• Why Safety?
• Machine Safety Standards
• Comparison of ISO 13849-1 and IEC 62061
• Safety-related parts of Control Systems

Tool to calculate safety levels
• Machine Safety Life Cycle Support
### Machine Safety
#### History of Safety - USA/Europe

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1877</td>
<td>Massachusetts, required guarding belts, shafts and gears</td>
</tr>
<tr>
<td>1890</td>
<td>Nine US states required machine guarding</td>
</tr>
<tr>
<td>1930</td>
<td>All US states had established job-related safety laws</td>
</tr>
<tr>
<td>1934</td>
<td>Bureau of Labor Standards (F.D. Roosevelt – Frances Perkins), Promote safety and health for working men and women</td>
</tr>
<tr>
<td>1971</td>
<td>Occupational Safety and Health Administration was established</td>
</tr>
<tr>
<td>1981</td>
<td>Lost Workday Incident Rates policy established by OSHA</td>
</tr>
<tr>
<td>1919</td>
<td>EN292 – Basic Concepts of Machine Safety</td>
</tr>
<tr>
<td>1996</td>
<td>EN 954 and EN 1050 – Machinery Safety</td>
</tr>
<tr>
<td>1989</td>
<td>1st pub. of the “Machinery Directive” as Directive 89/392/EC</td>
</tr>
<tr>
<td>1996</td>
<td>EN 954-1 with „Categories“ is published</td>
</tr>
<tr>
<td>1999</td>
<td>IEC 61508 &amp; SIL help to evaluate, “complex“ state of the art</td>
</tr>
</tbody>
</table>
| 1997-2000 | STSARCES project of EC: **EN 954-1 with SIL quantifiable?**
| 2005 | Pub. of **IEC 62061** (SIL, application standard of IEC 61508) |
| 2006 | Pub. of **ISO 13849-1** (PL, successor standard of EN 954-1) |
| 2009 | Commencement of the 3rd “Machinery Directive" 2006/42/EC |
| 2012 | New Work Item Proposal“ to merge ISO 13849 & IEC 62061 |
| 2017 | Planned completion of the merging into **ISO/IEC 17305** |
Machine Safety
USA - Safety Guidance & applicable standards information (Control Design)

North America (USA)

- ANSI: 46.9%
- OSHA: 64%
- EN: 25.2%
- IEC: 29.9%
- ISO: 30.6%
- NFPA: 51%
- Other: 12.2%
- Component Manufacturer: 26.5%

EUROPE

The regulations and standards applicable at the installation location of the system or machine are decisive. All countries follow the same basic principles for application. The European standards and regulations are recognized worldwide.
Machine Safety Standards
Subdivided into Type A, B & C Standards

TYPE A standards
(Basic standards)
Design guidelines and basic terms for machines
- IEC 61508 → SIL
- ISO 12100 → Risk assessment
- ANSI B11.0 Safety Of Machines

TYPE B standards
(Group standards)
B1 standards General safety aspects
- IEC 60204
- EN ISO 13849-1
- EN 693
- IEC 61800-5-2
- EN 81
- EN 693
- IEC 61508 → SIL
- ANSI B11.X Specific Machines

TYPE C standards
(Generic standards)
Specific safety-related requirements for certain machine types.
These standards have priority over A and B standards.
- EN 81 → lifts
- EN 693 → presses
- ANSI B11.19 & 11.20, NFPA 79
- ANSI B11.19 & 11.20, NFPA 79
- ANSI B11.X (1-18) Specific Machines
# Machine Safety Standards
## USA & OSHA

## USA – Machine Safety
- Ensure Safe and Healthy Work Conditions
- OSHA - The law “ have to comply”
- States must meet or exceed
- OSHA Regulations defined in Code of Federal Regulations Title 29
- Reference to Standards such as ANSI and NFPA
  - Considered consensus standards.
  - Standards are Voluntary
  - Unless - they become part of the law
  - "Incorporated by Reference"

