



Review

# Safety of Machinery: Significant Differences in Two Widely Used International Standards for the Design of Safety-Related Control Systems

Yuvin Chinniah <sup>1,\*</sup>, Douglas S. G. Nix <sup>2</sup>, Sabrina Jocelyn <sup>3</sup>, Damien Burlet-Vienney <sup>3</sup>, Réal Bourbonnière <sup>4</sup>, Benyamin Karimi <sup>1</sup> and Abdallah Ben Mosbah <sup>1</sup>

<sup>1</sup> Department of Mathematics and Industrial Engineering, Polytechnique Montreal, P.O. Box 6079, Station Centre-ville, Montreal, QC H3C 3A7, Canada; Benyamin.karimi@polymtl.ca (B.K.); Abdallah.ben-mosbah@polymtl.ca (A.B.M.)

<sup>2</sup> Compliance inSight Consulting Inc., 145 Deer Ridge Drive, Kitchener, ON N2P 2K9, Canada; dnix@complianceinsight.ca

<sup>3</sup> Department of Mechanical and Physical Risk Prevention, Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST), 505 De Maisonneuve Blvd. West, Montreal, QC H3A 3C2, Canada; sabjoc@irsst.qc.ca (S.J.); Damien.burletvienney@irsst.qc.ca (D.B.-V.)

<sup>4</sup> Consultation Réal Bourbonnière, 58, rue de la Crête, Orford, QC J1X 0C5, Canada; real@realbourbonniere.com

\* Correspondence: Yuvin.chinniah@polymtl.ca; Tel.: +1-514-340-4711 (ext. 2268)

Received: 8 August 2019; Accepted: 25 October 2019; Published: 29 October 2019



**Abstract:** Industrial machines are known to possess many hazards. There are many laws, regulations, standards and practices that aim at ensuring that machines are safe for different workers performing various tasks including operation and maintenance. Safeguards protect workers by stopping hazardous motion when actuated. Those safeguards are integrated into machinery using two widely used international standards for functional safety. However, these standards have some significant differences although they are both based on similar principles. This paper explores those differences and their potential impacts. Subjectivity in the specification and design of safety systems, based on the differences, can lead to different levels of reliability in the safety systems even when considering the same hazard zone of machinery based on which standard is used.

**Keywords:** machinery; hazards; risk analysis; ISO 13849; IEC 62061; functional safety

## 1. Introduction to Safety-Related Control Systems

Machine safety is crucial in industrial automation. Safety-related control systems and functional safety offer manufacturers flexibility and a way of improving competitiveness as well as productivity. Safety becomes an integral part of the functionality rather than a required constraint to meet regulations and standards. For instance, collaborative robotic systems provide a good example illustrating the importance of safe control systems. These robots are purposely designed to work in direct cooperation with human workers within a defined workspace. The human and the robot simultaneously perform tasks during production operation. Functional safety is at the heart of their use according to ISO 10218-1 and -2: 2011 [1,2]. The sharing of the workspace brings the flexibility the Industry 4.0 seeks, thanks to the inherently safe design of that kind of robots.

Inherently safe design measures are at the top of the Hierarchy of protective measures stated by the ISO 12100:2010 standard [3]. That Hierarchy is a fundamental part of ISO 12100 and many other safety-of-machinery standards. The Hierarchy provides a structured, linear approach to risk control. Inherently safe design includes the physical characteristics of the machinery like sharp corners

and edges, stability, and process chemicals. It also includes the basic principles associated with the safe design of a control system, including adherence to standards and codes for construction, and the functional safety characteristics of the Safety-Related Parts of a Control System (SRP/CS). The second layer in the hierarchy is called “Safeguarding and complementary protective measures.” This layer includes physical means to enforce safe distance or prevent access to hazards, and active controls like interlocks and safeguarding devices that control hazardous energy. Active safeguarding devices rely on the operation of the SRP/CS for correct operation. The third layer in the hierarchy is “Information for use,” which includes hazard warning signs and labels, information on the human-machine interface, instructions, manuals and other methods that convey operational information to the user. These three layers are available primarily to the machine designer, particularly those in the inherently safe design layer. Safeguarding and complementary protective measures, as well as information for use can be readily modified by users.

Another layer called “Protective measures implemented by the user” [3] is available in the hierarchy and is primarily the jurisdiction of the workplace. That layer includes administrative controls such as safe working procedures (e.g., hazardous energy control procedures), worker authorization and permitting, training and supervision, and “Personal Protective Equipment (PPE).”

The choice of risk control selected depends on both the life cycle stage of the machinery and the hazards present. For example, fixed guards are commonly used to reduce risk associated with hazards generated by the moving transmission parts of machinery. If selected for areas where frequent access, for e.g., more than once or twice a week, fixed guards can be inconvenient but straightforward. Interlocking guards with or without guard locking are used where more frequent access to the danger zone is needed. Interlocking guards and presence-sensing safeguarding devices are two of the risk reduction methods that can be used when access rates of more than once per shift is needed.

Safe control systems are fundamental to ensuring safety. Interlocking guards and safety devices rely heavily on safe control systems to fulfil their safety functions (SF), with increasing risk demanding greater reliability from the control system [3].

Safety devices such as:

- interlocks,
- light curtains, multi-beam and single beam optical sensing devices, and laser scanners,
- safety mats,
- safety relays, safety modules, and safety programmable logic controllers (PLCs) are all certified based on international standards making use of safe control systems (e.g., IEC 61496-1:2012 for electro-sensitive protective equipment [4]).

Two international standards, ISO 13849, and IEC 62061 guide the design and validation of safety-related control systems associated with machinery [5–7]. Those standards are considered to be the state of the art for safety engineers and machine designers when developing safeguarding systems for machinery. They give safety requirements namely by stating discrete reliability levels giving some insight to what extent a SF is able to reduce the risk associated with a dangerous situation on a machine. The ISO discrete reliability level is called “Performance level (PL)” whereas IEC’s is named “Safety integrity level (SIL)”. Those standards propose an equivalence chart between the PL and SIL based on their corresponding average probability of dangerous failure per hour. However, Malm, et al. [8] observed several differences in the PL or SIL required following risk estimation with the two standards. The analysis focused on users. On the contrary, this paper aims at identifying structural differences in ISO 13849 and IEC 62061 for the design of safety-related control systems for machinery. The method consists of a strict comparison of two standards. The originality of the paper relies in the fact that the comparison will fill a gap in the existing literature by using qualitative and descriptive analysis. Moreover, that comparison discusses and elucidates the fact that some parts of the standards can actually contribute to the variability in the results, i.e., the determination of the PL or SIL required. An overdesign led by a high required PL or SIL will have added costs and time

to machine builders and integrators, while under-design led by lower required PL or SIL will be hazardous to workers as failures in the control systems can lead to harm. Safe, reliable control systems are more expensive and complex to design since redundancy and monitoring of critical components are needed. Designing an appropriate safety-related control system based on risk is crucial.

