Introduction to Functional Safety

©2019 Compliance inSight Consulting Inc.

functional safety
is the portion of *system safety* that is dependant on the correct functioning of the safety-related parts of the control system

[1]

©2019 Compliance inSight Consulting Inc.

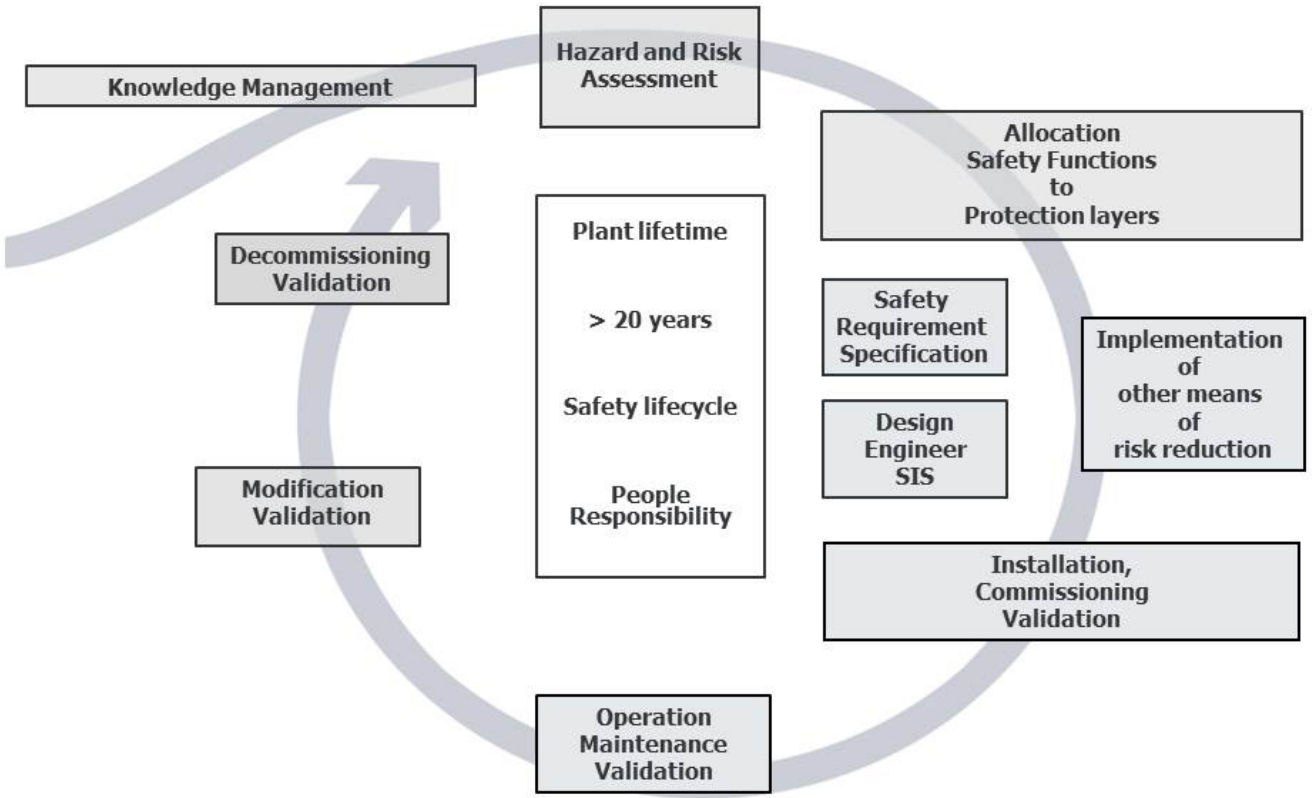
System Safety Aspects

What is "system safety"?

- **Physical Safety Measures**
  - Inherently safe design
  - Physical barrier guards
  - Fixed guarding
  - Trapped Key Systems (mechanical)
  - Mechanical pressure relief valves
  - "Velocity fuse" valves
  - Blow-out discs
  - Melt discs
  - Catchments/sumps
  - etc.
- **Control System Safety Measures**
  - Control functions (reduced speeds/feeds)
  - Control Software
  - Interlocked guards
  - Trapped Key systems (electrical/electronic)
  - Electrical/Electronic Guard locking
  - PSPE - Presence-Sensing Protective Devices (2-Hand Controls, Safety Mats, Safety Edges, etc.)
  - AOPD - Active Optical Protective Devices (Optical Safety Edges, Light fences and curtains, laser scanners, vision systems, etc.)
  - etc.

