STW
Making mobile machines perform.

Step by Step to Safe Machines

System Concept

Planning

Hazard and Risk Analysis

Analysis according to EN ISO 12100 and determining the PL_r in accordance with EN ISO 13849-1

S Severity of injury	F Frequency and / or duration of exposure to hazard	P Possibility of avoiding the hazard	Performance Level (PL_r)
S1: Slight injury	F1: Seldom to more often	P1: Possible under certain conditions	
S2: Serious injury	F2: Frequent to continuous	P2: Scarcely possible	

Risk matrix (low risk → high risk):

- S1, F1: P1 → a; P2 → b
- S1, F2: P1 → b; P2 → c
- S2, F1: P1 → c; P2 → d
- S2, F2: P1 → d; P2 → e

Safety Requirements

Specification of the Safety Functions

Safety Concept

Evaluation of the Performance Level

Performance Level (PL)	Cat. B	Cat. 1	Cat. 2		Cat. 3		Cat. 4
	DC < 60 % none	DC < 60 % none	60 % ≤ DC < 90 % low	90 % ≤ DC < 99 % medium	60 % ≤ DC < 90 % low	90 % ≤ DC < 99 % medium	99 % ≤ DC high
	CCF not relevant		Measures against CCF: Min. 65 points				
a							
b							
c							
d							
e							

Evaluation	$MTTF_D$
Low	3 Years ≤ $MTTF_D$ < 10 Years
Medium	10 Years ≤ $MTTF_D$ < 30 Years
High	30 Years ≤ $MTTF_D$ < 100 Years

Safety-related Block Diagram

Determination of Safety Characteristic Numbers: CCF – DC – $MTTF_D$ (e.g. with SISTEMA)

$PL \geq PL_r$? — No / Yes

Safety Architecture

Category B/1
- Input — Input Device → Logic — Processing Unit → Output — Output Device

Category 2
- Input — Input Device → Logic — Processing Unit → Output — Output Device
- m Monitoring
- TE — Test Equipment → OTE — Output of TE

Category 3/4
- Input 1 — Input Device → Logic 1 — Processing Unit → m → Output 1 — Output Device
- c Cross Monitoring
- Input 2 — Input Device → Logic 2 — Processing Unit → m → Output 2 — Output Device

Machine Safety according to EN ISO 13849

Process	Roles	Documents
Project Management	Project Manager	Project Management Plan Project Plan
Requirements Analysis & Design	System Architect Hardware Architect Software Architect	System and Safety Requirements System Design incl. Safety Concept Hardware Requirements and Design Software Requirements and Design Software Module Specification
Safety Management	Safety Engineer Safety Analyst Safety Assessor	Hazard and Risk Analysis Safety Plan Safety and Fault Analysis Document Plan (Safety Case) Assessment Report
Development Processes	Hardware Developer Software Developer Construction Engineer Technical Writer	Switching / Wiring Diagrams Software Implementation Construction Plans User Documentation
Test Management	Test Manager Test Analyst	Verification and Validation Plan Test Specification Test Reports Master Test Report
Configuration Management	Configuration Manager	Configuration List
Change Management	Change Manager	List of Changes

Glossary:

CCF	Common Cause Failure – Failures of different items, resulting from a single event
DC	Diagnostic Coverage – Measure of the effectiveness of diagnostics
$MTTF_D$	Mean Time To Dangerous Failure – Expectation of the mean time to dangerous failure
PL_r	Performance Level (required) – Required property of a safety function to reduce the risk adequately

Software Development

V-model:
- Software Requirements → Validation (Validation)
- Software Design ↔ Integration Test
- Module Specification ↔ Module Test (Verification)
- Implementation

Commissioning and Test

Approval

Operation and Maintenance

Decommissioning

Safety and conformity assessment, assessment by the notified body and preparation of the EC declaration of conformity in accordance with the Machinery Directive.