Safety Instrumented Systems & Functional safety of safety-related systems

A substantial new opportunity for Pfannenberg Signaling products
Safe Signaling

Signaling Technology

- Alarm
- Warning
- Indication
Why?

New edition of the European Directive for Machinery (2006/42/EG) which became mandatory end of 2009. This includes also the related safety standards.
Motivation for Safety of Machinery / Plants

Needless to say:
Safety for people and environment
But also:
Safety for property
Availability and economic efficiency of machines and plants
And of course:
Driven by authorities and inspection bodies

Manufacturer and Market Importer (EU Market Regulation)
Operator (Plant Owner) (Health and Safety Regulations)
International Safety Standards

Standards regarding to SIL & PL

Machinery Industry

Process Industry

Electric
Hydraulic
Pneumatic
Mechanic

IEC 62061

IEC 61511

EN ISO 13849

IEC 61508

Electric
Electronic
Program. Elec.
(E/E/PE)
Relevant standards / regulations:

USA

Process Safety is regulated by OSHA FCR 1910.119. It directs the End User to follow current standards, codes and best industry practice.

Safety Instrumented Systems are governed by ANSI/ISA S84.01, i.e. IEC 61511

Machine Safety: ISO 13849-1 is not mandatory in the US, it becomes more and more significance
## Correlation of Safety Standard

<table>
<thead>
<tr>
<th>SIL / PL and Correlation to Standards</th>
<th>Machinery Industry</th>
<th>Process Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mostly EU</td>
<td>Mostly USA</td>
<td>EU and USA</td>
</tr>
<tr>
<td>Umbrella Standard</td>
<td>IEC 61508</td>
<td>IEC 61508</td>
</tr>
<tr>
<td>Industry Specific Standard</td>
<td>ISO 13849 IEC 61062</td>
<td>ANSI/ISA-S84 / IEC 61511</td>
</tr>
<tr>
<td>Functional Safety Measure</td>
<td>PL SIL SIL</td>
<td>SIL</td>
</tr>
</tbody>
</table>
Safety of Machinery

Hierarchical Structure of EN-Standards

Generic Safety Standards

Type A-Standards
Basic concepts, general principles for design of machinery

Type B-Standards
B1-Standards
General safety aspects
B2-Standards
Relation to specific Protection devices

Type C-Standards
Specific security features of individual machinery classes (Paper/Textile/Presses/etc.)

Safety Group Standards

Technical- Standards
Functional Safety, SIL / PL - Basics

Hierarchical Structure of EN-Standards

Generic Safety Standards
e.g. EN ISO 12100

Safety Group Standards
e.g.
EN ISO 13849-1
EN 62061

Technical-Standards
e.g.
EN 415 Packaging-Mach.
EN ISO11111 Textile-Mach.

Type A-Standards
Basic concepts, general principles for design of machinery

Type B-Standards
EN 61310 visual, acoustic and tactile signals
EN 981 System of aud. and visual danger signals
EN ISO 842 Visual Danger signals
EN ISO 7731 Danger signals for work areas

Type C-Standards
EN 15093/15094 Rolling-Mach.
EN ISO11111 Textile-Mach.
EN 1010 Printing-Mach.
EN 692/693 Presses
EN 1248/1247 Casting-Mach.
Functional Safety

All Standards result in the same unit of measurement!

SIL => Safety Integrity Level)

PL => Performance Level
SIL and PL describe requirements for the maximum permissible probability of dangerous failure for a safety function:

- Probability of dangerous failure per hour $\text{PFH}_D$
- The higher the safety level, the lower the required $\text{PFH}_D$

<table>
<thead>
<tr>
<th>SIL</th>
<th>PL&lt;sub&gt;r&lt;/sub&gt;</th>
<th>$10^{-4}$</th>
<th>$10^{-5}$</th>
<th>$3 \times 10^{-6}$</th>
<th>$10^{-6}$</th>
<th>Not more than 1 dangerous failure of the safety function in <strong>10</strong> years</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PL&lt;sub&gt;r&lt;/sub&gt;b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not more than 1 dangerous failure of the safety function in <strong>100</strong> years</td>
</tr>
<tr>
<td>2</td>
<td>PL&lt;sub&gt;r&lt;/sub&gt;c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not more than 1 dangerous failure of the safety function in <strong>1000</strong> years</td>
</tr>
<tr>
<td>3</td>
<td>PL&lt;sub&gt;r&lt;/sub&gt;d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>PL&lt;sub&gt;r&lt;/sub&gt;e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$\text{PFH}_D$ decreases
The evaluation of the safety levels is based on several columns.
3 Steps of Risk Reduction:

Prio. 1: Safe design  (Integration of safety into the design of machines / plants / processes)

=> No application for our products!