©2019 Compliance inSight Consulting Inc.

Management of functional safety and functional safety assessment and audit



[2]

©2019 Compliance inSight Consulting Inc.

Safety Function

Definition

function to be implemented by an E/E/PE* safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC†, in respect of a specific hazardous event (see 3.4.1 and 3.4.2)

EXAMPLE Examples of safety functions include:

- functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor); and
- functions that prevent actions being taken (for example preventing a motor starting).

[1, 3.5.1]

*E/E/PE - Electrical/Electronic/Programmable Electronic System [1, 3.3.2]

†EUC - Equipment Under Control [1, 3.2.1]

©2019 Compliance inSight Consulting Inc.

Example Safety Functions

- Safety-related Stop Function (includes but is not limited to e-stop)
- Manual reset function
- Start/restart function
- Local control function (e.g., enabling devices, slow-speed control, etc.)
- Muting function
- Response time
- Safety related parameters (e.g., temperature, pressure, levels, etc.)
- Fluctuations, loss and restoration of power sources
- Etc.

©2019 Compliance inSight Consulting Inc.

[5, 5]

Functional Safety Standards

ISO Standards

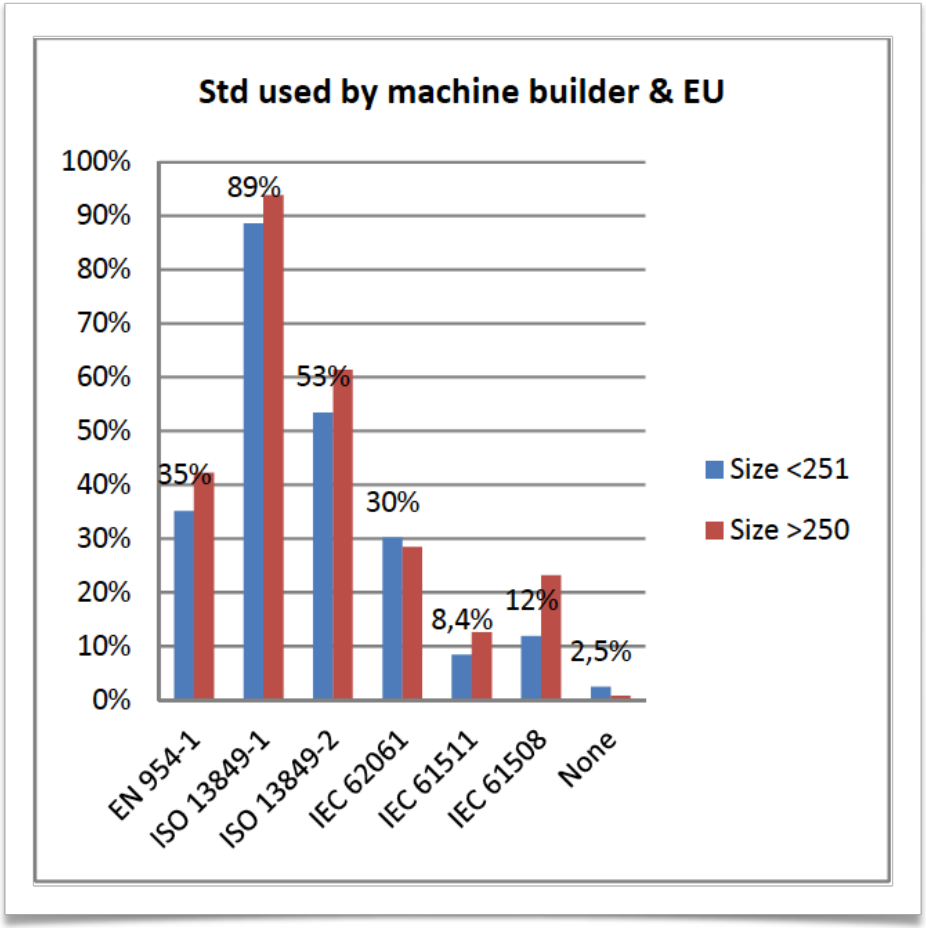
- **ISO 13849 - Industrial Machinery (2 parts)**
- ISO 26262 - Road vehicles (12 parts)
- ISO 19014 - Earth-moving machinery (5 parts)
- ISO/PAS 19695 Motorcycles—Functional safety
- ISO 13766-2 Earth-moving and building construction machinery—Electromagnetic compatibility (EMC) of machines with internal electrical power supply—Part 2: Additional EMC requirements for functional safety
- ISO/IEC 14762 Information technology—Functional safety requirements for Home and Building Electronic Systems (HBES)
- etc.