<table>
<thead>
<tr>
<th>ANSI – Coordinates Voluntary Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI – Official representative to ISO/IEC</td>
</tr>
<tr>
<td>TUV – OSHA recognized NRTL</td>
</tr>
</tbody>
</table>

## OSHA
- Part 1910: Occupational Safety and Health Standards
  - Subpart O: Machinery and Machine Guarding
    - 1910.211: Definitions
    - 1910.212: General Requirements for all Machinery
      - 1910.147(a)(2)(ii)
        - The minor service exception provides that minor tool changes and adjustments and other minor servicing activities which take place during normal operation may be exempt from LOTO if the activity is routine, repetitive, and integral to the use of the equipment for production purposes, provided that the work is performed using alternative measures which provide effective employee protection.
    - 1910.213-190.219: Machine Specific Regulations
  - Subpart J: General Environment Controls
    - 1910.147: The Control of Hazardous Energy (Lockout/Tagout)
## Machine Safety Standards
### NFPA 79

<table>
<thead>
<tr>
<th>Original NFPA 79 1997 - Restricted machine safety to electromechanical devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6.3 Where a Category 0 stop is used for the emergency stop function, it shall have only hardwired electromechanical components. In addition, its operation shall not depend on electronic logic (hardware or software).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NFPA 79 2002 – Allowed the use of safety PLC in safety-related.</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3.4 Use in Safety-Related Functions. Software and firmware-based controllers to be used in safety-related functions shall be listed for such use. [Annex to NFPA 79 2002, A.11.3.4 IEC 61508]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NFPA 79 2007 – Allowed drives as a final switching device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.5.4.1.4 Drives or solid-state output devices designed for safety-related functions shall be allowed to be the final switching element, when designed according to relevant safety standards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NFPA 79 2012 – Allowed the use of cableless control</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.7.1* General. Cableless control (e.g., radio, infrared) techniques for transmitting commands and signals between a machine control system and operator control station(s) shall meet the requirements of 9.2.7.1.1 through 9.2.7.1.4.</td>
</tr>
</tbody>
</table>
## Machine Safety Standards Overview

<table>
<thead>
<tr>
<th>Standards</th>
<th>Descriptions</th>
<th>USA</th>
<th>EU</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Organization for Standardization</td>
<td>ISO 13849-1, FS, Appl. specific std (PL), H-P ISO 13849-2, FS, Validation ISO 12100, FS, Risk Assessments</td>
<td>X</td>
<td>X</td>
<td>More guidance with safety calculations with the Safety Evaluation Tool</td>
</tr>
<tr>
<td>Occupational Safety and Health Administration</td>
<td>OSHA 29 CFR 1910, Subpart O, Machinery and Machine Guarding Safety OSHA 29 CFR 1910.147 Control of Hazardous Energy (Lockout / Tagout)</td>
<td>X</td>
<td>-</td>
<td>Siemens Safety Solutions Tested and certified by NRTL’s (as per OSHA’s requirement)</td>
</tr>
<tr>
<td>American National Standards Institute</td>
<td>ANSI B11 Series – 2007–2010</td>
<td>X</td>
<td>-</td>
<td>To be followed for application specific standards</td>
</tr>
<tr>
<td>Underwriters Laboratories</td>
<td>UL NRGF covers ANSI / UL 508 / 1998 / NFPA79 and IEC 61508 Also new UL Functional Safety mark like TUV</td>
<td>X</td>
<td>-</td>
<td>New UL Functional Safety Mark and recognition (similar to TUV-NRTL certification)</td>
</tr>
<tr>
<td>Robotics Industries Association</td>
<td>ANSI / RIA R15.06-2012, ANSI / RIA / ISO 10218-1-2007</td>
<td>X</td>
<td>X</td>
<td>Required for all robotic machine safety applications</td>
</tr>
<tr>
<td>Canadian Standards Association</td>
<td>CSA Z434: Safety requirements for robots and robot systems</td>
<td>-</td>
<td>-</td>
<td>Canadian requirement.</td>
</tr>
</tbody>
</table>
The EN 954-1 (CAT B, CAT 2, CAT3 & CAT4) was replaced by ISO13849-1:2006 because programmable electronic systems were considered insufficiently and the time response (e.g. testing intervals, life cycles) and the failure probability of components were not considered.

