



the standard in safety

Functional Safety: What It Is, Why It's Important And How to Comply

November 11, 2010

Functional Safety

- **Industry experts define:**
- **Functional safety**
 - What it is
 - Why it's important
 - How to comply with standards and regulations
- **Sponsor: Underwriters Laboratories**
- **Moderator: Gary Mintchell, Automation World, Editor-in-chief**

Presenters

Kevin Connelly

Underwriters Laboratories

Industry Manager, Power & Controls,
Functional Safety



Thomas Maier

Underwriters Laboratories

Principal Engineer, Functional Safety



Webcast Agenda

- **Overview of Functional Safety and Safety Assessments: Thomas Maier**
- **Functional Safety Demand Drivers: Kevin Connelly**
- **Common Functional Safety Standards: T. Maier**
- **Functional Safety Program and UL Listing Mark: K. Connelly**
- **Call-to-Action**
- **Live “Question and Answer” Session**

What is Functional Safety?

Functional Safety is part of the overall safety of a system that depends on the correct execution of specific functions.

Here is the exact definition according to IEC 61508:

- **“part of the overall safety relating to the *EUC* and the *EUC control system* which depends on the correct functioning of the *E/E/PE safety-related systems*, other technology safety-related systems and external *risk reduction facilities*”**

Why is there something called Functional Safety?

Functional safety as a property has always existed, of course.

Functional Safety, by definition, is not specific to any one technology.

But Functional Safety is not only a property, it has evolved into a technical term, and an engineering discipline. Standards were developed. Why?

- **Functional Safety as a term and as an engineering discipline have emerged with the advent of complex programmable electronics.**
 - because of the particular challenges involved with this technology when it is to implement safety functions.

Functional Safety as per IEC 61508

Challenges addressed by IEC 61508

- System safety
 - => Hazard and Risk Analysis
- System and product life-cycle
 - => Functional Safety Management
- Hardware random failures
 - => Redundancy, diversity, diagnostics, reliability
- Systematic failures
 - => V-model
 - => Methods and techniques for fault avoidance

EUC – E/E/PE System – Subsystems – Elements

IEC 61508 mandates an "overall" safety approach, could also be referred to as a

- System safety approach or
- Holistic approach (accounts also for the whole life cycle of a system)

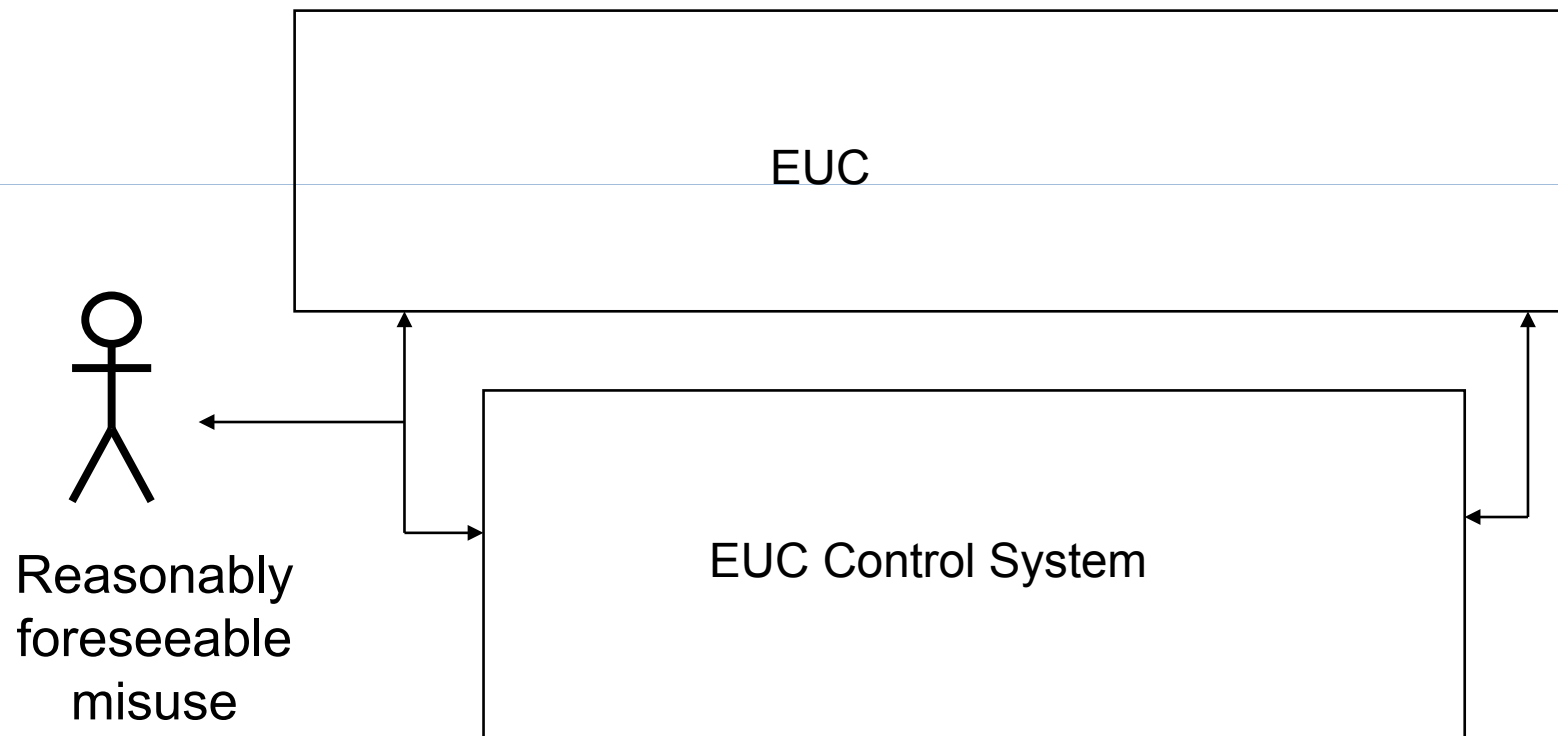
**The "system" is in IEC 61508 represented by the "EUC",
Equipment Under Control, plus the "EUC Control System"**

