Machinery Functional Safety using IEC 62061 and ISO 13849

Paul Reeve

SILMETRIC Ltd

Our Members


AFK Consultancy
ANALOX
arc AWE
NUCLEAR SECURITY TECHNOLOGIES
bp
CEPHA CONTROLS
cetix
CHARTER·TECH
CLEARLINE
cml Ex
CSA GROUP
DEKRA
DIAGEO
DNV
DOW CORNING
Dräger
EATON
Powering Business Worldwide
EDF
EMERSON
Process Management
ERM
evero
ExxonMobil
FICHTNER
Consulting Engineers Limited
FRAZER·NASH
CONSULTANCY
HAZCON
Haden Freeman Ltd
hitex
EMBEDDED TOOLS & SOLUTIONS
Honeywell
I&E SYSTEMS
IC&T
its
Invertek Drives
iti
Group
LR
=M
=Method
MOORE INDUSTRIES
MUTECH
national gas transmission
P & I Design Ltd
ProcessSafety
Solutions
procon
ProSalus
SAFETY CONSULTANTS
ROAKENGINEERING
ROSAS
rotork
Schneider Electric
SELLA CONTROLS
SENSIA
SGS
Baseefa
SIEMENS
SILMETRIC
sse
TAIT
UK Atomic Energy Authority
RACE
UL Solutions
uniper
VEOLIA
VAL-FSR
Virdee Advantage Limited
WITTENSTEIN
wsp
YOKOGAWA

Who Are We?

- **We are a cross-industry group of organisations with a common interest in functional safety, particularly in applying IEC 61508 and related standards (e.g., IEC 61511, IEC 62061) correctly in order to demonstrate compliance and improve safety for all.**
- Our members include end-users (from many industry sectors), EPC companies, systems integrators, product manufacturers, consultants and certifiers. We also have active relationships with related industry organisations and safety regulators who often attend our meetings.
- We develop and publish many useful and informative guides and assessment tools which are available to all (not just our members) and are free of charge.

Scope of this presentation

Notes (in green text) added later based on speaker's verbal notes

- Audience assumptions
  - Familiar with FS principles in IEC 61508 / 61511
  - And the common FS abbreviations!
- Purpose:
  - Overview of IEC 62061 and ISO 13849 (why two standards?)
  - Compare and contrast some key differences
  - Some personal commentary
  - It's not a technical training session!

Historic (time-line) reasons:
13849 based on older EN 954-1 (pre-61508);
62061 based on 61508;
More like cousins than siblings!

When to use these standards?

- When a hazard (or hazardous situation) originates from the machine itself
- If you're integrating a machine SCS

From OEM devices, many of which are 62061 and/or 13849 specified

E.g., the moving parts

- When another standard specifies SFs… "in accordance with 62061/13849"
- Typical applications:

Safety functions are (or must be rendered by annual test) high/continuous demand mode

  - Interlocked access (e.g., via gate/barrier) to moving parts of machinery
  - Safe torque-off (STO), safe limited speed (SLS), local or pendant control
  - Monitoring to prevent dangerous machine behaviour
  - Prevention of unexpected start-ups or restarts of machinery
  - Safety functions for maintenance tasks

Typical machinery hazards:

- *Cutting*
- *Crushing*
- *Entrapment*
- *Collision*
- *Electrical,*
- *Thermal*
- *etc*

Typical machines:

- *Packaging / palletising*
- *Materials handling, conveyors*
- *Turbo-machinery*
- *Robotics*

Current versions

- IEC 62061:2021 (ed. 2)
  - Functional safety of safety-related control systems (SCS)
  - Safety integrity levels (SIL 1, 2, or 3) are used
- ISO 13849-1:2023 (ed. 4)
  - Safety-related parts of control systems (SRP/CS) – principles for design
  - Performance levels (PL a, b, c, d or e) are used
- ISO 13849-2:2012 (ed. 2)
  - Safety-related parts of control systems – validation
  - Normative clauses now in Part 1 (ed. 4), but informative annexes are still applicable

These contain the definitions of many of the basic (systematic type) measures for each of the technologies in scope (electrical, mechanical, hydraulic, pneumatic), faults to be considered, and justifications for fault exclusions. So, really, these annexes are indispensable!

Key changes in the latest editions

- IEC 62061:2021
  - Much improved document structure, contents, and annexes
  - Now includes non-electrical technologies
  - Includes FSM (plan), CM and references to security standards
  - Better alignment of terms with IEC 61508-4

More cross references to each other making for easier comparisons

- ISO 13849-1:2023
  - Significant technical developments/updates on many sections, and more annexes
  - Includes FSM (at last!) – although only informative
  - Refers to Part 2 (still 2012) informative annexes for validation methods

Informative annexes

- Both standards have lots of useful informative annexes, such as:
  - The SIL or PL assignment methods
  - How to apply the design methodology, with safety function examples
  - Examples of MTTFD (and B10D) values for single components
  - Qualitative methods for DC and CCF
  - Guideline for software development
  - Lookup tables for qualitative to numerical correspondence
  - Simplified approaches to evaluate the PFH, SIL/PL, etc
  - FSM, systematic measures, validation methods, etc

The annexes in both standards offer:

- *Excellent guidance/examples on how to apply their approaches*
- *More practical and simplified methods than in 61508*

Key points about IEC 62061

- Well aligned with IEC 61508 concepts and approach

Good alignment and demarcation between 61508 and 62061

- Can be used on its own to integrate safety systems from…

For non-portable machines

  - IEC 61508-compliant subsystems/elements… and/or (mixed with)
  - Single components or “low complexity” devices

So, essentially, the building blocks must be pre-compliant with 61508 unless they are low complexity single components

- Think of it as the machinery version of IEC 61511 (but with no prior use!)
- Requirements for software on a 61508 pre-compliant platform:
  - LVL (≤ SIL 3) and FVL (≤ SIL 2)

The “IEC 61508-compliant subsystems/elements” must be to Route 1H (not Route 2H)

- Accepts ISO 13849-compliant subsystems
  - but only if “low complexity”!