18 December 2009: [EN 954-1 extension confirmed as two years], until 31 December 2011.

Two important standards:


ISO 13849-1:2006 builds on the “categories” of safety structure, uses the term “performance level” (PL), and then uses the alphabet, PLa through Ple.

IEC 62061 builds on the foundation of the structure or what is called “Hardware Fault Tolerance” and uses the term “safety integrity level” (SIL), Only three SILs apply to machine systems: SIL1, SIL2 and SIL3

A third element, diagnostics, not new at all, is added to the picture to give the safety system designer more flexibility to achieve the safety requirements. Putting these three elements together yields a time-sensitive level of integrity in a safety system.
Machine Safety
Comparison of ISO 13849-1 and IEC 62061

<table>
<thead>
<tr>
<th>Feature</th>
<th>EN 954-1</th>
<th>EN ISO 13849-1</th>
<th>IEC 61508</th>
<th>EN 62061</th>
</tr>
</thead>
<tbody>
<tr>
<td>For manufacturers of</td>
<td>Machinery</td>
<td>Machinery</td>
<td>Components</td>
<td>Machinery</td>
</tr>
<tr>
<td>Technology</td>
<td>Also non-electrical</td>
<td>Also non-electrical</td>
<td>Electrical</td>
<td>Electrical</td>
</tr>
<tr>
<td>Concept:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety function</td>
<td>Parts</td>
<td>Total</td>
<td>Total</td>
<td>Total</td>
</tr>
<tr>
<td>Required safety level</td>
<td>Categories</td>
<td>PL&lt;sub&gt;r&lt;/sub&gt;</td>
<td>SIL</td>
<td>SIL</td>
</tr>
<tr>
<td>Probability of failure</td>
<td>---</td>
<td>PFH&lt;sub&gt;D&lt;/sub&gt;</td>
<td>PFH&lt;sub&gt;D&lt;/sub&gt;</td>
<td>PFH&lt;sub&gt;D&lt;/sub&gt;</td>
</tr>
<tr>
<td>Use of programmable electronics (PLC, …)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Presumption of conformity, if applied</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Machine Safety
## Comparison of ISO 13849-1 and IEC 62061

The SIL and/or PL safety levels define just how reliable a safety system must be:

<table>
<thead>
<tr>
<th>Performance Level (PL)</th>
<th>Mean probability of one dangerous failure per hour</th>
<th>SIL as per IEC61508 and EN IEC 62061</th>
<th>Maximum acceptable safety system failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>$\geq 10^{-5}$ to $&lt;10^{-4}$</td>
<td>-</td>
<td>One risk failure every 10,000 hours</td>
</tr>
<tr>
<td>b</td>
<td>$\geq 3 \times 10^{-6}$ to $&lt;10^{-5}$</td>
<td>1</td>
<td>One risk failure every 1,250 days</td>
</tr>
<tr>
<td>c</td>
<td>$\geq 10^{-6}$ to $&lt;3 \times 10^{-6}$</td>
<td>2</td>
<td>One risk failure every 115.74 years</td>
</tr>
<tr>
<td>d</td>
<td>$\geq 10^{-7}$ to $&lt;10^{-6}$</td>
<td>3</td>
<td>One risk failure every 115.74 years</td>
</tr>
<tr>
<td>e</td>
<td>$\geq 10^{-8}$ to $&lt;10^{-7}$</td>
<td>4</td>
<td>One risk failure every 1,157.41 years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology</th>
<th>EN ISO 13849-1</th>
<th>EN 62061</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hydraulic</td>
<td>Applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Pneumatic</td>
<td>Applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Mechanical</td>
<td>Applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Electrical</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>Electronics</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
</tbody>
</table>

- When a safety system is correctly used - its **probability of failure is the same as the probability of a hazard**.
- This means that IEC 62061 and ISO 13849 define a **quantitative** risk and therefore go further than EN 954-1.
## Machine Safety
Comparison of different safety standards per ANSI B11.0:2010