The remainder of the paper gives an historical background regarding standards ISO 13849 and IEC 62061. A literature review follows as well as a content-based comparison between the two standards. That comparison is necessary to shed light upon the main conceptual differences and similarities able to guide machine builders through their design process, including the choice of the standard. The comparison may also encourage another attempt from ISO and IEC's working groups to merge those two standards in order to facilitate the work of the machine designers and integrators.

## 2. History and Content of Safety-Related Control Systems Standards for Machinery

ISO 13849 is a two-part standard that applies to all types of safety control systems namely electrical, electronic, pneumatic and hydraulic. The first part, ISO 13849-1:2015 aims at the design of SRP/CS [5] whereas the second part, ISO 13849-2:2012 deals with the validation of SRP/CS [7]. The origins of ISO 13849 are found in EN 954-1:1996 [9]. EN 954-1 originated the concept of the architectural categories used in ISO 13849-1 for the estimation of PL. These categories (B, 1, 2, 3 and 4) are qualitative measures of a system's behavior: its resistance to faults and its behavior once one or more faults have occurred [10]. The categories rely on both the physical arrangement of the control components and subsystems used in the SRP/CS, the selection and the inherent reliability of the components themselves. The ISO 13849 process results in grouping the resulting system performance into a series of five Performance Levels.

IEC 62061: 2005 deals with electrical, electronic and electronic programmable systems (E/E/PES) to the exclusion of electromechanical and mechanical components and subsystems [11]. IEC 62061 follows the IEC 61508 (2002) model and is also intended to be used by machine builders in the specification of the performance and the design of safety-related electrical control. IEC 62061 takes the probabilistic approach developed in IEC 61508, which results in grouping the performance of the resulting systems into a series of four Safety Integrity Levels.

In ISO 13849-1:2015, there are five performance levels from the lowest, PL<sub>a</sub>, to the highest, PL<sub>e</sub>, each with a defined range of probability of a dangerous failure per hour. In contrast, IEC 61508-1 (2010) defines four safety integrity levels (SIL1-4) in two ways; Probability of Dangerous Failure on Demand (PFD<sub>avg</sub>) for low demand systems (demand  $\leq 1/a$ ), and as a frequency for high demand or continuous operation, called the Average Frequency of Dangerous Failure per Hour (PFH<sub>avg</sub>) [12]. Since the safety-related control systems used on machinery typically is required to operate more than once per year and often multiple times per hour, the SILs used in IEC 62061 are considered only from the perspective of high or continuous demand. Additionally, IEC 62061:2005 [11], is limited to SIL 1 to SIL 3 due to the practical limitations of achieving very high reliability in high-demand applications. Table 1 compares PLs and SILs based on their average probability of dangerous failure per hour [PFH<sub>D</sub>] (Tables 2 and 3 of ISO 13849 [5]).

**Table 1.** PL and SIL compared based on their average probability of dangerous failure per hour (PFH<sub>D</sub>).

PFH <sub>D</sub>	PL (ISO 13849-1:2015)	SIL (IEC 62061:2005)
$\geq 10^{-5}$ to $< 10^{-4}$	PL <sub>a</sub>	No correspondence
$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	PL <sub>b</sub>	SIL1
$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	PL <sub>c</sub>	SIL1
$\geq 10^{-7}$ to $< 10^{-6}$	PL <sub>d</sub>	SIL2
$\geq 10^{-8}$ to $< 10^{-7}$	PL <sub>e</sub>	SIL3

The five performance levels were originally conceived to correspond to the five original architectures in EN 954-1:1996 [9] and ISO 13849-1:1999 [13]. This mapping was left behind when the

probabilistic models were considered. No correspondence with the IEC 61508 model was considered when the EN/ISO standards were being developed.

A safety-related control circuit that performs a safety function can be decomposed into three basic building blocks: input, logic and output. For example, consider an interlocking guard: the input block is the physical interlock switch, which is actuated by the guard in the open position, the logic block is formed by the safety relay which monitors the state of the input block, and the output block formed by the electrical contractor, which controls power to an electric motor on the machine.

The reliability of the control system depends on three aspects of the design: the structure or architecture, the inherent reliability of the components selected and the diagnostic capability of the system. High-risk applications use redundant and monitored control systems designed to detect as many of the dangerous faults as possible. For example, the hazard zone surrounding the mould in an injection moulding machine is protected by three independent safety control systems using three different technologies (electrical, hydraulic and mechanical), each monitoring the physical guard or the state of the mould, and each having self-monitoring features which create the interlock for that zone.

Very low risk applications may achieve adequate reliability using single channel architecture and basic safety principles. This type of approach is used in SRP/CS of Category B. More reliable SRP/CS for low-risk situations can be designed using single channel architectures following basic and well-tried safety principles, and using well-tried components in lieu of having any diagnostics (Category 1 and 2). These SRP/CS may achieve increased reliability by implementing diagnostics capable of detecting many of the dangerous failures that occur. In that case, the diagnostic coverage (DC), i.e., “the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures [5]” goes from DC <60% to DC <99%. Reliable safety control systems (Category 3 and 4) for moderate to high-risk situations incorporate redundant architectures that include diagnostics capable of detecting most of the dangerous failures, and are configured using well-tried safety principles. In that case, the diagnostic coverage goes from DC ≥60% to DC ≥99% and the SRP/CS can be resistant to many types of random and systematic failures. Examples of basic safety principles can be found in ISO 13849-2: 2012, Annexes A through D [7]. Components that have been certified under product specific safety standards, i.e., IEC 61439-1, can be considered equivalent to “well-tried” components [14]. Components not specifically listed as well-tried in ISO 13849-2: 2012 [7] can be declared as well-tried by the manufacturer following the methodology outlined in IEC 61508.

