Safety requirements

Article 95 EC Treaty
(free movement of goods)

- e.g. machines
  - Low-voltage directive (2006/95/EC)
  - Machinery directive (2006/42/EC)
  - Harmonized European standards
  - Manufacturer

Article 137 EC Treaty
(industrial safety)

- "Industrial safety" framework directive (89/391/EEC)
  - Separate directive "Use of operating equipment" (89/655/EC)
  - National laws
  - User
<table>
<thead>
<tr>
<th><strong>Design and risk evaluation of the machine</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EN ISO 12100</strong></td>
</tr>
<tr>
<td>Safety of machines</td>
</tr>
<tr>
<td>Basic terms,</td>
</tr>
<tr>
<td>general principles</td>
</tr>
<tr>
<td>Safety of machines</td>
</tr>
<tr>
<td>Risk assessment, part 1: principles</td>
</tr>
<tr>
<td><strong>EN ISO 14121-1</strong></td>
</tr>
</tbody>
</table>

**Functional and safety-relevant requirements**
for safety-related control systems

**Development and realization of safety-related controls**

| **EN 62061:2005**                           |
| Safety of machines                         |
| Functional safety of safety-related       |
| electrical, electronic and programmable    |
| electronic control systems                 |

| **EN ISO 13849-1:2006**                     |
| Safety of machines                         |
| Safety-related components of controls,     |
| part 1: general principles                 |
| *Successor standard of EN 954-1:1996*      |
| *Transition period until end of 2011*      |

| **Any architectures**                      |
| Safety Integrity Level (SIL)               |
| SIL 1, SIL 2, SIL 3                       |

| **Designated architectures**               |
| *(categories)*                             |
| Performance Level (PL)                    |
| PL a, PL b, PL c, PL d, PL e              |

| **Electrical safety aspects**              |
| **EN 60204-1**                             |
| Safety of machines                         |
| Electrical equipment of machines,          |
| component 1: general requirements          |
Step 1
Management of functional safety

LAWS, REQUIREMENTS
Machinery Directive (EHSR)

RISK IDENTIFICATION
Risk assessment & evaluation, risk reduction

SAFETY FUNCTION
Specification - Functionality
- Safety performance (SIL, PL)

IMPLEMENTATION
Architecture, subsystems, safety / reliability parameters

FUNCTIONAL TESTING
Functional testing, achieved SIL / PL level

VERIFICATION

DOCUMENTATION
Compliance assessment, technical file, documentation

COMPLIANCE

VALIDATION
Document the design, residual risk, user instructions

Does the function fulfill the risk reduction requirement?

Step 2 - 3

Step 4

Step 5

Step 6

Step 7

Step 8

Step 9
START

Risk Assessment
- Determination of the limits of the machine (specification)
- Hazard Identification
- Risk Estimation
- Risk Evaluation

Is the risk tolerable?
- Document
- END

Risk Reduction
- Risk reduction process:
  1. Inherently safe design
  2. Guards and protective devices
  3. Information for use
- Design of Safety-Related Part of the Control System (SRP/CS)

Does the protective measures depend on the Control System?
- YES
- NO

New hazards?
- NO
- YES

If the protective measure depend on the Control System

1. Identify the Safety Functions
2. Specify the requirements
3. Determined the required Performance Level (PLr)
4. Design the Safety Functions
5. Evaluate the PLr (Category, MTTF, DC, CCF, Software)
6. Verification of PLr (is PLr ≥ PLr) [YES NO]
7. Validation. Are all requirements met?
- YES
- NO

Back to Risk Assessment (ISO14121) / Risk Reduction (ISO12100)
Relationship of standards to various European Directives related to machinery

Selection of relevant Directives and associated standards

Base Documents:
Machinery Directive (98/37/EC)
ISO 12100-1,-2: Basic concepts
ISO 14121: Risk assessment
IEC 60204-1: Basic electrical reqts
ISO 13849-1: Safety-related parts
ISO 14118: Prevention of unexpected start-up

ISO 13852, ISO 13854, ISO 13853:
Safety dist.
ISO 13855: Hand/arm speed
ISO 13850: Emergency stop:
Marking and actuation
Acoustical noise
Documentation
Ergonomics

Does the EMC Directive apply?

Yes

Base Documents:
EMC Directive
EN 50081, EN 50082
IEC 61000-4

No

Base Documents:
ISO 14120: Fixed and movable guards
ISO 14119: Interlocking devices ...

Guards and Interlocks?

Yes

ISO 13851: Two-hand control
IEC 61496-1 to -3: ESPE
ISO 13856-1: PSPD

Protective devices?

Yes

ISO 4413: Hydraulics
ISO 4414: Pneumatics

Fluid power components?

Yes

ISO 14123-1,-2: Hazardous substances
EN 1093: Airborne emissions
ISO 14122-1 to -4; Requirements for permanent access

Other?

Yes

Does the ATEX Directive apply?

Yes

Base Documents:
ATEX Directive (94/9/EC)
EN 1127-1

No

Does the Simple Pressure Vessel Directive apply?

Yes

Base Documents:
SPV Directive (87/404/EEC)

END
Identify the safety functions to be performed by SRP/CSs

For each safety function specify the required characteristics (see Clause 5)

Determined the required performance level PL (see 4.3 and Annex A)

For each selected safety function

Design and technical realisation of the safety function:
Identify the safety-related parts which carry out the safety function (see 4.4)

Evaluate the performance level PL (see 4.5) considering:
- category (see Clause 6)
- MTTFd (see Annex C and D)
- DC (see Annex E)
- CCF (see Annex F)
- If existing: software (see 4.6 and Annex J) of the above safety-related parts

Verification of PL for the safety function:
Is PL ≥ PL (see 4.7)

Validation (see Clause 8a)
Are all requirements met?

Yes

Have all safety functions been analysed?

Yes

To Figure 1 (ISO 12100)
Start

Validation plan

Validation principles

Documents

Criteria for fault exclusion

Fault lists

Design considerations

Analysis

Is analysis sufficient?

Testing

Specification of the Safety functions

Safety function

PL and categories:
- determination of the category
- MTTFd, DC, CCF
- systematic faults
- software
- verification of the PL for SRP/CS
- combination of SRP/CS

Environmental requirements
Maintenance requirements
Technical specification/user information

Category 2, 3, 4

Test of safety function under fault condition

Modification of the design

Validation record

All safety functions validated?

End