<table>
<thead>
<tr>
<th>Risk Reduction</th>
<th>System Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column 1</td>
<td>Column 2</td>
</tr>
<tr>
<td>Highest: Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that a single fault in any of these parts does not lead to a loss of the safety function, and the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to loss of the safety function.</td>
<td>Highest: Redundancy w/ continuous self-checking (e.g., Dual channel w/ continuous monitoring)</td>
</tr>
<tr>
<td>Intermediate / High: Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that a single fault in any of these parts does not lead to the loss of the safety function, and whenever reasonably practicable, the single fault is detected.</td>
<td>Intermediate / High: Redundancy w/ self-checking upon start-up (e.g., Dual channel w/ monitoring at cycle/start-up)</td>
</tr>
<tr>
<td>Low / Intermediate: Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.</td>
<td>Low / Intermediate: Redundancy that may be manually checked (e.g., Dual channel w/ optional manual monitoring)</td>
</tr>
<tr>
<td>Lowest: Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.</td>
<td>Lowest: Single channel</td>
</tr>
<tr>
<td>B: SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.</td>
<td>R3B / R4 (Simple)</td>
</tr>
</tbody>
</table>

*Taken from ANSI B11.0:2010*
Two standards: ISO 13849 and IEC 62061 are overlapping and can be used alternatively.

What do? Optimizing or to strike a new path?

Optimizing:
- ISO 13849-1 – Amendment is still not practice-oriented

New Concepts:
- Working Draft 17305
- The planned Merging of both standards ISO 13849 and IEC 62061
Status of ISO/IEC 17305
Why improving & merging? – the most relevant reasons for -

• Need for a **simple/practical standard**, with practical examples to be added:
  More explanation/guidance (to avoid deviating interpretation)

• The request to have **more flexibility** for the quantification of the risk estimation seems to be interlinked with the problems reported with regard to the determination of the required PL or SIL

• The ideas behind **“functional safety” and “safety related control system”** need to be clarified

• Particular problems with **DC, CCF and validation**:
  Those parts need more guidance/clarifications
### Status of ISO/IEC 17305
#### Design of Safety Control System (SCS)

<table>
<thead>
<tr>
<th>Activities</th>
<th>Safety Manager</th>
<th>Construction</th>
<th>Electric</th>
<th>Commissioning</th>
<th>Ergonomics</th>
<th>...</th>
<th>QM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety-Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mounting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Documentation
- Safety Plan, Verification plan...
- Risk Analysis
- Specification, Manuals
- Data sheets, ...
- Wiring Diagrams
- Software Documentation
- Test Reports
- Verification Reports
- Technical Documentation

Unrestricted © Siemens Industry, Inc. 2014-2015 All rights reserved.
Safety Related Parts of Control System
Basic Implementation Procedure – Risk Reduction

Steps to be performed by the machine manufacturer

• 1 Risk assessment
• 2 Risk reduction
  - Step 1: Safe design
  - Step 2: Technical protective measures
  - Step 3: User information on residual risks
• 3 Validation of the machine
• 4 Placing the machine on the market

Technical documentation

Each step must be comprehensibly documented:
  - Procedure and results
  - Test strategy and test results
  - Responsibilities, …
Technical protective measures

• A safety function must be defined for each hazard that cannot be eliminated by design

• Safety functions can be performed by safety systems

Example: Safety function, without safety system

Access to the hazardous location is permanently prevented (fixed mechanical cover, …)

Example: Safety function, with safety system

“When the protective cover is opened during normal operation, the motor must be switched off.”
Safety Related Parts of Control System
Step 2: Technical Protective Measures

Safety system
• Performs safety functions
• Consists of subsystems

Subsystems of a safety system
• Detecting (position switch, light curtain, …)
• Evaluating (fail-safe controller, safety switching device, …)
• Reacting (contactor, frequency converter, …)
Relevant standards for designing and realizing safety systems for machinery

EN 954-1 (was valid until the end of 2011)

EN ISO 13849-1

EN 62061 (identical to IEC 62061)
Step 2: Technical Protective Measures

Basic procedure for each safety function

a) Specifying the safety function

b) Determining the **required** safety level

c) Designing the safety function

d) Determining the **achieved** safety level

e) Realizing and testing the safety function
Boundary conditions of the safety function

- Hazard to be prevented on the machine
- Affected persons on the machine
- Concerned operating modes of the machine
- ...