IEC Standards

- IEC 61508 (7 parts) the “mother standard”
- IEC 62061 - Machinery
- IEC 61511 - Process systems
- IEC 60079-29-3 Explosive atmospheres - Part 29-3: Gas detectors - Guidance on functional safety of fixed gas detection systems
- IEC 61000-6-7 Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations
- etc.

©2019 Compliance inSight Consulting Inc.

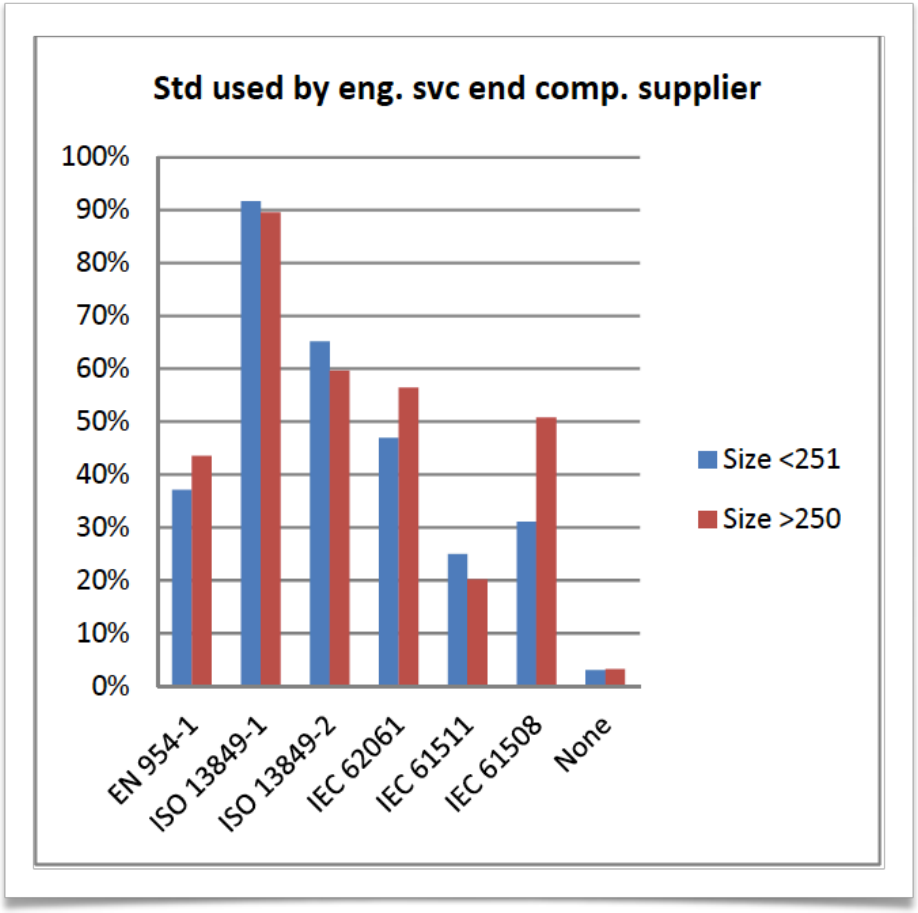
Use of FS Standards



[4, Graph 2]

©2019 Compliance inSight Consulting Inc.

Use of FS Standards



[4, Graph 3]

©2019 Compliance inSight Consulting Inc.

Linkage to Risk

Functional safety target requirements are:

- Determined by
  - the inherent risk sometimes called the “first pass” risk, and
  - the Mode of Operation
- Expressed as either:
  - Performance Level (PL_r), or
  - Safety Integrity Level (SIL_r)

©2019 Compliance inSight Consulting Inc.