Defeat resistance is a key design criterion for reliable safety systems. However, if operators or mechanics are motivated to defeat a reliable control system, a way to defeat the system will almost certainly be found. On this specific subject, Haghghi, et al. [15] propose a detailed literature review on the incentives and solutions for the bypassing of guards and protective devices on machinery. ISO 14119 (2013) provides guidance on defeat resistant design where interlocking devices are used [16].

The two standards are referred to in regulations and fundamental machine safety standards (e.g., ANSI B11.19: 2010 in the U.S. [17]). According to Hauke, et al. [18], ISO 13849-1:2015 is used by 90% of machine builders and end users while IEC 62061:2005 is used by 30%. ISO 23849: 2010 gives guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery [19].

### 3. Literature Review on Safety Control Systems

In this section, a literature review associated with safety control system is organized into five parts. In the first part, the application of safety control systems standard is considered, and technical reports from occupational health and safety (OHS) research institutes in Germany, France, UK and Canada are briefly described. In the second part, research on the application of safety control systems standards is described. In the third part, research on the variability in the specification and the validation of the safety control system when applying standards is outlined. In the fourth part, an overview of new methods and tools to facilitate the application of the standard is presented. In the fifth part, research on the analysis of accidents caused by failures in control systems is described.

### 3.1. Part 1: Technical Reports and Guides

In order to facilitate the application of control system safety standards, several technical reports and guides have been produced. In 1999, the BIA in Germany explained the categories for safety-related control systems in accordance with EN 954-1 (the forerunner of ISO 13849) [20]. The practical implementation of these categories is illustrated using many examples based on the following technologies: electromechanical, electronics, electronic programmable, hydraulics and pneumatics. Moreover, an extensive fault list for electrical, hydraulic and pneumatic components is tabulated as a fault assumption, fault exclusion and remarks [20]. In 1998, the HSE in the UK published a guide explaining the link between the EN 954-1 and IEC 61508 standards. The STSARCES (STandards for SAfety-Related Complex Electronic Systems) project was to examine the retrospective application of the EN 954-1 and IEC 61508 standards to existing machinery [21]. In 2003, the INRS in France produced a guide on safety control system describing the categories and giving several examples based on EN 954-1 standard [22]. In 2005, the IRSST in Canada produced a guide on the design of safety control systems [23]. Categories were explained through eight examples of industrial machinery, two examples for each category, including a safety edge on a guard, interlocking guards with and without guard locking, safety light curtain, safety light beam and a two-hand control. For each example, a photograph illustrated the hazard zone, and a risk graph shows how the required category was developed. An example safety system circuit is presented and explained.

In 2009, the BGIA in Germany published the revised version of its previous report entitled “Functional safety of machine controls and application of EN ISO 13849,” [24]. The report explains the revision in the standard and explains its application with reference to numerous examples from electromechanics, fluidics, electronics and programmable electronics, including control systems using mixed technologies. The required performance level is explained, and the requirements in terms of the associated categories, component reliability diagnostic coverage, software safety and measures for preventing systematic and common-cause failures are discussed. In 2013, the INRS produced one guide for ISO 13849 and another guide for IEC 62061 [25,26]. The guide for designers of machine control systems with only one or a few basic safety functions such as an emergency stop or a movable guard based on ISO 13849 was produced. The guide explains the modifications and the new concepts in ISO 13849 that deal with quantifying a number of parameters. It also presents a practical case study and all the phases of design. It provides tools such as graphs and tables to facilitate the understanding and use as well as the choices designers will have to make. The IEC 62061 guide helps designers of machine control circuit incorporating functional safety of safety-related electrical, electronic and programmable electronic control systems. The guide targets designers of automated systems that must integrate complex components such as programmable logic controllers dedicated to safety. Finally, some specific books are also available such as Schmidt [27].

### 3.2. Part 2: Case Studies on The Application of Standard

Paques, et al. [28] presented an example of a technical analysis used to support the safety assessment of an automatic mining truck using IEC 61508 and EN 954-1 standards. Poisson, et al. [29] presented the design process for a reliable safety control system for the verification step of zero electrical energy. ISO 13849-1 and 2 were used to design and validate the programmable safety control system based on dedicated safety PLCs. Zahálka, et al. [30] calculated the performance level for an emergency stop based on ISO 13849-1 and presented all the required steps. Hata and Hirao [31] propose a new functional safety control for the collaboration of press machines and operators. Jones [32] describes the application of IEC 62061 on a robot cell application.

### 3.3. Part 3: Variability Due To Users Of The Standards

Hietikko, et al. [33] discussed and compared three risk estimation case studies for one control function of a machine using ISO 13849 and IEC 62061. Significant divergence was detected in the risk parameters of all the case studies, and thus the required safety integrity level from IEC 62061 and performance level from ISO 13849 of the pre-defined control function varied. In this paper, dispersion in the risk estimation results were explained by

- (i) the lack of familiarity to the machine under study and its control system,
- (ii) variability in the participants' background,
- (iii) not reading or understanding the input documentation carefully and
- (iv) different assumption made by the participants.

Malm, Stålhane, Bésche, Venho-Ahonen and Hietikko [8] went further than the previous study. A round-robin test was run with 19 assessors on nine cases related to mobile work machines and seven cases related to industrial robots. A difference between final PL and SIL results was observed.

Jocelyn, et al. [34] discussed and presented a posteriori (post design) validation study of a safety function of an injection molding machine based on ISO 13849. The procedure is studied for two contexts of use of the machine: in industry, and in the laboratory. The calculations required by the ISO standard were done using Excel, followed by SISTEMA software. It is shown that, based on the context of use, the estimated performance level was different for the same safety-related circuit. The variability in the results is explained by the assumptions made by the person undertaking the validation without the involvement of the machine designer. Furthermore, systems that require evaluation of Common Cause Failure (CCF) mitigation using ISO 13849-1 Annex F cannot be effectively scored post-design, since many of the CCF mitigation measures may not be self-evident to a reviewer of the design. Without achieving the minimum CCF score of 65, no PL claim can be made.