Requirements for the functionality of the safety function

- Functional description of the safety function
- Required reaction time
- Reaction to faults
- Number of operations for electromechanical components
- ...

Safety Related Parts of Control System
Step 2: Technical Protective Measures, a) Specifying the Safety Function
Significance of the required safety level

The required safety level is a measure for the reliability of the safety function.

The required safety level depends on:

- Severity of the injury
- Frequency / exposure time
- Possibility of avoiding

The more severe the injury and the more probable its occurrence, the higher the required safety level.

EN 62061 and ISO 13849 show procedures for determining the required safety level.
### Safety Related Parts of Control System

#### Step 2: Technical Protective Measures, b) Determining the reqd. Safety Level

#### Specification according to EN 62061: SIL 1 to SIL 3

<table>
<thead>
<tr>
<th>Frequency / exposure time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fr</td>
</tr>
<tr>
<td>Less than 1 hour</td>
</tr>
<tr>
<td>1 h to 1 day</td>
</tr>
<tr>
<td>1 day to 2 weeks</td>
</tr>
<tr>
<td>2 weeks to 1 year</td>
</tr>
<tr>
<td>More than 1 year</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probability of occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pr</td>
</tr>
<tr>
<td>Frequently</td>
</tr>
<tr>
<td>Likely</td>
</tr>
<tr>
<td>Possible</td>
</tr>
<tr>
<td>Rarely</td>
</tr>
<tr>
<td>Negligible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Possibility of avoiding</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
</tr>
<tr>
<td>Impossible</td>
</tr>
<tr>
<td>Possible</td>
</tr>
<tr>
<td>Likely</td>
</tr>
</tbody>
</table>

#### Severity of the injury

<table>
<thead>
<tr>
<th>Class Cl = Fr + Pr + P</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 to 4</td>
</tr>
<tr>
<td>5 to 7</td>
</tr>
<tr>
<td>8 to 10</td>
</tr>
<tr>
<td>11 to 13</td>
</tr>
<tr>
<td>14 to 15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity of the injury Se</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

- **Irreversible**: E.g., losing limb(s)
- **Irreversible**: E.g., broken limb(s)
- **Reversible**: E.g., requiring attention from a medical practitioner
- **Reversible**: E.g., requiring first aid

Unrestricted © Siemens Industry, Inc. 2014-2015 All rights reserved.
Safety Related Parts of Control System
Step 2: Technical Protective Measures, b) Determining the reqd. Safety Level

Specification according to EN ISO 13849: PLr a to PLr e

<table>
<thead>
<tr>
<th>Severity of the injury</th>
<th>Se</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irreversible injury</td>
<td>Se2</td>
</tr>
<tr>
<td>Reversible injury</td>
<td>Se1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency / exposure time</th>
<th>Fr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent up to continuous / long</td>
<td>Fr2</td>
</tr>
<tr>
<td>Seldom up to quite often / short</td>
<td>Fr1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Possibility of avoiding</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scarcely possible</td>
<td>P2</td>
</tr>
<tr>
<td>Possible</td>
<td>P1</td>
</tr>
</tbody>
</table>

Unrestricted © Siemens Industry, Inc. 2014-2015 All rights reserved.
### Requirements of the safety levels: Probability of failure

EN 62061 and EN ISO 13849 describe requirements for the maximum permissible probability of failure of the safety function:

- Probability of dangerous failure per hour $PFH_D$
- The higher the safety level, the lower the required $PFH_D$