Demand Rate & Mode of Operation

- "Mode of Operation" refers to how often there is a demand on the safety function, i.e., how often it's used
- Three broad ranges:
  - Low demand: < 1 per year (e.g., reactor over-pressure relief or air receiver over-pressure relief)
  - High demand: >1 per year
  - Continuous: maintains safe state as part of normal operation (e.g., light curtains, or interlocked guards)
- Machinery operates in low demand mode very rarely
- Machinery is usually considered to operate in high/continuous demand mode
- ISO 13849 is focused on high/continuous demand

©2019 Compliance inSight Consulting Inc.

Risk Assessment

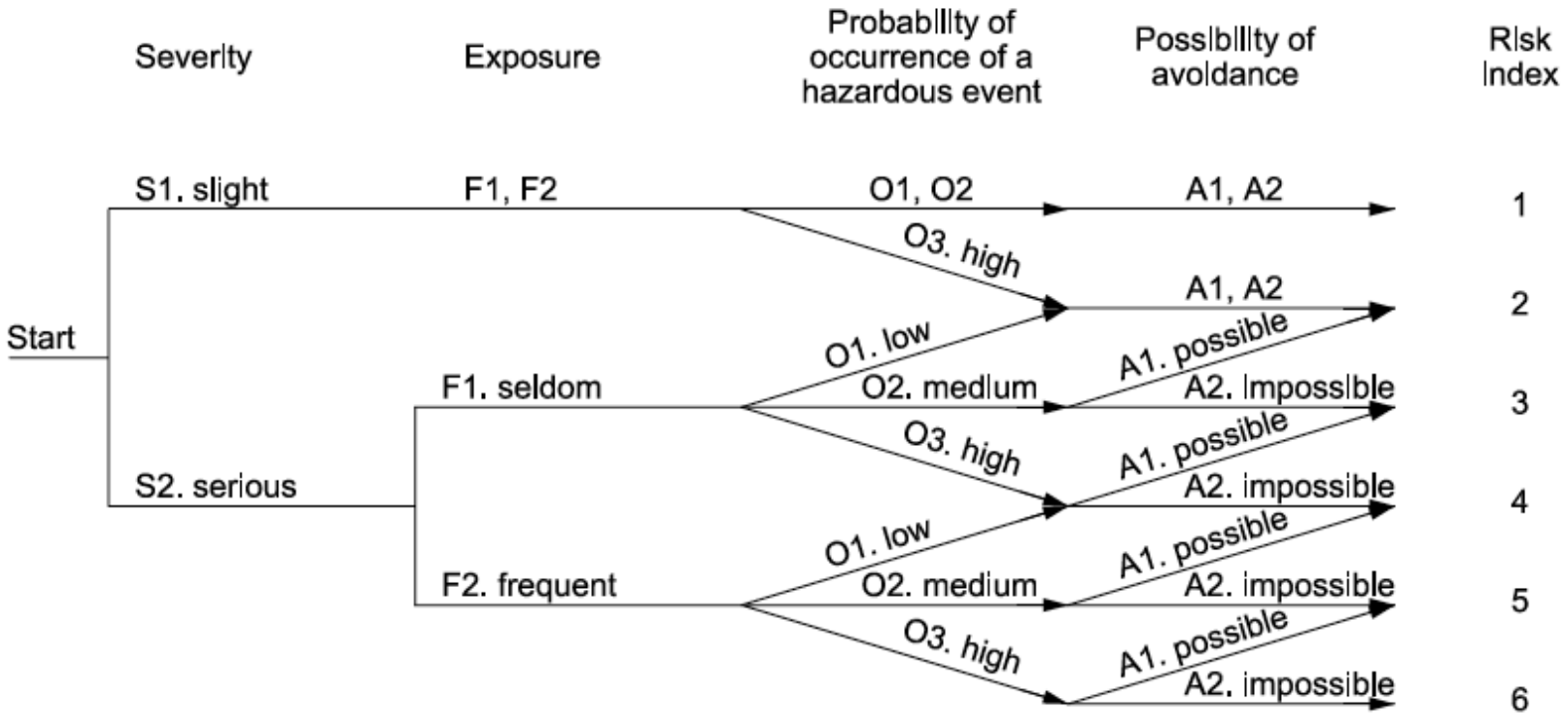
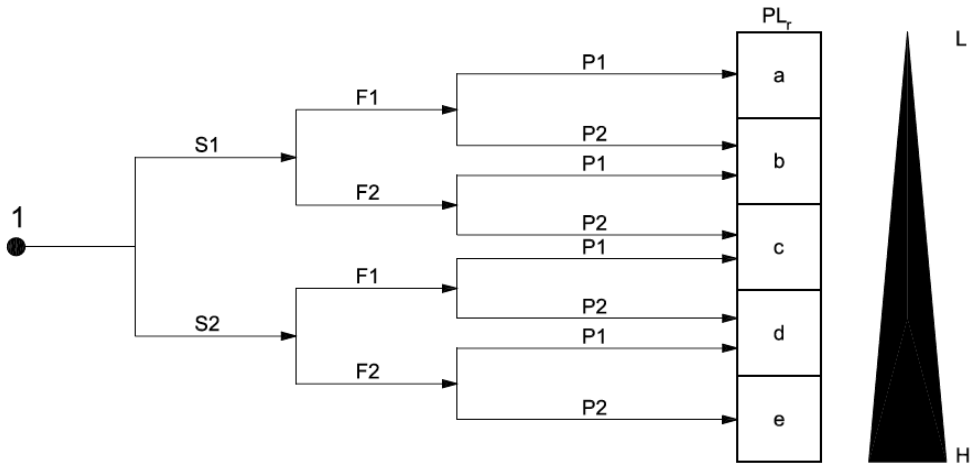