### 3.4. Part 4: Methods And Tools To Facilitate The Use Of Standards

Hauke, Apfeld, Bömer, Huelke and Becker [18] explained and illustrated the improvement of ISO 13849-1 (2015) such as integration of components without safety rating by the manufacturer (e.g., standard PLCs); consideration of the "probability of occurrence of a hazardous event"; higher typical  $MTTF_D$  estimates for hydraulic components with a small number of annual operations; evaluation of the quantifiable aspects of the PL without using  $MTTF_D$  values but based on the use of well-tried components. The IFA also developed the SISTEMA, which is offered for free via the IFA website. The latest version, 2.0.7, was launched in 2017 [35]. The IFA also developed a method of meeting the requirements of EN ISO 13849-1 concerning safety-related application software for machinery [36].

Recently, Porras-Vázquez and Romero-Pérez [37] proposed a new methodology for facilitating the design of safety control systems according to ISO 13849. The workflow presented in the standard for designing systems is based on trial and error procedure and increases the time needed for selecting adequate components. A software tool has been developed and is evaluated through two practical cases.

### 3.5. Part 5: Accidents Linked To Failures Of The Control System

In 2003, the UK Health and Safety Executive (HSE) published a guide to raise awareness of the technical causes of control system failure [38]. Incidents that have been reported are presented and analyzed. The analysis of the incidents shows that the majority were not caused by some failure mode of the control system but by defects that could have been anticipated if a systematic risk-based approach had been used throughout the life cycle of the system.

Villard [39] described four accidents caused by the failure of guard operated interlocking switches in Switzerland. Dźwiarek [40] analyzed 144 machine-related accidents in the period 1996–2002 in Poland. He found that improper functioning of machine control systems caused 54 of those accidents. Chinniah [41] analyzed 106 accident reports the period 1990–2011 in Quebec on stationary machinery. Three accident reports mentioned modification or bypassing of the existing safety control system.

Despite all the references available in the literature to help or advice designers and integrators in the design and validation of safety-related control systems, machine builders are still questioning the presence of the two standards: ISO 13849 and IEC 62061 instead of one. They also complain about how hard those standards are to understand. Even though this paper does not solve that problem, the structural comparison between those standards in the next section will at least enlighten the common ground and divergences between them. That comparison will be somehow a first aid to: (1) machine builders and (2) working groups wishing to merge or revise the standards for an easier understanding by their users.

#### 4. Content-Based Comparison between ISO 13849:2015 and IEC 62061:2005

Significant differences were identified in the risk estimation step (parameters used, calculation of the level of risk), the use of the results of the risk estimation, the CCF and the DC.

##### 4.1. Parameters for Risk Estimation

ISO 12100 provides some general guidance on the design of safety-related control systems for machinery and refers to ISO 13849 and IEC 62061 for additional guidance [3]. It defines risk as the combination of the probability of occurrence of harm (Tables 2 and 3), and the severity of harm (Tables 4 and 5) [3]. That definition of risk is widely accepted in the field of safety of machinery. ISO 13849 and IEC 62061 refer to this definition of risk when specifying the required performance level and safety integrity level using all or some of the ISO 12100 parameters (Table 2). Tables 5–8 gives an overview of the term “risk” in the two safety-related control system standards, as well as the parameters used to define it.

**Table 2.** Parameters used for risk estimation in three fundamental standards.

	ISO 12100	ISO 13849	IEC 62061
	Severity of harm	Severity of injury	Severity of harm
Probability of occurrence of harm	Exposure of persons to hazards	Frequency and/or exposure to hazard	Frequency and duration of exposure
	Occurrence of hazardous events	Not mentioned	Probability of occurrence of a hazardous event *
	Possibilities of avoiding or limiting harm	Possibility of avoiding the hazard	Probability of avoiding or limiting harm

\* This paper assumes that Section A.2.4.2 of IEC deals with the probability of occurrence of a hazardous event as suggested by the title of that clause: “Probability of occurrence of a hazardous event”. That assumption is due to the confusion generated by the first sentence in the clause: “The probability of occurrence of **harm**[not the probability of occurrence of a hazardous event] should be estimated . . . ”. On the other hand, by the absence of definition of the expression “hazardous event” in the standard.

**Table 3.** Factors affecting the three parameters defining the probability of occurrence of harm based on ISO 12100.

Probability of Occurrence of Harm		
Exposure of Person to the Hazard	Occurrence of a Hazardous Event	Technical and Human Possibilities to Avoid or Limit Harm
Need for access to the hazard zone	Reliability	Persons are skilled or unskilled
Nature of access	Accident history	Speed in a hazardous situation leads to harm
Number of persons requiring access	History of damage to health	<ul style="list-style-type: none"> <li>• Suddenly</li> <li>• Quickly</li> <li>• Slowly</li> </ul>
Frequency of access	Comparison of risks	Awareness of risk
		<ul style="list-style-type: none"> <li>• Direct observation</li> <li>• Warning signs</li> <li>• Information for use</li> </ul>
		Ability to avoid or limit harm
		<ul style="list-style-type: none"> <li>• Reflex</li> <li>• Agility</li> <li>• Possible escape</li> </ul>
		Practical experience and knowledge
		<ul style="list-style-type: none"> <li>• Of the machinery</li> <li>• Of similar machinery</li> <li>• No experience</li> </ul>

**Table 4.** Factors affecting the severity of harm based on ISO 12100.

Severity of Harm	
Severity of injuries or damage to health	Extent of harm
<ul style="list-style-type: none"> <li>• Slight</li> <li>• Serious</li> <li>• Death</li> </ul>	<ul style="list-style-type: none"> <li>• One person</li> <li>• Several persons</li> </ul>

**Table 5.** Comparison between ISO 13849-1:2015 and IEC 62061:2005 relative to parameters of risk.

Parameters of risk	Levels of The Parameters According to ...	
	ISO 13849-1:2015	IEC 62061:2005
Severity of harm	S1-slight (normally reversible injury) S2-serious (normally irreversible injury or death)	Reversible: requiring first aid; Se = 1 Reversible: requiring attention from a medical practitioner; Se = 2 Irreversible: broken limb(s), losing a finger; Se = 3. Irreversible: death, losing an eye or arm; Se = 4
Exposure of the persons to hazards	F1—Seldom-to-less-often and/or exposure time is short F2—Frequent-to-continuous and/or exposure time is long	≤1 h: Fr = 5 >1 h to ≤1 day: Fr = 5 >1 day to ≤2 weeks: Fr = 4 >2 weeks to ≤1 year: Fr = 3 >1 year: Fr = 2
Occurrence of hazardous event	The probability of avoiding the hazard and the probability of occurrence of a hazardous event (Pe) are both combined in the parameter P. The probability of occurrence of a hazardous event is assumed to be 100%, the worst-case scenario. Where the probability of occurrence of a hazardous event can be justified as low, the PL <sub>r</sub> may be reduced by one level.	Very high: Pr = 5 Likely: Pr = 4 Possible: Pr = 3 Rarely: Pr = 2  Negligible: Pr = 1
Possibility of avoiding or limiting harm	P1—Possible under specific conditions P2—Scarcely possible	Impossible: Av = 5 Possible: Av = 3 Probable: Av = 1



4.2. Safety Requirement Obtained

Depending on the standard used, one can obtain two different safety requirements for a same scenario defining a hazardous situation (Table 6).