<table>
<thead>
<tr>
<th>Safety Level</th>
<th>$PL_r$</th>
<th>$PFH_D$ (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>$PL_r a$</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td></td>
<td>$PL_r b$</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td></td>
<td>$PL_r c$</td>
<td>$3 \times 10^{-6}$</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$PL_r d$</td>
<td>$10^{-7}$</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$PL_r e$</td>
<td>$10^{-8}$</td>
</tr>
</tbody>
</table>

$PFH_D$ decreases

- Not more than 1 dangerous failure of the safety function in **10 years**
- Not more than 1 dangerous failure of the safety function in **100 years**
- Not more than 1 dangerous failure of the safety function in **1000 years**
Requirements of the safety levels: Safety system

EN 62061 and EN ISO 13849 describe requirements for the reliability of safety systems:

<table>
<thead>
<tr>
<th></th>
<th>PL_r a</th>
<th>PL_r b</th>
<th>PL_r c</th>
<th>PL_r d</th>
<th>PL_r e</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIL 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIL 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Increasing requirements for the reliability of safety systems

All phases of the lifetime of a machine are considered:

- From planning
- to shutdown
Requirements of the safety levels: Safety system

The requirements concern:

• Engineering (depends strongly on the required safety level)
• Procedure

Requirements for **engineering**: (low → high safety level)

• Hardware structure (one-channel → two-channel)
• Fault detection capability (none → comprehensive diagnostics)
• Reliability of components (increasing)

Requirements for the **procedure**:

• Project management
• Test concept
• Technical documentation, …
Objective of the design

The safety system performing the safety function must meet the requirements of the necessary safety level (SIL, PL_r).

Example

Safety function: “When the protective cover is opened during normal operation, the motor must be switched off.”

Required safety level: SIL 3 or PL_r e
Safety Related Parts of Control System
Step 2: Technical Protective Measures, d) Determining achieved Safety Level

Design review
Can the required safety level (SIL, PLr) be achieved?

Basic procedure
Assessment of the individual subsystems
- Achieved safety level (SILCL, PL)
- Probability of failure PFH_D

Assessment of the safety system
- Achieved safety level (SILCL, PL):
  Normally, the lowest achieved safety level of a subsystem determines the achieved safety level of the safety system.
- Probability of failure PFH_D: Total of PFH_D of the subsystems
- Achieved safety level of the safety system (SILCL, PL) = required safety level of the safety function (SIL, PLr)?
Safety Related Parts of Control System
Step 2: Technical Protective Measures, d) Determining achieved Safety Level

Assessment of the subsystems

Safety-relevant characteristics of a subsystem:
• Achieved safety level (SILCL, PL)
• Probability of failure PFH\textsubscript{D}

Finished subsystem
• Characteristics and certificates from the manufacturer

Designed subsystem
• Characteristics have to be calculated
• EN 62061 and EN ISO 13849 show how
User information warns of **residual risks**

User information does **not** replace

- safe design
- technical protective measures

Examples:

- Warnings in the operating instructions
- Special work instructions
- Icons
- Personal protective equipment
# Document the measures

## External and internal documentation

### External technical documentation

For customer

- Operating instructions with description for intended use
- Necessary circuit diagrams
- Safety guidelines
- Where appropriate, servicing manual
- EC certificate of conformity

### Internal technical documentation

Stays with manufacturer

- Description of machine
- Overall drawing
- Full detailed drawing
- Documents on risk assessment
- Applicable standards and other technical specifications
- Technical reports with results on inspections/ tests carried out
- Operating instructions
- Copy of EC certificate of conformity
- Declaration of incorporation / assembly instructions for partly completed machinery
Machine Safety Standards

SET – Tool to calculate safety levels
Safety Evaluation Tool SET

**Safety Evaluation Tool (SET):**

- **Online tool for determining safety levels**
  of safety functions according to:
  - EN ISO 13849-1 (Performance Level, PL)
  - EN 62061 (Safety Integrity Level, SIL).

- **Detailed configuration of the safety functions**
  - Emergency stop, fence, etc.

- **This tool is one of a kind**
  - Product information (PFHd-, SIL- and PL-values) of Siemens components are used directly in the safety-calculations.
  - Input of components from ‘Third-Party-Manufacturers’ is also possible.