"EUC Control System":

- causes the EUC to operate in the desired manner
- includes input devices and final elements
- The EUC control system is separate and distinct from the EUC

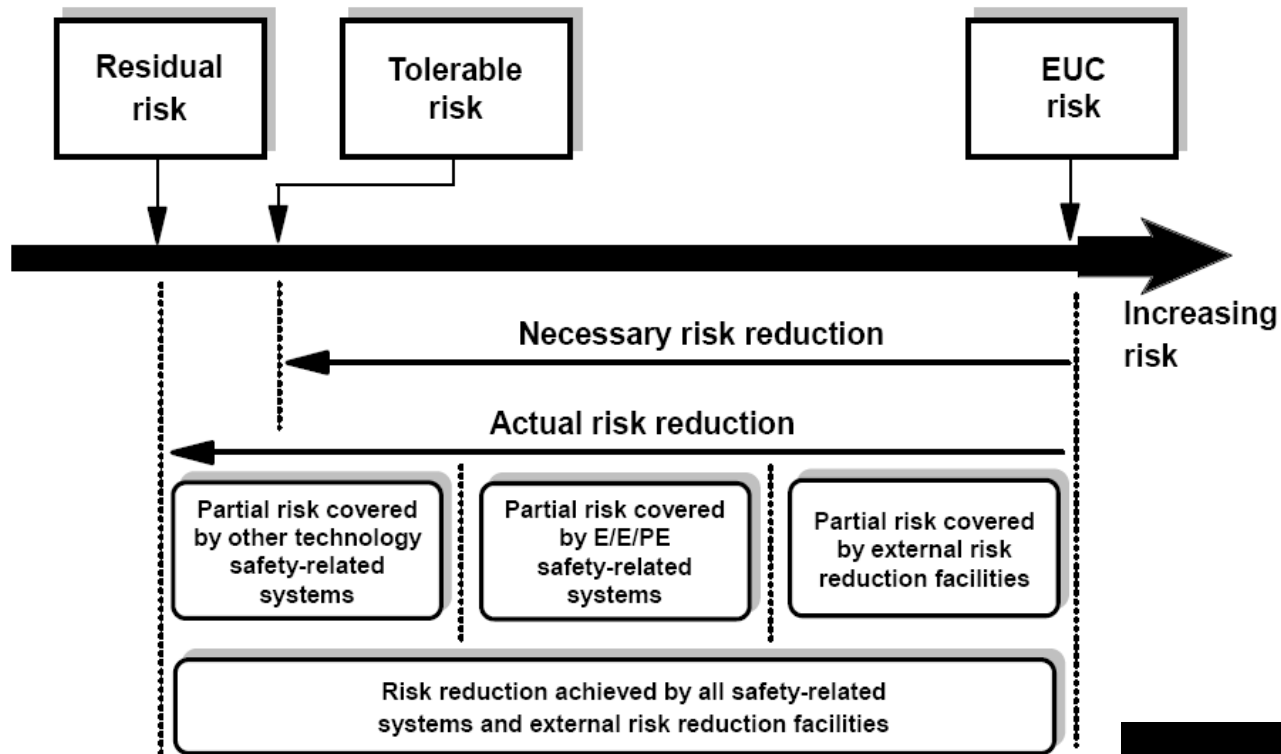
EUC and EUC Control System