Table 6. Theoretical test scenarios based on the two standards.

Scenarios	ISO 13849-1 (2015)						IEC 62061 (2005)				Remarks
Scenario 1	S	F	Pe	P	PL <sub>r</sub>	Se	Fr	Pr	Av	SIL	Remark 1
Harm: Laceration; Exposure: Once per shift; Prob. event: Very high; Avoidance: Impossible	S1	F1	-	P2	b	2	5	5	5	2	PL b and SIL 2 are not equivalent, meaning that depending on the standard being used, a different safety requirement is obtained.
Scenario 2	S	F	Pe	P	PL <sub>r</sub>	Se	Fr	Pr	Av	SIL	Remark 2
Harm: Fracture; Exposure: Once per 10 min; Prob. Event: Low; Avoidance: Possible	S2	F2	-	P1	d	3	5	2	3	1	PL d and SIL 1 are not equivalent, meaning that depending on the standard being used, a different safety requirement is obtained.
Scenario 3	S	F	Pe	P	PL <sub>r</sub>	Se	Fr	Pr	Av	SIL	Remark 3
Harm: Amputation; Exposure: Twice per shift; Prob. event: low; Avoidance: Possible	S2	F1	-	P1	c	4	5	2	3	2	PLc and SIL 2 are not equivalent, meaning that depending on the standard being used, a different safety requirement is obtained.
Scenario 4	S	F	Pe	P	PL <sub>r</sub>	Se	Fr	Pr	Av	SIL	Remark 4
Harm: Bruises; Exposure: weekly; Prob. event: high; Avoidance: impossible	S1	F1	-	P2	b	1	4	4	5	OM	PL b and SIL “other measure (OM)” are not equivalent, meaning that depending on the standard being used, a different safety requirement is obtained.
Scenario 5	S	F	Pe	P	PL <sub>r</sub>	Se	Fr	Pr	Av	SIL	Remark 5
Harm: Losing a finger; Exposure: Yearly; Prob: high; Avoidance: possible	S2	F1	-	P1	c	4	3	4	3	2	PL c and SIL 2 are not equivalent, meaning that depending on the standard being used, a different safety requirement is obtained.

4.3. Distribution of Performance Levels And Safety Integrity Levels

Annex A of ISO 13849-1:2015 suggests a tree-view risk graph allowing for determination of the required PL, based on chosen values of risk parameters. Table 7 shows the matrix version of that tree-view for a high probability of occurrence of the hazardous event.

Table 7. Converted risk graph for high probability of occurrence of the hazardous event.

	F1		F2	
	P1	P2	P1	P2
S2	PL c	PL d	PL d	PL e
S1	PL a	PL b	PL b	PL c

Table 8 represents the matrix version of the risk graph of ISO 13849 (2015) with a low probability of occurrence of the hazardous event.

**Table 8.** Converted risk graph for low probability of occurrence of the hazardous event.

	F1		F2	
	P1	P2	P1	P2
S2	PL b	PL c	PL c	PL d
S1	PL a	PL a	PL a	PL b

Tables 7 and 8 have more than one-unit difference when comparing the PL values regarding each level of severity. For example, in Table 7, when going from S2 to S1, their PLs are not consecutive: it goes from “c” to “a” in the “F1-P1” column instead of from “c” to “b” and so on. The risk graph of ISO 13849-1:2015 is therefore “overly sensitive to a single incremental change” Chinniah, et al. [42] of the severity parameter “S”, except in the F1-P1 case for a low probability of occurrence of the hazardous event. Having more than one unit change between adjacent cells reveals that parameter “S” contributes unevenly in the determination of the required PL [42]. On that point of view, the risk graph of IEC 62061 (2005) is better balanced (Table 1) due to more levels of severity available.

Recent studies on the architecture of risk estimation tools for machinery have shown that a unit change per cell is preferred as explained previously for Tables 7–9 [43–45].

**Table 9.** Risk graph for IEC 62061 using two severity of harm Se and probability of harm “CI”.

Se	CI = Fr + Pr + Av				
	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

#### 4.4. Common Cause Failures

The quantitative process for reducing common cause failures consists of a list of measures and associated values based on engineering judgement (Table 10). The following general measures are mentioned in both standards:

- Separation: Separating operation control systems from safety-related control systems
- Diversity: Different technologies and/or physical principles, e.g., programmable electronic system and hardwired, components from different manufacturers
- Design: protection against over-voltage, over-pressure, over-current, reliability of components
- Assessment: use of failure mode and effect analysis to avoid CCF
- Competence: Designers trained to understand CCF
- Environmental: Electromagnetic compatibility, immunity to temperature, shock, vibration, humidity

Measures against CCF are than estimated according to specified score thresholds (Table 11).

#### Common Cause Failures and the β-factor

The β-factor is a variable that originates in IEC 61508 and represents the contribution to the probability of dangerous failure of the system arising from the susceptibility of hardware components to dangerous random common-cause failures (CCF). The failure rate attributable to CCF (β) is added to the random failure rate of the hardware, i.e., adding to the likelihood of a hardware failure. The β-factor is determined using Equation (1).

$$\beta = \frac{n_{CCF}}{\lambda} \tag{1}$$

where

$\beta$  represents the ratio of CCF to the total failure rate

$n$ CCF represents the number of CCF

$\lambda$  represents the total number of failures

IEC 61508-6 (2010) provides detailed guidance on methods that can be used to calculate the  $\beta$ -factor [46], and IEC 62061 attempts to remove some of the analytical burden from standard users by providing a simplified method for selection of the  $\beta$ -factor based on a scoring checklist similar, but not identical to, that found in ISO 13849-1, see Table 10.

