
March 30, 2011
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.
Webcast Agenda

• Functional safety defined
• Functional safety standards you need to know
• How to achieve functional safety compliance by considering an automation systems as a whole and the environment within which they operate
• Critical role of the functional safety assessment to determine a system’s ability to meet standards, requirements, and protect against certain potential risks
• UL functional safety marks speed component integration while maintaining integrity of overall system’s safety level
• Overview of UL testing and certification programs
• “Question and Answer” session
Background

As complex systems have become increasingly prevalent in safety critical applications, industry has begun to recognize the need to manage the risks associated with such systems and their components - including the consideration of Functional Safety.
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 become increasingly necessary 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
Verification and Validation Throughout Development – The “V” Model

Source: Office of Operations Federal Highway Administration
http://ops.fhwa.dot.gov/publications/tptms/primer
System - Subsystem - Component

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)

Certification can occur at multiple levels:
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:

![Diagram showing EUC and EUC Control System with a person and reasonably foreseeable misuse]

- EUC
- EUC Control System
- Reasonably foreseeable misuse
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)
EUC – EUC Control System – E/E/PE System

E/E/PE Safety-related system

EUC

EUC Control System

E/E/PE Safety-related 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.
In most cases, the FS products certified by UL will be subsystems of an E/E/PE safety-related system.
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
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)
- ASME A17.1 (SIL)
- CSA 22.2 no 0.8 (Class)
- EN 50271 (SIL)
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

<table>
<thead>
<tr>
<th>Performance level (PL)</th>
<th>PFH_{Davg} [1/h]</th>
<th>Safety Integrity Level (SIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>10^{-5} to &lt; 10^{-4}</td>
<td>no special safety requirements</td>
</tr>
<tr>
<td>b</td>
<td>3 \times 10^{-6} to &lt; 10^{-5}</td>
<td>1</td>
</tr>
<tr>
<td>c</td>
<td>10^{-6} to &lt; 3 \times 10^{-6}</td>
<td>1</td>
</tr>
<tr>
<td>d</td>
<td>10^{-7} to &lt; 10^{-6}</td>
<td>2</td>
</tr>
<tr>
<td>e</td>
<td>10^{-8} to &lt; 10^{-7}</td>
<td>3</td>
</tr>
</tbody>
</table>
UL Functional Safety Program

Announcing the New UL Functional Safety Mark Program
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
- 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
- Guidance from UL on how to design their product
- Discuss prototyping

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

Certification Audit
- UL audits the system’s compliance with the designated standard and functional safety rating
- Evaluation of documentation
- Product is certified

Follow-up Surveillance
- 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
Triennial Audit

The triennial audit allows UL to leverage the initial assessment of manufacturers’ Functional Safety Management, which are often a subset of the Product Lifecycle Management processes over the course of that three year period.
Benefits of the UL FS Mark

Demonstrate to your customers that your products can help to mitigate system risks.

Demonstrate to Authorities Having Jurisdiction (AHJ’s) that the installation meets the latest standards for safety.

Allow system integrators to coordinate the ratings and installation conditions associated with the Mark to build safer systems and more easily demonstrate the level of safety integrity to stakeholders.

Provide an increased level of confidence in the inner workings of “black box” controls with the assurance that a long known and trusted third-party certification organization has evaluated them.
Call-to-Action

For more information, download the whitepaper:

“UL Functional Safety Mark Program”

found at [www.ul.com/functionalsafety](http://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
Kevin.Connelly@us.ul.com
631-546-2691

Thomas Maier
Underwriters Laboratories
Principal Engineer, Functional Safety
Thomas.Maier@dk.ul.com
+45-421-37-452