- The "system" in IEC 61508 terms:



E/E/PE Safety-related System and Risk Reduction

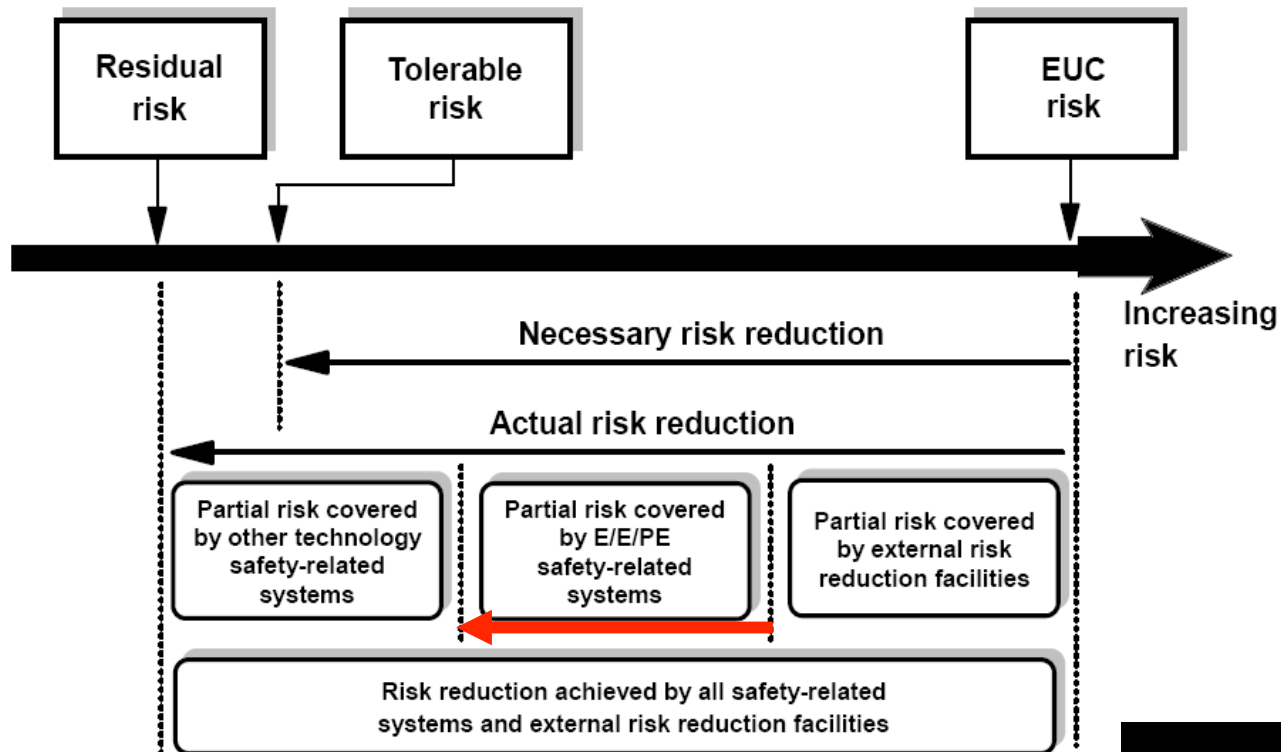
EUC (+ EUC control system) poses risk, E/E/PES contributes to reduce risk below a tolerable level