**Table 10.** Scoring process for measures against Common Cause Failure (CCF) from ISO 13849 and IEC 62061.

ISO 13849 Scoring Process for CCF		IEC 62061 Criteria for Estimating CCF	
Measures against CCF	Score	Item	Score
Separation/Segregation	15	Separation/Segregation	25
Diversity	20	Diversity/Redundancy	38
Design/application/experience	20	Complexity/design/application	2
Assessment/analysis	5	Assessment/analysis	18
Competence/training	5	Competence/training	4
Environmental	25	Environmental control	18
Other influences	10		
Total	100	Total	105

**Table 11.** Estimation of CCF.

ISO 13849 (2015)		IEC 62061(2005)	
Total Score	Measures for Avoiding CCF	Overall Score	CCF Factor $\beta$
$\geq 65$	Meets the requirements	$< 35$	0.1
$< 65$	Process failed	35–65	0.05
		65–85	0.02
		85–100	0.01

#### 4.5. Diagnostic Coverage

The diagnostic coverage (DC) is the fraction of the failure rate of detected dangerous failures ( $\lambda_{DD}$ ) to the failure rate of total dangerous failures ( $\lambda_{Dtotal}$ ). Improvements in DC will result in increased reliability of the system. The decrease in the probability of dangerous hardware failures resulting from the operation of the automatic diagnostic tests.

Following the methodology in ISO 13849, the performance level is estimated using quantifiable aspects (MTTF, DC, CCF, structure) and non-quantifiable aspects (behavior under fault conditions, software, systematic failure and environmental conditions). First, a block diagram representation (input, logic and output) is drawn. Each of the input, the logic and the output is performed by an SRP/CS. Second, depending on the availability of the PL of every SRP/CS, the estimation process of the performance level will differ. If the designer knows the PL of the SRP/CS, Table 11 of ISO 13849-1:2015 will be used to calculate the PL for series alignment of SRP/CS [5]. Otherwise, is the PL of an SRP/CS is unknown a thorough calculation and estimation process of the PL is required by the designer. That calculation and estimation process includes:

- Representing the block diagram (input, logic and output) for each channel.
- Calculating the mean number of annual operations called  $n_{op}$ . It is calculated using the mean operation in days per year, the mean operation in hours per day and the mean operation time between the beginning of two successive cycles of the component in seconds per cycle.
- Using the  $n_{op}$  and the  $B_{10D}$  value, calculate the  $MTTF_D$  for each component. The  $B_{10D}$  is the “number of cycles until 10% of the components fail dangerously (for pneumatic and electromechanical components)” [5].
- Finding the  $MTTF_D$  of each channel of the designated architecture.
- Calculating the combined  $MTTF_D$  (i.e., the  $MTTF_D$  of the whole designated architecture) and determining its level: Low, Medium or High (Table 13).
- Establishing the DC of each component using the tables in Annex E of ISO 13849-1:2015 [5].
- Calculating the average DC (Table 12).
- Evaluating the measures against CCFs.
- Determining the category (the designated architecture).
- Checking the software.
- Checking the measures against systematic failures.
- Determining the performance level based on the previous steps and according to the requirements of Figure 5 or Table 6 of ISO 13849-1:2015 [5].

**Table 12.** Diagnostic coverage as defined in the two standards.

ISO 13849		IEC 62061	
Diagnostic Coverage	%	Diagnostic Coverage	%
None	$DC < 60$	-	0
Low	$60 \leq DC < 90$	-	$60 < DC < 90$
Medium	$90 \leq DC < 99$	-	$DC > 90$
High	$DC \geq 99$		

**Table 13.** Mean time to dangerous failure of each channel.

ISO 13849-1:2015	
Years	
Low	$3 \leq MTTF_D < 10$
Medium	$10 \leq MTTF_D < 30$
High	$30 \leq MTTF_D \leq 100$

Following the IEC 62061 methodology, the SIL is estimated using quantifiable aspects (Probability of dangerous failure of the system, the CCF, test interval, DC, Sub-System Architecture) and non-quantifiable aspects (software).

There is no classification of DC as high, medium and low.

Contrary to the five designated architectures associated with the five categories (B, 1, 2, 3 and 4) proposed by ISO 13849, IEC 62061 describes four types of system architectures used in the analysis of random hardware failures, identified as Type A, B, C, and D (Table 14).

**Table 14.** System architectures used in the analysis of random hardware failures based on two standards.

Type (IEC62061)	Category (ISO13849)	Remarks
A	B and 1	Type A is single channel architecture similar to ISO 13849-1 Categories B and 1. This architecture has zero fault tolerance and no diagnostics.
B	-	Type B has no direct analogue in ISO 13849-1. This architecture is single fault tolerant but has no diagnostic capability. This structure is typical of a system with redundancy but no inherent diagnostic capability.
C	2	Type C is similar to ISO 13849-1 Category 2. This architecture is single channel, but has some degree of diagnostic capability.
D	3 and 4	Type D is similar to both ISO 13849-1 Categories 3 and 4. This architecture is single fault tolerant and has diagnostic capability.

Consideration of the effects of DC on the reliability of the system is integrated into the equations for calculating the failure rate for Types C and D only, as these are the only structures that include diagnostics.

There is no classification of MTTF as low, medium and high. The failure rate of each component is used to reach a failure rate for the system

Subsystems are used instead of predefined architectures of input, logic and output. The use of subsystems offers greater versatility in the design.

## 5. Conclusions

The existence of two functional safety standards focused on the machinery sector has been a significant problem for machine builders since IEC 62061 was published in 2005. At least one informal study by G. Steiger [47], has shown that the ISO13849 approach has much greater market acceptance than the IEC standard, despite the significant advantages that the IEC approach provides to designers such as consideration for complex electronic systems. ISO 13849 provides a significantly simplified approach to probabilistic functional safety analysis than that in the IEC standard, but that alone is not enough to account for the difference in market acceptance. The use of architectural categories that remained essentially unchanged from their first use in 1995 through the current edition of the ISO standard, along with the use of relatively familiar terminology and an acceptance of electromechanical subsystems by the analytical methodology was likely significant.

A significant shortcoming has been identified with respect to the availability of reliability data for fluidic components. Some testing has been done by European fluidic industry companies and organization, however, the sample sizes in the studies have been quite small leading to difficulty in generalizing the data. Early indications are that the figures provided in ISO 13849-2 Annex B for fluidic valves may be overly conservative [7], but no conclusions have been made available as yet.

