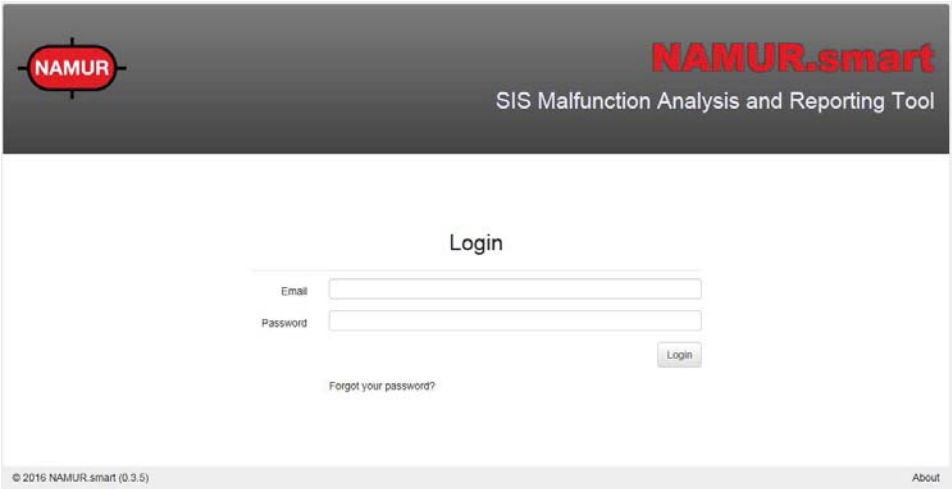
Automation Security



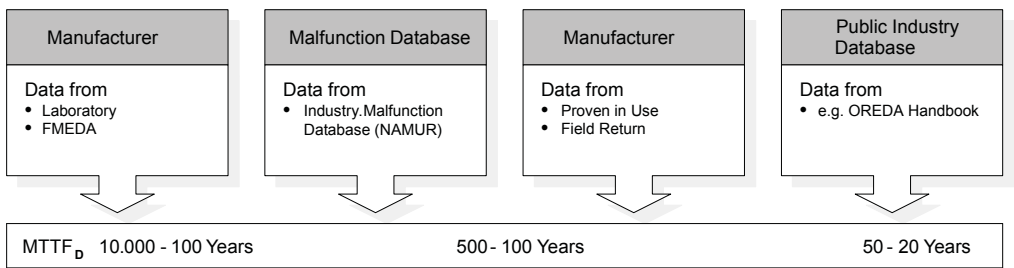
■ Security for Safety Instrumented Systems