IEC 61508-5, Figure A.1

E/E/PE Safety-related System and Risk Reduction

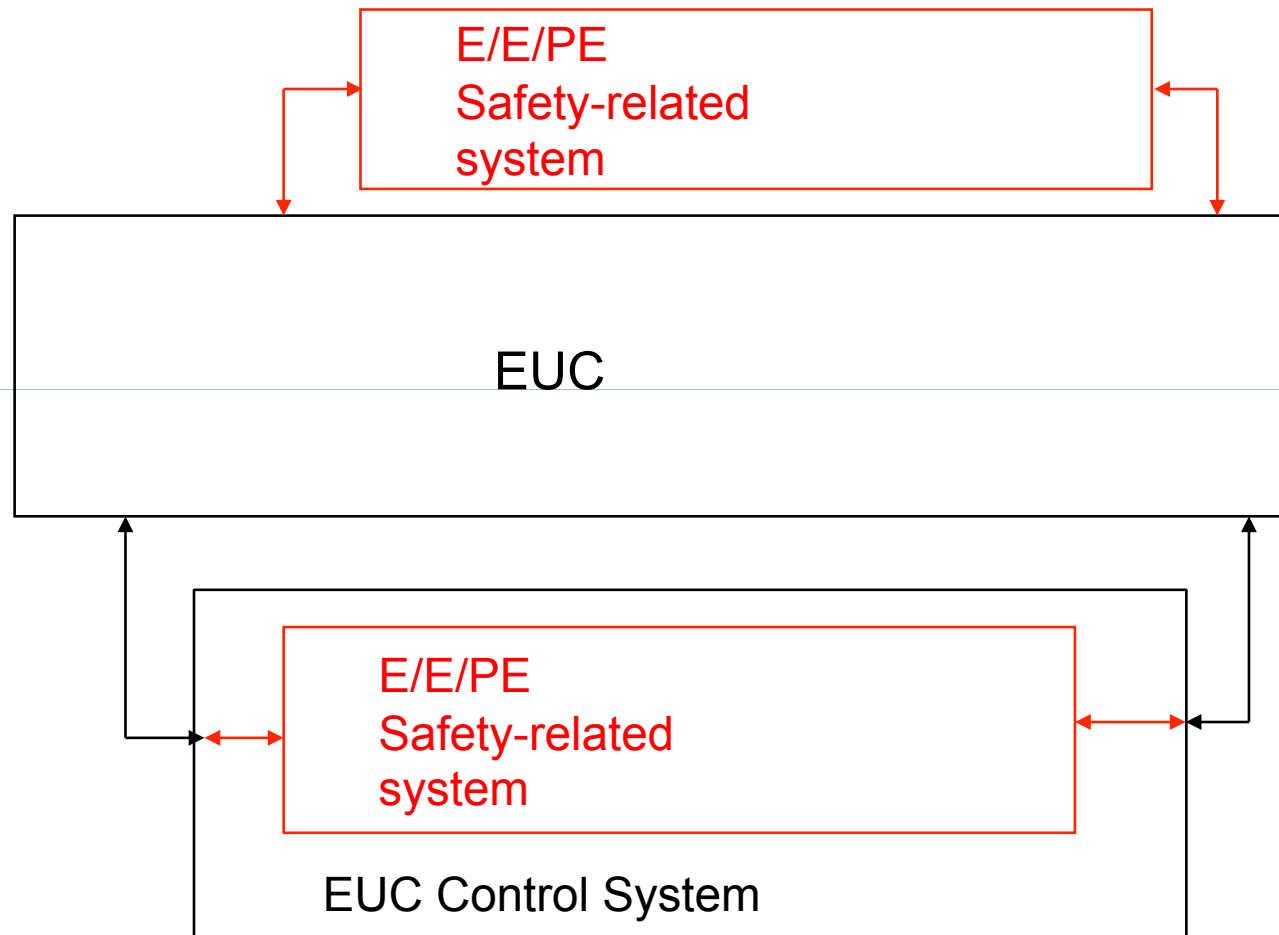
EUC (+ EUC control system) poses risk, E/E/PES contributes to reduce risk below a tolerable level