Use of reliability data from sources outside of either the ISO or IEC standards can lead to errors in the final analysis if the basis of the data is not the same as that provided in the standard. Users of the standards need to be aware of this difference and should take steps to ensure that only a single source of data is used.

While the two standards offer the user a similar outcome in terms of a declared range of reliability, the two methods differ significantly in terms of the details of the methods. The differences mentioned in Section 4, were (i) parameters for estimating PL and SIL, (ii) safety requirement obtained, (iii) distribution of PL and SIL, (iv) common cause failures and (v) diagnostic coverage. Thus, system designers, technologists and engineers should be educated in using both standards so that they can make an informed decision regarding the most appropriate choice of method for a given design.

Further development work on a merged functional safety standard has been put on hold by ISO TC199 and Joint Working Group 1 was disbanded in 2018 [48]. However, work is continuing in both ISO TC199/WG1 and IEC TC44 to reduce the areas of conflict in the two standards with a view to eventually merging the two standards at some future date. Having a single standard would undoubtedly benefit the machinery sector and as well as the operators themselves, but despite the desire to achieve this goal, many roadblocks remain. Ongoing support for this work is needed to ensure that this goal will one day be met.

**Author Contributions:** Conceptualization, Y.C.; methodology, Y.C.; validation, Y.C.; formal analysis, Y.C.; investigation, Y.C.; writing—original draft preparation, Y.C., D.S.G.N., S.J., D.B.-V., and R.B.; writing—review and editing, Y.C.; reading and editing, B.K., and A.B.M.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

SRP/CS	Safety-Related Parts of a Control System
PPE	Personal Protective Equipment
SF	Safety Functions
PLCs	Programmable Logic Controllers
PL	Performance Level
SIL	Safety Integrity Level
E/E/PES	Electrical, Electronic and Electronic Programmable Systems
SIL1-4	Safety Integrity Levels
PFDavg	Probability of Dangerous Failure on Demand
PFHavg	average Frequency of dangerous Failure per Hour
PFHD	average Probability of dangerous Failure per Hour
OHS	Occupational Health and Safety
STSARCES	STandards for SAfety-Related Complex Electronic Systems
CCF	Common Cause Failure
SISTEMA	Safety Integrity Software Tool for the Evaluation of Machine Applications
HSE	Health and Safety Executive
OM	Other Measure
CCF	Common-Cause Failures
DC	Diagnostic Coverage

## References

1. ISO 10218-1. *Robots and Robotic Devices—Safety Requirements for Industrial Robots—Part 1: Robots*; International Organization for Standardization: Geneva, Switzerland, 2011.
2. ISO 10218-2. *Robots and Robotic Devices—Safety Requirements for Industrial Robots—Part 2: Robot Systems and Integration*; International Organization for Standardization: Geneva, Switzerland, 2011.
3. ISO 12100. *Safety of Machinery—General Principles for Design—Risk Assessment and Risk Reduction*; International Organization for Standardization: Geneva, Switzerland, 2010.
4. IEC 61496-1. *Safety of Machinery—Electro-Sensitive Protective Equipment—Part 1: General Requirements and Tests*; International Electrotechnical Commission: Geneva, Switzerland, 2012.
5. ISO 13849-1. *Safety of Machinery—Safety-Related Parts of Control Systems—Part 1: General Principles for Design*; International Organization for Standardization: Geneva, Switzerland, 2015.
6. IEC 62061. *Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*; International Electrotechnical Commission: Geneva, Switzerland, 2012.
7. ISO 13849-2. *Safety of Machinery—Safety-Related Parts of Control Systems—Part 2: Validation*; International Organization for Standardization: Geneva, Switzerland, 2012.