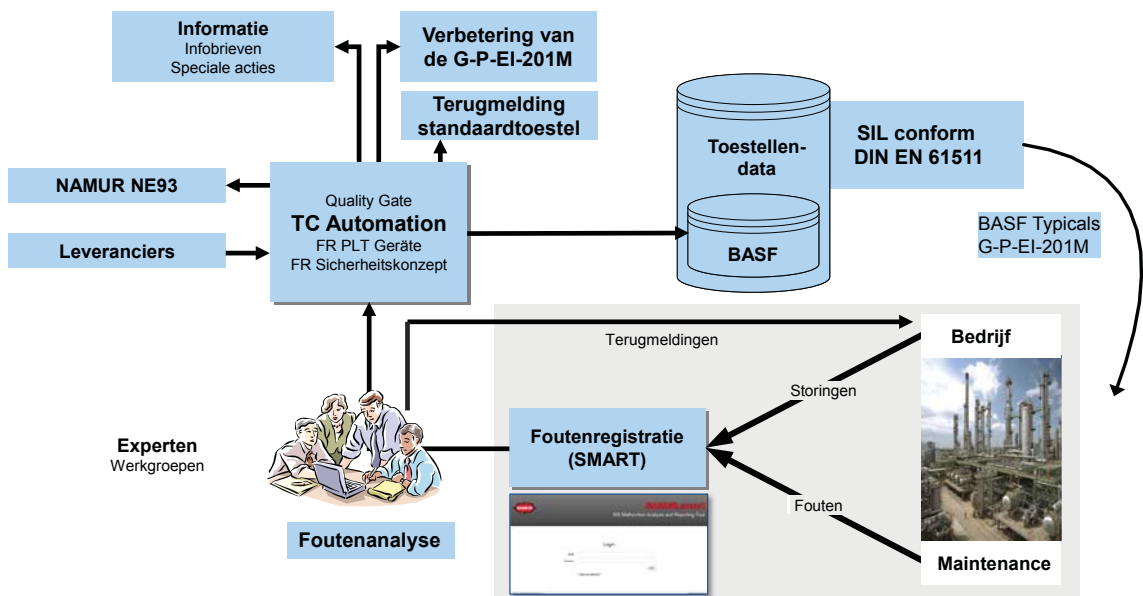
Monitoring and analysis for SIS



Comparison of Reliability Data

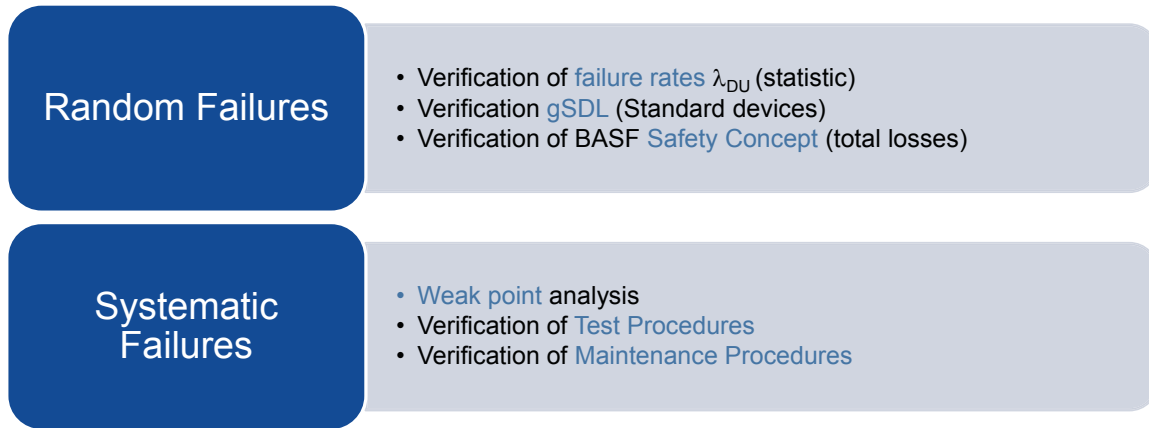


SIF Malfunction Recording - BASF-concept

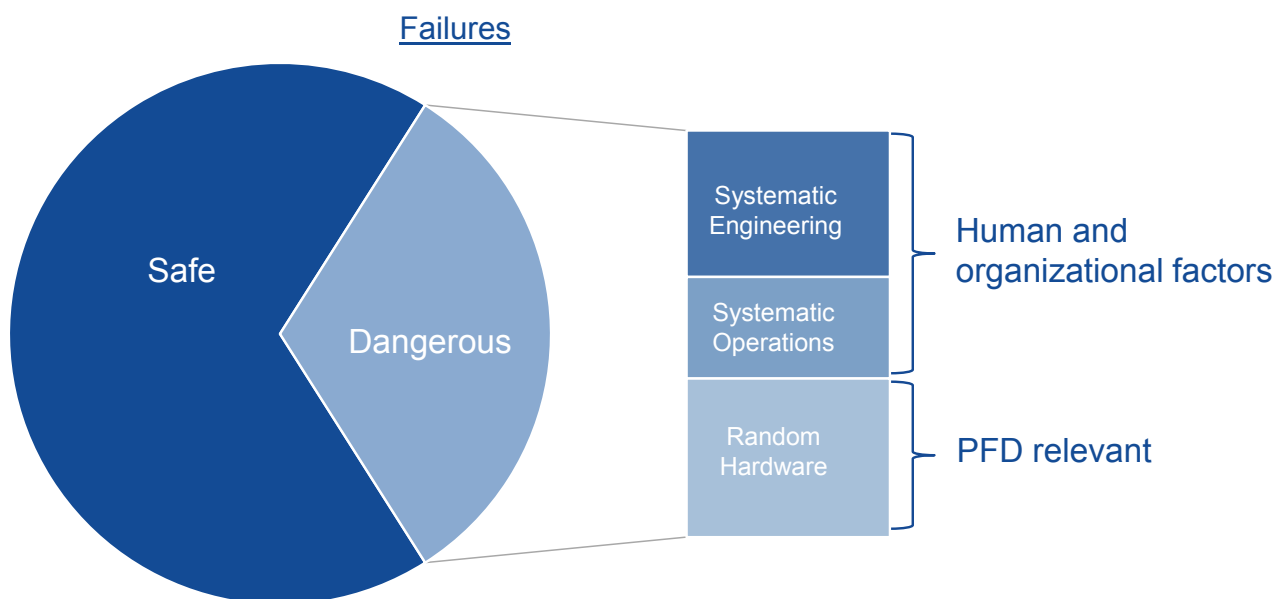


NAMUR.smart to BASF-concept

■ Investigation of Dangerous failures



Distribution of Failures of Instruments



Functional Safety Management