**Target failure measure =>
SIL (SIL1 ... SIL4)**

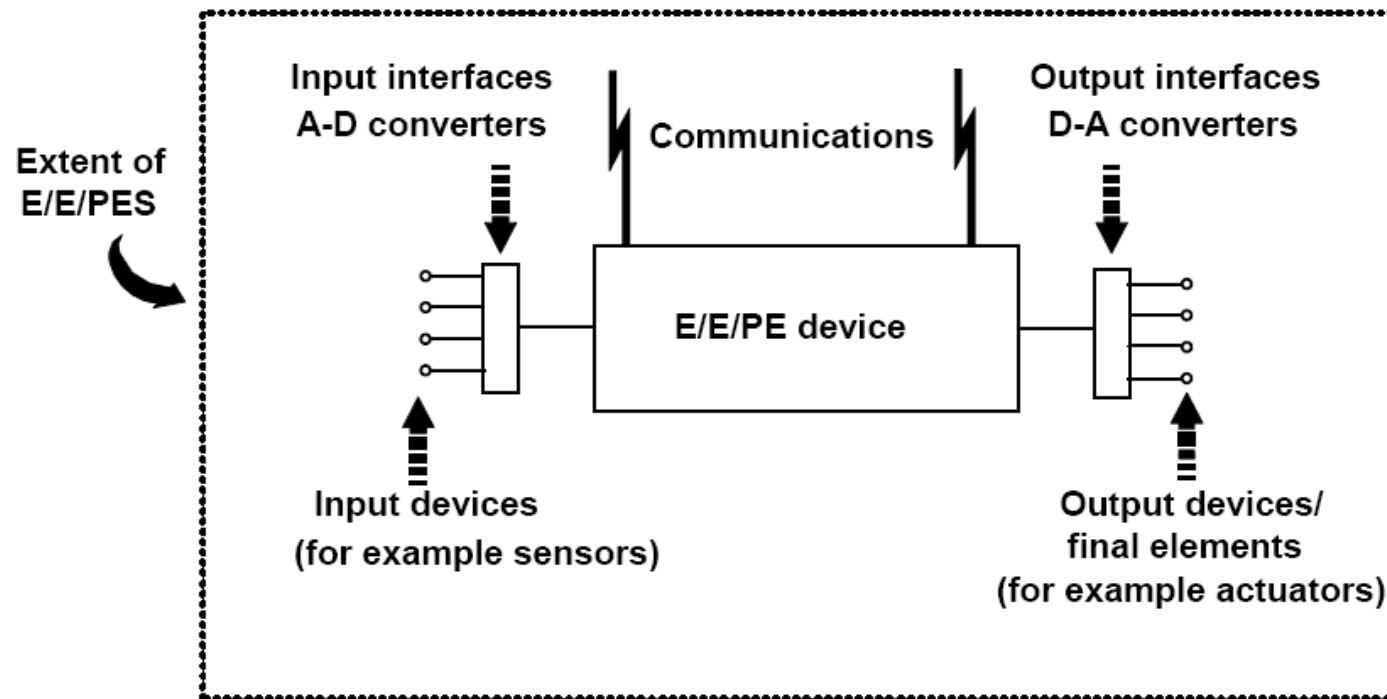
IEC 61508-5, Figure A.1

EUC – EUC Control System – E/E/PE System



E/E/PE System and Subsystems

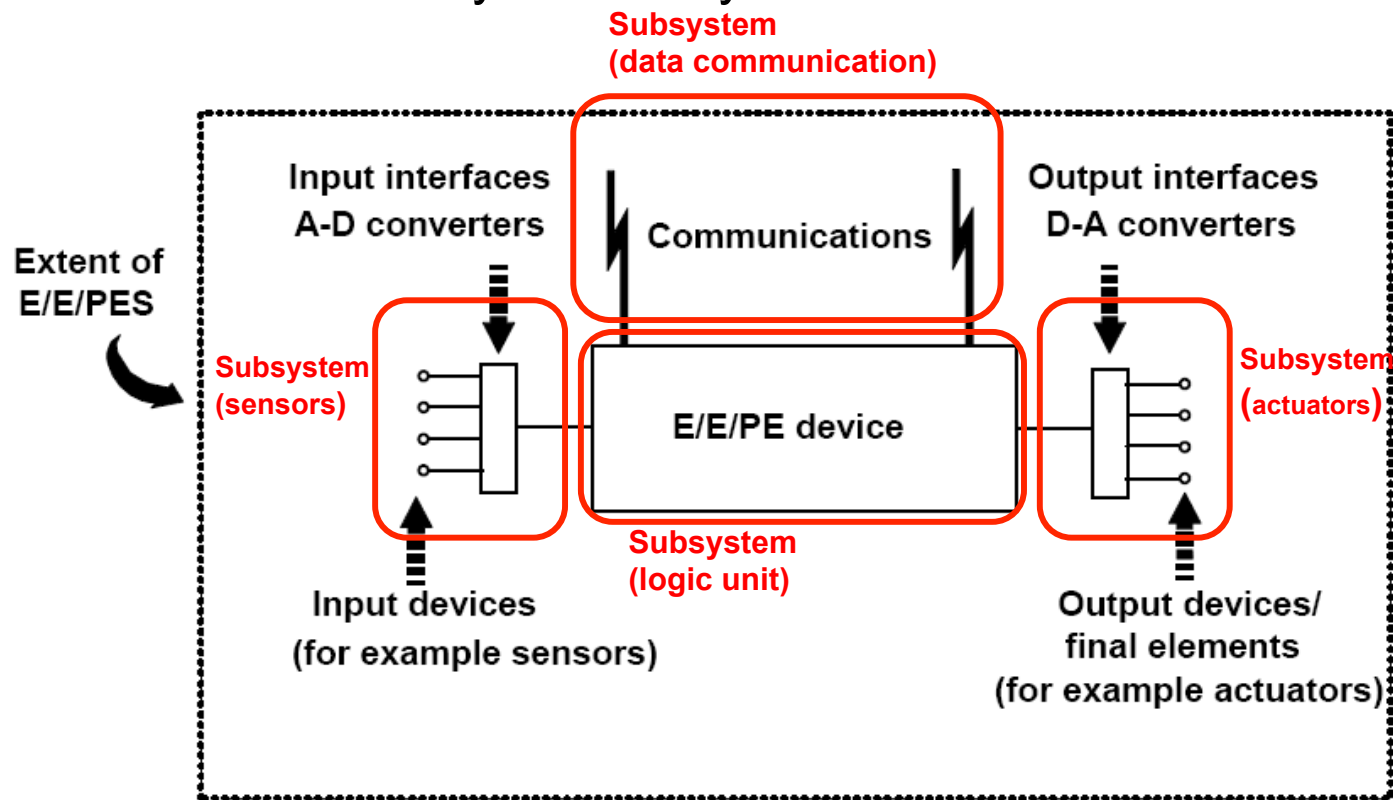
- In most cases, the FS products certified by UL will be sub-systems of an E/E/PE safety-related system.



IEC 61508-4, Figure 3

E/E/PE System and Subsystems

- In most cases, the FS products certified by UL will be sub-systems of an E/E/PE safety-related system.



IEC 61508-4, Figure 3

Demand Drivers for Functional Safety

Why evaluate your product/system for functional safety?

- A functional safety assessment determines whether your products meet standards and performance requirements created to protect against potential risks, including injuries and even death.
- Compliance is driven by customer requirements, legislation, regulations, and insurance demands

Demand Drivers for Functional Safety

Customer Requirements

- Customers may demand functional safety evaluation before purchasing equipment

Market Acceptance

- Having a functional safety certification maintains a product's competitiveness in the marketplace

Legislation

- Legislative requirements, such as some European Directives, require a functional safety evaluation

Demand Drivers for Functional Safety

Regulations

- Some regulatory bodies, such as OSHA, require or encourage functional safety evaluation

Trade Unions

- Some unions require or encourage functional safety certified products in the workplace

Insurance companies

- Insurers may require a functional safety evaluation before equipment is installed in the workplace, or may provide discounted premiums for using products evaluated for functional safety

Common Functional Safety Standards

Standards play a key role in the Functional Safety evaluation and certification process.