Figure 3 — Example of a risk graph for risk estimation

[3]

©2019 Compliance inSight Consulting Inc.

Performance Level Assignment



Key

1	starting point for evaluation of safety function's contribution to risk reduction
L	low contribution to risk reduction
H	high contribution to risk reduction
PL$_r$	required performance level

Risk parameters:

S	severity of injury
S1	slight (normally reversible injury)
S2	serious (normally irreversible injury or death)
F	frequency and/or exposure to hazard
F1	seldom-to-less-often and/or exposure time is short
F2	frequent-to-continuous and/or exposure time is long
P	possibility of avoiding hazard or limiting harm
P1	possible under specific conditions
P2	scarcely possible

Figure A.1 — Graph for determining required PL$_r$ for safety function

[5, Fig. A.1]

The 3rd Ed. (2015) allows for consideration of the Probability of the Hazardous Event, although it is not shown as a variable on the graph above.

©2019 Compliance inSight Consulting Inc.

Safety Integrity Level Assignment

Cl = Fr + Pr + Av

Table A.6 – SIL assignment matrix

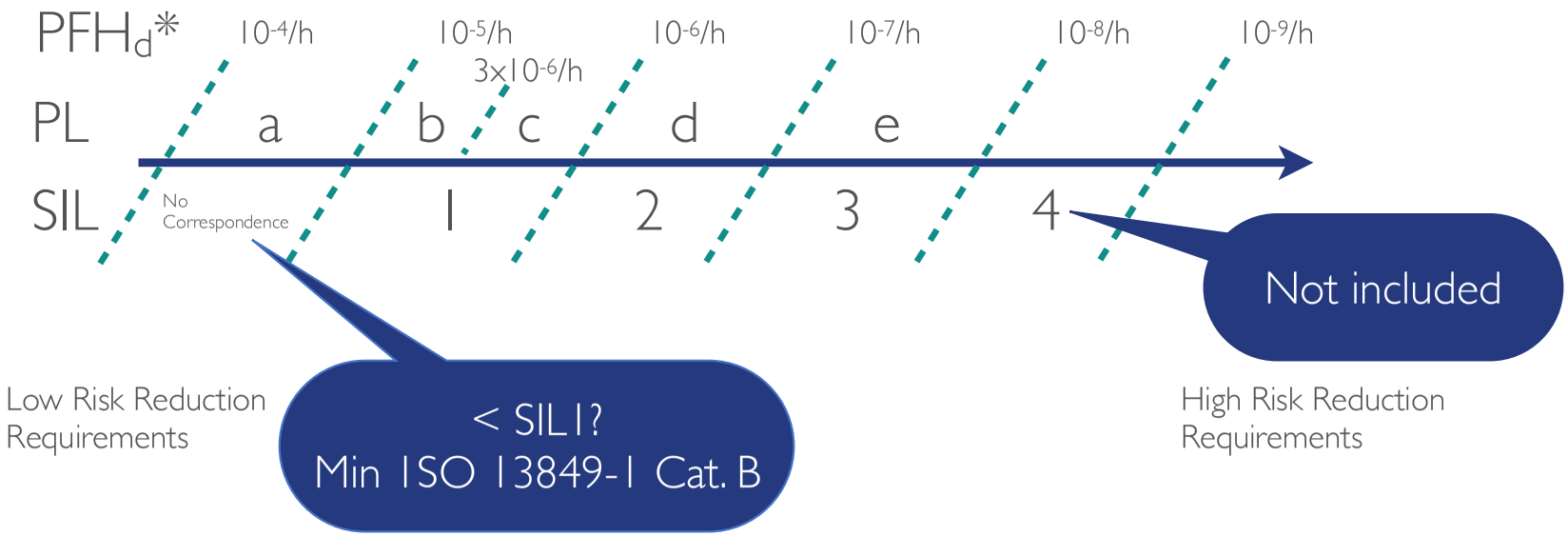
Severity (Se)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