Prio. 2: Technical protective measures  (A safety function must be defined for each hazard that cannot be eliminated by design)

=> Partly application for our products!

Prio. 3: User information warns of residual risks

=> Definitely application for our products!
A "safety function" is executed by a "system".
A "system" is combined of "subsystems".
A "subsystem" consists of "subsystem elements".

Complete SIL/PL of the Safety System

SIL/PL Subsystem 1  SIL/PL Subsystem 2  SIL/PL Subsystem 3
Generally alarming devices perform safety-relevant protective functions within process engineering plants.

This means, if a warning device has to warn in case of failure, at the same time the consequence of a failure of the warning device itself, is always a potential risk.

Application of SIL – calculated Components and inserting into the safety loop!

Machinery Engineering

EN 61310-1, Chapter. 4.1:

„The selection of the used equipment (safety related signaling) has to take into account the consequences of any defect that can result from one of these devices.“

... The measures have to be determined by a risk analysis"
Manufacturer of machinery and plants have to perform a risk evaluation to identify the needed safety level for each system / subsystem.
Risk = Function of:

- Extent of damages (S)
- Frequency and duration (F)
- Possibility of avoidance (P)

Risk reduction estimation:
- Starting point for:
  - Se1
  - Se2

- Low Risk
  - PL a
  - PL b
  - PL c

- High Risk
  - PL d
  - PL e

SIL classification:
- SIL1
- SIL2
- SIL3
Risk: Starting of Machinery

All Safety Functions have to be SIL1 or PLc!
Safe Signaling

Safety Function: Machine-Start-up - Equipment

Command Unit S1

Start-up Control K1

Safety Relay Q1

Command Unit S2

Warning Signal P1

Diagnostic Device G1

Machinery Control K2
Safe Signaling

Safety-Related Block Diagram:

Required SIL/PL Value of the Safety-System „Machine-Start-up Alarming“

\( PL_{r\,c} / SIL \, 1 \)
At least the following control systems shall satisfy table 2 which shows the relevant applications. Others are specified in the other parts of EN1010.

<table>
<thead>
<tr>
<th>Safety Function</th>
<th>PL, &quot;c&quot; or SIL 1</th>
<th>PL, &quot;d&quot; or SIL 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency stop for main drive movement</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Electrically inter-locked protective devices (limit switches)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Operating modes (e.g. hold-to-run, crawl speed)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Acoustic start-up warning signal / flashing warning lights</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Sheet pile rails in the delivery</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Pull lay adjustment on the feeder</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**All Safety Functions have to be SIL1 or PLc!**
Functional Safety

Where to find our products:

Logical illustration of the safety function

Detect (Sensor) → Evaluate (Logic) → React (Actor)
SIL / PL – conform Products:

- **Sounder DS 5 / DS 10-SIL**
  105 / 110 dB, 24Vdc/115Vac/230Vac
  Integrated diagnose function
  suitable for Safety Systems till SIL 2 / PL d

- **Flashlight Quadro F12-SIL**
  10J / 118cd, 24Vdc/115Vac/230Vac
  Integrated diagnose function
  suitable for Safety Systems till SIL 2 / PL d

- **Flashlight PMF 2015-SIL**
  10J / 200cd, 24Vdc/115Vac/230Vac
  Integrated diagnose function
  suitable for Safety Systems till SIL 2 / PL d

Certified according newest Standards
Where to find our products:

Some application examples

Machinery:
- warning for machine start up
- muting mode, in which cases the other safety functions are bypassed

Cranes:
- Warning in case of movement

Process:
- alert in case of gas or chemical leaks
- Acoustic alarm on casting platforms
Functional Safety

SIL / PL relevant target markets / countries:

In general Europe & all associated countries

Countries:
- USA
- Canada
- Japan
- Australia
- China (because of the huge export rate)

Industries
- machinery (manuf. & end user)
- plants (manuf. & end user)
- ind. Processes (end user)
Pfannenberg blazes a trail, that’s for sure!
Safety? Yes
But not too safe!
Any questions?
Please don’t hesitate to ask!