Important to specify a published standard and safety rating for testing and evaluation:

- Safety Integrated Level (SIL) for IEC and EN standards
- Performance Level (PL) for ISO standards
- Class for UL standards

Next slides will explain some common functional safety standards

Common Functional Safety Standards

- **IEC 61508 Safety Related Systems (SIL)**
 - IEC 62061 Safety Related Systems specifically for machinery (SIL Claim Limit)
 - IEC 61511 Safety Related Systems specifically for process sector equipment (SIL)
 - IEC 61800-5-2 Safety Related Systems specifically for power drive systems (SIL Capability)
 - IEC 61496 Functional Safety for electro-sensitive products (SIL)
 - ISO/DIS 26262 Functional Safety of Road Vehicles (ASIL)
- **ISO 13849 Safety Related Systems specifically for machinery (Performance Level)**
- **EN 954 Safety of Machinery (Category)**
- **UL 1998 Software and programmable devices (Class)**
- **UL 991 Solid state controls (Failure In Time)**

SIL vs. PL: IEC 62061

For safety-related control systems in machine applications, there exist two sector specific standards, IEC 62061 and ISO 13849-1:

IEC 62061: “SRECS”

- Derived from IEC 61508, defines safety integrity in terms of SIL.
 - Applies also to subsystems of a SRECS, (“SIL Claim Limits”)
- Only SIL (CL) 1 ... 3.
 - SIL 4 usually not relevant for automation
- SIL (CL) consists therefore of the following parameters:
 - PFH (safety-related reliability)
 - HFT (degree of redundancy)
 - SFF (degree of diagnostic capabilities)
 - CCF (like IEC 61508’s β -factor, measure of susceptibility for common cause failures)

SIL vs. PL: ISO 13849-1

ISO 13849-1: “SRP/CS”

- Enhances predecessor EN 954-1 with IEC 61508 principles:
 - Quantitative approach to risk reduction
 - Addresses systematic failure avoidance
 - Self contained. Refers to IEC 61508-3 only for PL e and “Full Variability languages (FVL)” and if there is no SW diversity
- Safety integrity defined in terms of Performance Levels (PL)
 - For both complete SRP/CS or subsystems thereof
- Suggests a simplified approach
- PL consists of following parameters:
 - MTTFD (reliability measure per channel)
 - Category (as of EN 954-1, now a parameter)
 - DC (diagnostic coverage)
 - CCF (common cause failure, determined by point-score system)
 - PFH can be determined on basis of above parameters

SIL and PL: Compatible and Merging Together

- **New ISO/TR 23849** (also published as IEC/TR 62061-1):
 - Recognizes compatibility with respect to risk reduction
 - SRP/CS can be integrated in SRECS and vice versa
 - Differences in Functional Safety Management
 - Standards to be merged. 3, 4, 5 years?

Performance level (PL)	PFH_{Davg} [1/h]	Safety Integrity Level (SIL)
a	10^{-5} to $< 10^{-4}$	no special safety requirements
b	3×10^{-6} to $< 10^{-5}$	1
c	10^{-6} to $< 3 \times 10^{-6}$	1
d	10^{-7} to $< 10^{-6}$	2
e	10^{-8} to $< 10^{-7}$	3