- **Result**
  - Ready made TÜV-certified and compliant safety functions.
  - Time saving: Less manual calculations required.
  - Project documentation for the technical dossier of the machine.

**Free use of the online tool:** [www.siemens.com/safety-evaluation-tool](http://www.siemens.com/safety-evaluation-tool)
Safety Evaluation Tool
Risk graph for determining the required SIL/PL level

Integrated risk graph for determining the required SIL/PL level

Risk graph for PL (EN ISO 13849-1)
Risk graph for SIL (EN 62061)
Safety Evaluation Tool

Basic steps

Create a safety function

<table>
<thead>
<tr>
<th>Detection</th>
<th>Evaluation</th>
<th>Reaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image of detection]</td>
<td>[Image of evaluation]</td>
<td>[Image of reaction]</td>
</tr>
</tbody>
</table>

SIEMENS
Safety Evaluation Tool
Basic steps

Create components

<table>
<thead>
<tr>
<th>Detection</th>
<th>Evaluation</th>
<th>Reaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Detection Image]</td>
<td>![Evaluation Image]</td>
<td>![Reaction Image]</td>
</tr>
</tbody>
</table>
Safety Evaluation Tool
Basic steps

Enter data for components
Safety Evaluation Tool
Basic steps

Repeat steps for the other components
## Safety Evaluation Tool
### Basic steps

<table>
<thead>
<tr>
<th>Order number</th>
<th>Max. service life (in years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>35E53</td>
<td>20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>More order numbers</th>
<th>DTof (operation cycles)</th>
<th>MTTfd (in years)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5,000,000.00</td>
<td>5.797.76 (high)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of operations/test interval (switching cycles)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Per hour</td>
</tr>
</tbody>
</table>

### Consideration of safety integrity acc. to ISO 13849-1

<table>
<thead>
<tr>
<th>CCF (points)</th>
<th>Estimate CCF</th>
<th>PL</th>
<th>PL d</th>
</tr>
</thead>
<tbody>
<tr>
<td>x&lt;65</td>
<td></td>
<td>PL</td>
<td>PL d</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consideration of safety integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety function</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>PL</td>
</tr>
<tr>
<td>PL d</td>
</tr>
</tbody>
</table>

PLd = 4.29 E-08

### Show overall result
Safety Evaluation Tool

Basic steps

Generate documentation and save as PDF
## Major Software-tools available to simplify and speed up the calculations:

<table>
<thead>
<tr>
<th>SISTEMA</th>
<th>Safety Evaluation Tool (SET)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Integrity software tool for evaluation of machine applications available at no charge</td>
<td>The SET for the IEC 62061 &amp; ISO 13849-1 standards takes you to your goal faster.</td>
</tr>
<tr>
<td>Tool for easy application of control standard EN ISO 13849-1</td>
<td>This TÜV-tested free-to-use, online tool supports the fast &amp; reliable assessment of your machine’s safety functions</td>
</tr>
<tr>
<td>Modeling tool for designated architectures &amp; automated calculation of reliability values as per 13849-1</td>
<td>Automatic calculation in accordance with IEC 62061 &amp; ISO 13849-1, certainty regarding compliance.</td>
</tr>
<tr>
<td>SISTEMA Cookbooks available</td>
<td>Faster online access to current product data</td>
</tr>
<tr>
<td>Printable summary document</td>
<td>Standard-compliant report, which can be integrated in the documentation as a proof of safety</td>
</tr>
</tbody>
</table>

Siemens Safety Integrated
Evolution of Machine Safety

**FUTURE**
Focus on Machine Productivity & Safety
- Integrated Safety
- Intelligent safety devices
- Productivity Enhancing

**PAST**
Focus on Machine Productivity
- Safety cumbersome
- Safety Often bypassed
- Increased injury & risks
- Standards often not implemented
- LOTO only