(OM) - Other Measures

[6, Annex A]

©2019 Compliance inSight Consulting Inc.

PL vs. SIL



* Probability Dangerous of Failure per Hour

©2019 Compliance inSight Consulting Inc.

Safety Requirement Specification

Provides the detailed requirements for the realization of each safety function.

Includes details like:

- Required PL or SIL
- Input conditions
- Safe state
- Proposed architecture
- Response time
- See [5, 5.1]

©2019 Compliance inSight Consulting Inc.

Key Concepts

1) **Performance Level (PL) - 5 ranges of failure rate: a, b, c, d, e**
2) Architecture (Category) - 5 types: B, 1, 2, 3, 4
3) Mean Time to Dangerous Failure (MTTFD) - 3 ranges: Low, Medium, High
4) Diagnostic Coverage (DC) - Ratio between detectable failures and all failures
5) Common Cause Failures (CCF) - Systematic failures (Category 3, 4 only)

©2019 Compliance inSight Consulting Inc.

References

[1] IEC/TC 65A. *IEC 61508-4—Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4: Definitions and abbreviations*, 2nd ed. Geneva, Switzerland: International Electrotechnical Commission, 2010.

[2] "Management of Functional Safety", *Web-material3.yokogawa.com*, 2018. [Online]. Available: http://web-material3.yokogawa.com/f263b738901951048f2dfc494a202af9114d77b5.jpg. [Accessed: 28- Nov- 2018].

[3] Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods. ISO/TR 14121-2. 2012.

[4] A. Butaye, "Report from ISO/TC 199/JWG 1/Sub group 2 “Questionnaire”—ISO/TC 199/JWG1 N0038", ISO, Geneva, 2013.

[5] ISO/TC 199. *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design, ISO Standard 13849-1*. 3rd Ed.. ISO International Organization for Standardization, Geneva. 2015.

[6] IEC/TC 44. *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.* 1st Ed. IEC International Electrotechnical Commission. 2005.

[7] M. Hauke, M. Schaefer, R. Apfeld, T. Boemer, M. Huelke, and T. Borowski, “BGIA Report 2/2008e Functional Safety of Machine Controls – Application of ISO 13849-1,” DGUV/BGIA - Institute for Occupational Safety and Health of the German Social Accident Insurance, Berlin, Germany, 2009.

[8] *ISO/TC 199. Safety of machinery—Safety-related parts of control systems—Part 2: Validation, ISO Standard 13849-2*. 2nd Ed.. ISO International Organization for Standardization, Geneva. 2012.

©2019 Compliance inSight Consulting Inc.

Compliance inSight Consulting Inc.

Expert Advice, Safety Reviews, In-Depth Training

Doug Nix, C.E.T., SM-IEEE'14

Managing Director & Principal Consultant

+1.519.650.4753

dnix@complianceinsight.ca

Web: www.complianceinsight.ca

Blog: machinerysafety101.com

Courses: courses.complianceinsight.ca

©2019 Compliance inSight Consulting Inc.

PSES Product Safety Engineering Society IEEE