UL Functional Safety Program

Announcing the new

UL Functional Safety Mark Program

**FUNCTIONAL
SAFETY**



**FUNCTIONAL
SAFETY**



UL Functional Safety Program

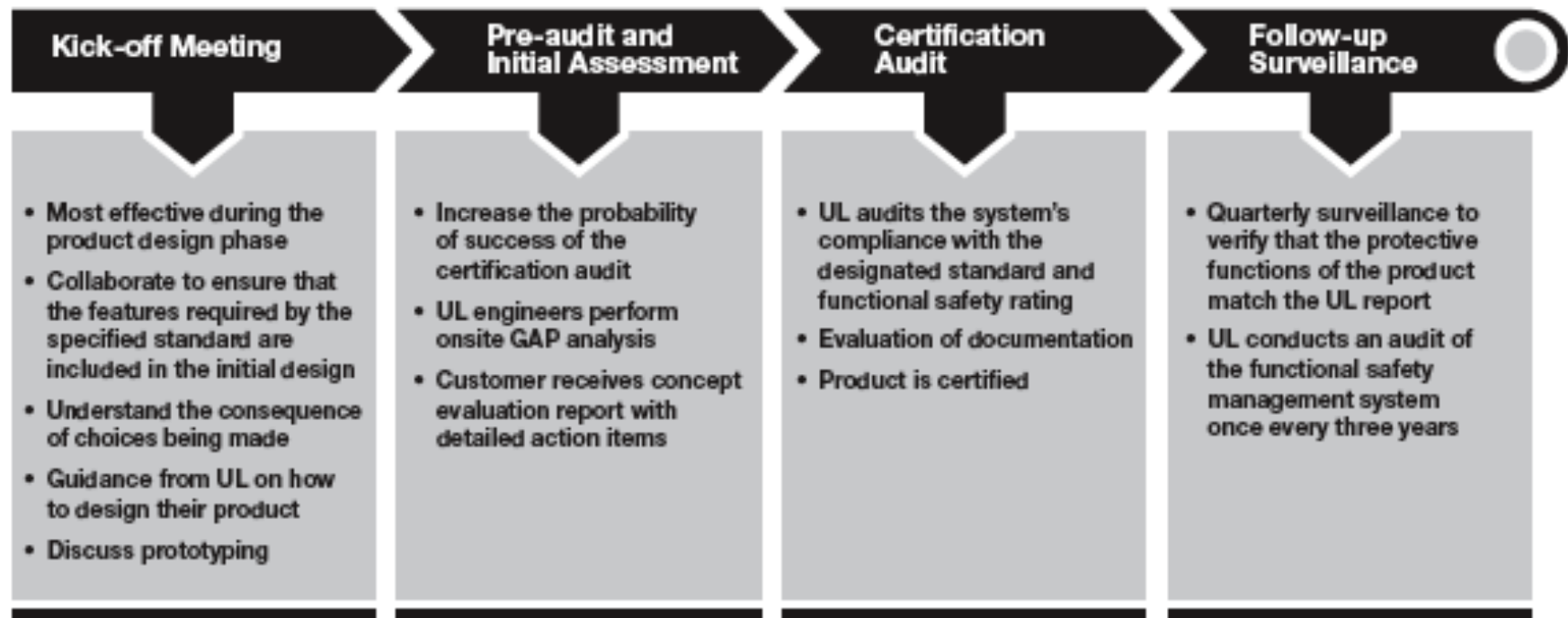
UL Deliverables:

- Advisory Services
- Functional Safety Listing Mark
- Functional Safety Component Recognition Mark
- Informative test reports
- 3-year Functional Safety Certificate
- Type examination reports

Functional Safety Certification Process

- Kick-off Meeting
- Pre-audit and Initial Assessment
- Certification Audit
- Review Current Functional Safety Management System
- Follow-up Surveillance

Functional Safety Certification Process



Functional Safety Certification Process

Kick-off Meeting

- Most effective during the product design phase
- Collaborate to ensure that the features required by the specified standard are included in the initial design
- Understand the consequence of choices being made
- Discuss prototyping
- Discuss Functional Safety Management System requirements

Functional Safety Certification Process

Pre-audit and Initial Assessment

- Increase the probability of success of the certification audit
- UL engineers perform onsite GAP analysis
- Customer receives concept evaluation report with detailed action items
- Continue review of Functional Safety Management System

Functional Safety Certification Process

Certification Audit

- UL audits the system's compliance with the designated standard and functional safety rating
- Evaluation of documentation
- Functional Safety Management System verified
- Product is certified

Functional Safety Certification Process

Follow-up Surveillance (FUS)

- Quarterly surveillance to verify that the protective functions of the product match the UL report
- UL conducts an audit of the functional safety management system once every three years

UL Advisory Services

**As part of the Functional Safety Certification program,
UL offers Advisory Services to:**

- Calculate or verify SIL, PL, class, etc.
- Develop validation plans
- Develop FMEA and FMEDA Analysis
- Draft Functional Safety Management and Integrated Test Plans
- Create a Safety Manual
- Develop Software FMEA and HAZOP Analysis

Call-to-Action

For more information, download the whitepaper:

“UL Functional Safety Mark Program”

found at www.ul.com/functionalsafety

and located under “Additional Resources” at the bottom of page.

Questions?

Kevin Connelly

Underwriters Laboratories

Industry Manager, Power & Controls,
Functional Safety



Thomas Maier

Underwriters Laboratories

Principal Engineer, Functional Safety