**PRESENT**
Focus on Machine Productivity & Safety
- Use of safety rated devices
- Increased focus on safety standards
- Safety Standards implemented & enforced
- Better diagnostics
Siemens Safety Integrated
Evolution of Safety Solutions

**FUTURE**
- Focus on Machine Productivity & Safety
- Integrated Safety
- Intelligent safety devices
- Productivity Enhancing

**PAST**
- Separate Automation controls
- Stand alone safety
- Hardwired safety
- Standards behind technology

**PRESENT**
- Acceptance of Safety PLC
  - for safety & non-safety functions
- Wide range of safety devices available
- Programmable Safety
Siemens Safety Integrated
Evolution of Safety Standards

FUTURE
- Global Standards
- ISO 17305 – Merging of
  - ISO 13849 & IEC 62061
- Partnerships between
  - IEC / ISO / ANSI

PRESENT
- Mix of National & Global Standards,
  - Implemented & enforced
- ANSI B11, NFPA 79
- ISO 13849, IEC62061

PAST
- Used only Nationally Recognized Standards
- ANSI B11
- NFPA 79
Machine Safety
Key Trends in Safety

• Globalization of Safety Control Standards – ISO/IEC
• Increased focus on Safety Design to Improve Productivity
• Merging of Standards. Ex. ISO 13849/IEC 62061
• Transition from Electro-Mechanical to Electronic Safety Controls
• Safety Technology Integrated into Standard Automation Hardware
• Integration of Standard Controls and Safety Controls
• Addition of Configurable and Programmable Safety Devices
• Addition of Safe Motion Technology
• Safety Networks
• Safety being transparent
Machine Safety
Use of Safety – Increased Overall Equipment Efficiency (OEE)

- Work productively while minimizing their risk of injury
- Enable design flexibility and increased diagnostics
- Increased likelihood that Standard Operating Procedures will be followed.
- Make machinery safer and easier to operate and maintain
- Reduce the motivation to bypass
Machine Safety Standards
Machine Safety Life-Cycle Support
Siemens Safety Integrated
Machine Safety Life-Cycle Support — USA

Siemens provides competent support throughout the entire machine safety lifecycle

**Support**
- Safety Consultants
- Safety Core Team
- Safety Validation

**Implementation**
- Siemens Solution Partners — Safety
- Safety Functional Examples
- Safety Training
- Risk Assessment Training

**Products and Solutions**
- Safety Products
- Safety Software
- Wireless Safety
- PC-Based Safety
- BMS

**Safety Education**
- Machine Safety Standards
- Safety Webinars
- Newsletter
- Safety White Papers
- Siemens Safety Website

**Compliance**
- OSHA Website
- Consensus Standards
- Risk Assessment Standard
- Safety Evaluation Tool - SET
Machine Safety Standards

Thank you for your time.
DISCLAIMER / TERMS OF USE:

THE INFORMATION PROVIDED HEREIN IS PROVIDED AS A GENERAL REFERENCE REGARDING THE USE OF THE APPLICABLE PRODUCTS IN GENERIC APPLICATIONS. THIS INFORMATION IS PROVIDED WITHOUT WARRANTY. IT IS YOUR RESPONSIBILITY TO ENSURE THAT YOU ARE USING ALL MENTIONED PRODUCTS PROPERLY IN YOUR SPECIFIC APPLICATION. ALTHOUGH THIS PRESENTATION STRIVES TO MAINTAIN ACCURATE AND RELEVANT INFORMATION, THERE IS NO OFFICIAL GUARANTEE THAT THE INFORMATION PROVIDED HEREIN IS ACCURATE. IF YOU USE THE INFORMATION PROVIDED HEREIN IN YOUR SPECIFIC APPLICATION, PLEASE DOUBLE CHECK ITS APPLICABILITY AND BE ADVISED THAT YOU ARE USING THIS INFORMATION AT YOUR OWN RISK. THE PURCHASER OF THE PRODUCT MUST CONFIRM THE SUITABILITY OF THE PRODUCT FOR THE INTENDED USE, AND_ASSUME ALL RISK AND LIABILITY IN CONNECTION WITH THE USE.