Standard architectures are defined (for HFT and diagnostics) and the relevant equations provided

Key points about ISO 13849

- Aimed at integrating safety systems from…
  - Pre-compliant modules, devices, units, and/or (combined with)…
  - Single components
- Also used for evaluation of subsystems (above)
- Defines subsystem categories with certain quantitative and qualitative characteristics, with simple rules on how used
- Qualitative approach to evaluating parameters like DC, CCF
- Simplified rules for evaluating the final PL achieved
- Plenty of look-up tables to avoid “long-hand” calculations!

Pragmatic, building block approach with simplified rules, aimed at efficiency and avoidance of complex and detailed analysis

Defines five categories based on:

- *Selection of components and safety design principles*
- *Test functions (designed-in) to check the functional channel*
- *Diagnostic coverage, DC (none, low, medium or high)*
- *Fault tolerance (0 or 1)*
- *Probabilistic mean time to failure, MTTFD (low, medium or high)*
- *Systematic failure avoidance measures (e.g., in software)*

The performance level is then based on the Category, $MTTF_D$ and DCavg

Machinery risk assessment

- ISO 12100:2010 (ed. 1)
  - General principles for risk assessment and risk reduction
  - For machine designers
  - Determines whether SFs are required (at the machine level)
  - Common starting point for both the FS standards
- Type A (basic) standard and applies to all machines
- Contains a 5-stage strategy with flow diagram(s)
- Contains guidance for identifying possible hazards
- Harmonised with the machinery directive 2006/42/EC (see later)

The ISO 12100 standard:

- *Applies to all machines*
- *Applies at the overall machine level*
- *Is a precursor to 62061 or 13849 unless another relevant safety standard (type B or C) specifies certain safety functions and what their SILs or PL shall be*
- *Assumes the machine is clearly defined in what it does, how it does it, how humans interface with it, etc*
- *Is well-structured (diagrams and text) so the principles are easy to understand*
- *Has a good level of guidance in the body and appendices (e.g., a typical list of machine hazard types to consider)*

Typically, a hazard risk number (HRN) method is used to evaluate machine hazards/risks.

SIL / PL determination

- General:
  - Neither standard is prescriptive about the method used
  - Both offer a suggested method, supported with good guidance
- IEC 62061 (Annex A)
  - Offers a risk matrix method that leads to the SIL assignment
- ISO 13849-1 (Annex A)
  - Offers a risk graph method that leads to the PL assignment

Both methods are qualitative and may yield slightly different results to other methods

More developed guidance (scoring system) in latest 13849 Annex A for making judgments

Design process & safety management

- Stronger emphasis in IEC 62061 (in line with IEC 61508)
- Systematic measures in ISO 13849 are stronger now in ed. 4 (but possibly still a lighter touch than in 62061)
- Both have a work activity flow chart for the design process with a defined validation stage
- Both have a v-model for the software lifecycle
- FSM is normative in IEC 62061, versus informative in ISO 13849
- Both have strong validation requirements (includes verification)

13849-1 Annex G (systematic measures) still only 3 pages and "informative" (what…really?!)

Verification of certain items/documents is specified rather than a structured lifecycle model with staged verification (other than for software)

Factors to consider when choosing

- Application (common vs. novel, or sector norm?)
- Technology (e.g., is embedded software involved?)
- System integration or subsystem design?
- Organisational policy, procedures, competence, familiarity
- Availability of suitable subsystems/elements (for the application)
- Customer/stakeholder preference or expectation?
- A few years ago, the difference was more marked (the choice was clearer) – the latest editions are closer in their methods - although still not equivalent!

Is the application common in machine safety and are OEM parts designed and fully specified for it (many ISO 13849 parts are available).

More complex E/E/PE should consider 62061/61508 more appropriate

e.g., are these already in place for 61511?

62061 is for non-portable machines; no such restrictions in 13849

The standards state equivalence of objective, but still different enough in the methods/rigour used to get there. Correspondence between PL and SIL is only true in terms of the PFH_D achieved

Recent changes in regulations

- Both standards are harmonised with the MD 2006/42/EC, but…
- Machinery Regulation (EU) 2023/1230 replaces it, becoming law in the EU in January 2027
- The UK government has indefinitely extended CE marking for machinery beyond 2024
- CE and UKCA marking can both be used after December 2024
- The new Machinery Regulation has cybersecurity requirements (not detailed in IEC 62061 or ISO 13849)

Now published in the EU Official Journal

These are currently not detailed in either standard

Any Questions?

Presenter: Paul Reeve - Consultant

Contact Details: paul.reeve@silmetric.com

What's next…

Slot	Start Time	Paper	Workshop	Finish Time
	15:05	***** COMFORT BREAK (20 MINS) *****		**15:25**
10	15:25	Slot A-10: The Importance of Alarms for Functional Safety	Slot B-10: SIL Calculations and use of IEC 61508 Part 6	15:55
11	16:00	Slot A-11: Functional Safety and Communication Links	Slot B-11: TBA	16:30

We would be more than happy to discuss membership with you (https://61508.org/membership/)