8. Malm, T.; Stålhane, T.; Bésche, C.D.; Venho-Ahonen, O.; Hietikko, M. From risks to requirements—A round robin test. In Proceedings of the 8th International Conference on the Safety of Industrial Automated Systems (SIAS-2015), Königswinter, Germany, 18–20 November 2015.
9. EN 954-1. *Safety Of Machinery—Safety-Related Parts Of Control Systems—Part 1: General Principles For Design*; British Standard: London, UK, 1996.
10. Brown, S.J.; Frost, S. *Annex 11—Applicability of IEC 61508 & EN 954—Taks 1: A study of the links & divergences between draft IEC 61508 and EN 954—Final Report of WP4*; European Project Stsarces (Standard for Safety Related Complex Electronic Systems); HSE: London, UK, 1998.
11. IEC 62061. *Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*; International Electrotechnical Commission: Geneva, Switzerland, 2005.
12. IEC 61508-1. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 1: General Requirements*; International Electrotechnical Commission: Geneva, Switzerland, 2010.
13. ISO 13849-1. *Safety of Machinery—Safety-Related Parts of Control Systems—Part 1: General Principles for Design*; International Organization for Standardization: Geneva, Switzerland, 1999.
14. IEC 61439-1. *Low-Voltage Switchgear and Controlgear Assemblies—Part 1: General Rules*; International Electrotechnical Commission: Geneva, Switzerland, 2011.
15. Haghghi, A.; Chinniah, Y.; Jocelyn, S. Literature review on the incentives and solutions for the bypassing of guards and protective devices on machinery. *Saf. Sci.* **2019**, *111*, 188–204. [[CrossRef](#)]
16. ISO 14119. *Safety of Machinery—Interlocking Devices Associated with Guards—Principles for Design and Selection*; International Organization for Standardization: Geneva, Switzerland, 2013.
17. ANSI B11.19. *Performance Criteria for Safeguarding*; American National Standards Institute: Washington, DC, USA, 2010.
18. Hauke, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Becker, K. Improvement of ISO 13849-1 as a result of practical feedback: Amendment. In Proceedings of the 8th International Conference on the Safety of Industrial Automated Systems (SIAS-2015), Königswinter, Germany, 18–20 November 2015.
19. ISO 23849. *Guidance on the Application of ISO 13849-1 and IEC 62061 in the Design of Safety-Related Control Systems for Machinery*; International Organization for Standardization: Geneva, Switzerland, 2010.
20. Kleinbreuer, W.; Kreuzkamp, F.; Meffert, K.; Reinert, D. *Categories for Safety-Related Control Systems in Accordance with EN 954-1*; BIA Report 6/97e; HVBG: Sankt Augustin, Germany, 1999; pp. 60–61.
21. Brown, S.J.; Frost, S. *Health & Safety Executive, Electrical and Control Systems Unit, Technology Division; A Study of the Links & Divergences between Draft IEC 61508 and EN 954*. STSARCES, WP4 Task1 Report Ref: STS-WP4-1001; HSE: London, UK, 1998.
22. Marsot, J.; Klein, R.; Pagliero, D.; Dei-Svaldi, D. Sécurité des machines et des équipements de travail-Circuits de commande et de puissance. In *Principes D'intégration des Exigences de Sécurité ED 913*; INRS: Paris, France, 2003.
23. Bourbonnière, R.; Paques, J.J.; Monette, C.; Daigle, R. *Guide de conception des circuits de sécurité-Introduction aux catégories de la norme ISO 13849-1:1999, R-405*; IRSST: Montreal, QC, Canada, 2005.
24. Hauke, M. *Functional Safety of Machine Controls: Application of EN ISO 13849*; DGUV: Berlin, Germany, 2009.
25. Baudoin, J.; Bello, J. *Aborder la Norme NF EN ISO 13849-1 via la Conception D'une Fonction de Sécurité Basique*; INRS: Paris, France, 2013.
26. Baudoin, J.; Bello, J. *Exemple Didactique D'application de la Norme NF EN 62061*; INRS: Paris, France, 2013.
27. Schmidt, F. Safety of machinery in Europe. In *New Information on 'Safety of Machinery and Machine Control Systems'*; Schmersal: Wupata, Germany, 2014.
28. Paques, J.J.; Durka, J.L.; Bourbonniere, R. Practical use of IEC 61508 and EN 954 for the safety evaluation of an automatic mining truck. *Reliab. Eng. Syst. Saf.* **1999**, *66*, 127–133. [[CrossRef](#)]
29. Poisson, P.; Chinniah, Y.; Jocelyn, S. Design of a safety control system to improve the verification step in machinery lockout procedures: A case study. *Reliab. Eng. Syst. Saf.* **2016**, *156*, 266–276. [[CrossRef](#)]
30. Zahálka, J.; Tůma, J.; Bradáč, F. Determination and Improvement of Performance Level of Safety Function of Emergency Stop for Machinery. *Procedia Eng.* **2014**, *69*, 1242–1250. [[CrossRef](#)]
31. Hata, Y.; Hirao, Y. Functional safety application for collaboration work of machines and persons on the basis of safety levels defined by position and velocity vectors. In Proceedings of the 8th International Conference on the Safety of Industrial Automated Systems (SIAS-2015), Königswinter, Germany, 18–20 November 2015.

32. Jones, D. Functional Decomposition from IEC 62061—How to determine individual safety functions. From requirement to implementation. In Proceedings of the 8th International Conference on the Safety of Industrial Automated Systems (SIAS-2015), Königswinter, Germany, 18–20 November 2015.
33. Hietikko, M.; Malm, T.; Alanen, J. Risk estimation studies in the context of a machine control function. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 767–774. [[CrossRef](#)]
34. Jocelyn, S.; Baudoin, J.; Chinniah, Y.; Charpentier, P. Feasibility study and uncertainties in the validation of an existing safety-related control circuit with the ISO 13849-1: 2006 design standard. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 104–112. [[CrossRef](#)]
35. IFA. Software-Assistant SISTEMA: Safety Integrity Software Tool for the Evaluation of Machine Applications. 2017. Available online: <https://www.dguv.de/ifa%3B/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp> (accessed on 24 October 2019).
36. Huelke, M.; Becker, K. IFA Matrix Method for development of safety-related application software. In Proceedings of the 8th International Conference on the Safety of Industrial Automated Systems (SIAS-2015), Königswinter, Germany, 18–20 November 2015.
37. Porras-Vázquez, A.; Romero-Pérez, J.A. A new methodology for facilitating the design of safety-related parts of control systems in machines according to ISO 13849: 2006 standard. *Reliab. Eng. Syst. Saf.* **2018**, *174*, 60–70. [[CrossRef](#)]
38. HSE. *Out of Control: Why Control Systems Go Wrong and How to Prevent Failure*; Health and Safety Executive: London, UK, 2003.
39. Villard, J. Accidents caused by the failure of safety components. In Proceedings of the 3rd Safety of Industrial Automated System Conference-SIAS 2003, Nancy, France, 15 October 2003.
40. Dźwiarek, M. An analysis of accidents caused by improper functioning of machine control systems. *Int. J. Occup. Saf. Ergon.* **2004**, *10*, 129–136. [[CrossRef](#)]
41. Chinniah, Y. Analysis and prevention of serious and fatal accidents related to moving parts of machinery. *Saf. Sci.* **2015**, *75*, 163–173. [[CrossRef](#)]
42. Chinniah, Y.; Gauthier, F.; Lambert, S.; Moulet, F. *Experimental Analysis of Tools Used for Estimating Risk Associated with Industrial Machines (Report R-684)*; IRSST: Montréal, QC, Canada, 2011.
43. Gauthier, F.; Chinniah, Y.; Burlet-Vienney, D.; Aucourt, B.; Larouche, S. Risk assessment in safety of machinery: Impact of construction flaws in risk estimation parameters. *Saf. Sci.* **2018**, *109*, 421–433. [[CrossRef](#)]
44. Chinniah, Y.; Gauthier, F.; Aucourt, B.; Burlet-Vienney, D. Validation of the impact of architectural flaws in six machine risk estimation tools. *Saf. Sci.* **2018**, *101*, 248–259. [[CrossRef](#)]
45. Gauthier, F.; Chinniah, Y.; Burlet-Vienney, D.; Aucourt, B. *Machine Safety—Hands-On Experimentation with Risk Estimation Parameters and Tools (Report R-980)*; IRSST: Montréal, QC, Canada, 2017.
46. IEC 61508-6. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3*; International Electrotechnical Commission: Geneva, Switzerland, 2010.
47. Steiger, G. *Questionnaire: Result of German Enquiry*; ISO TC199/JWG1 N25; DIW: Berlin, Germany, 2012.
48. ISO/IEC. *Directives, Part 1: Consolidated JTC 1 Supplement*; International Organization for Standardization: Geneva, Switzerland, 2018.

