Control Systems

Insights on ISO 13849-1

By Bruce W. Main and C. Fred Hayes

Imagine this scenario. You are asked to audit a machine and determine whether it is safe enough for use. Or, perhaps your firm is purchasing a new machine and wants to confirm its safety. The machine has two interlock switches on a guard door. Is it safe enough? To simplify the discussion, assume you determine that the switches are wired in parallel (Figure 1, p. 42). You are asked whether they should be wired in series to be safer.

What is your answer? The answer is important because it will affect safety and costs. If the wiring or components need to be changed, the company will incur significant costs and schedule delays. If the wiring is deemed acceptable, yet it is not, an employee could suffer a serious injury. The answer, of course, is "it depends." The application, reliability and quality of the components used, how the components are combined, and the system's ability to detect problems all play a role in determining the safety or adequacy of the control system.

This article highlights several factors of control system safety and discusses an important international machinery safety standard that applies to control systems, ISO 13849-1. Some significant areas addressed by the standard are reviewed, several controversies surrounding it are discussed, and guidance is provided to machinery suppliers and users on how to work effectively in the current situation.

Redundancy is generally considered as a means to increase control system reliability. Two switches are usually considered more reliable than one because the probability of failure is reduced. That is, unless a single switch is more reliable. Using two cheap switches may not be better than using a single high-quality switch. Two high-quality switches wired in parallel might be more reliable than two cheap switches wired in series. Two switches wired in series are generally considered a safer design because in the event that either switch fails the circuit is opened and the system stops. Two switches wired in parallel provide reliable operation because the system will continue to function even if one switch fails.

The application is important because a guard that prevents access to a cutting tool may be different from one used for a chemical process. With a cutting tool, a series circuit may be more appropriate to stop the tool if either switch fails. With a chemical process that is hazardous to interrupt midstream because of high pressures or flammability, a parallel circuit design may be more appropriate.

So how does one sort through these factors to arrive at a reasonable decision? The company wants a basic go/no-go decision on safety. What is your answer? A good place to start is to understand more about the industry standards that address safety control systems.

IN BRIEF

- **Audits of existing machinery and purchases of new machinery often involve reviewing safety control systems.**
- **Control systems on machinery are increasingly complex.**
- **Control systems standards are also complex and not necessarily scientific engineering documents.**
- **Safety professionals must be aware of the issues surrounding control systems to guide decisions so that safety and engineering budgets may be expended most effectively.**

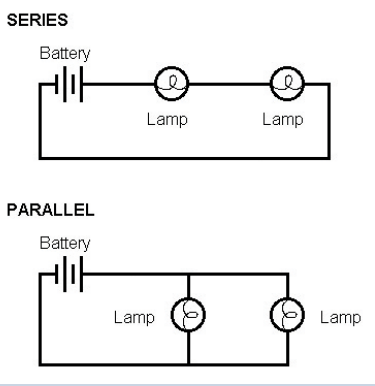
Bruce W. Main, P.E., CSP, is president of design safety engineering inc., an Ann Arbor, MI-based engineering consulting firm specializing in risk assessment and safety through design. Main holds mechanical engineering degrees from MIT and the University of Michigan, and an M.B.A. from University of Michigan. He is chair of ANSI B11.0, Safety of Machinery, chair of ISO TC 199/Working Group 5 that is responsible for ISO 12100, Safety of Machinery, and a member of several industry committees on risk assessment. He is also ASSE's representative to the B11 Committee on machine tool safety. A professional member of ASSE's Greater Detroit Chapter, Main has authored numerous articles, papers and books, including *Risk Assessment: Basics and Benchmarks* and *Risk Assessment: Challenges and Opportunities*.

C. Fred Hayes is director of technical services for PMMI, The Association for Packaging and Processing Technologies. He holds a B.S. in Mechanical Engineering and Engineering Administration from Michigan Technological University. Hayes has played a key role in the ongoing development of the ANSI/PMMI B155 packaging machinery safety standard. He is a member of ASSE's West Michigan Chapter.

Machine Control Safety Standards

Machine controls have evolved from simple hardware circuits to increasingly complex hardware and software systems. Although still used, relays have been supplanted by programmable logic controllers (PLCs) and more recently by safety-rated PLCs. Control systems use increasingly sophisticated complex integrated circuits, microprocessors and firmware. This has enabled great advancements in many respects, yet has added complexity to control system designs. When control systems fail to perform as expected, machines can move unexpectedly or not stop when expected, which can cause injuries or damage equipment or products. The more complex the systems, the greater the difficulty in identifying and preventing unintended consequences.

Figure 1
Simple Series & Parallel Circuits



Control system safety standards have also evolved from EN 954-1 (1996) to the more recent ISO 13849-1 (2006). The term *control reliability* has been used in the U.S. for several years, but much confusion remains regarding exactly what the term means. As a result, the definition as it relates to a specific control system is open to interpretation.

The term *functional safety* emerged as a result of the effort to evaluate the safety-related performance of control systems at the black box or functional level. Functional safety formed the basis for the standards that followed.

EN 954-1 (1996) and ISO 13849-1 (1999) introduced categories (B, 1-4) that provide the structure or architecture for control circuits. As the categories increase, the required architecture also increases, from single channel (a simple circuit) to monitoring (such as an indicator light), redundancy (two switches and/or two wires) and self-checking (active testing to ensure operational). Figure 2 illustrates the standard's guidance on category selection.

The 2006 revision of ISO 13849-1 introduced a probabilistic determination of potential control system failures. The standard's introduction includes the following:

> The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). These performance levels are defined in terms of probability of dangerous failure per hour.

The standard uses PLs as the metric used to discuss control systems (Figure 3, p. 44).

Initially, the standard was published with great expectations. Over the ensuing years, the effort to introduce reliability calculations has met some resistance in industry. Some are pushing to require the PL methodology while others are resisting that effort. The primary concerns can be summarized as follows: The theory, although apparently sound, does not work easily in practice.

As described in EN 954-1 and ISO 13849-1 (1999), categories have been largely adopted and used by machinery suppliers worldwide. Most machinery builders in the global marketplace are familiar with and use categories to design control systems. However, even though a revised version of ISO 13849-1 was published in 2006, few machinery suppliers and users in the U.S. are familiar with it. While machines will increasingly be built to this standard, it may take a decade or more before this occurs in great numbers, in part because of the complexity of control systems and of the standard itself.

For SH&E professionals, understanding the basics and central issues can inform negotiations with suppliers and aid decision making that affects safety and costs. The easy answer is, "We want the best/safest for our employees." Although an admirable sentiment, this is no smarter than walking into a car dealership and expressing the same thought. You will likely drive out with the top-line vehicle, a car loan, a service plan, an extended warranty and other extras that have little to do with your actual transportation needs.

In the past 2 years, three European companies that supply machinery have budgeted €250,000, €300,000 and €350,000 ($340,800, $409,000 and $447,470, respectively) to confirm that their machinery designs met ISO 13849-1 requirements. None changed their designs as a result of the analyses. Perhaps these funds would have been better spent to achieve actual safety improvements rathter than simply documenting compliance to a standard. As Manuele (2013) states:

> Resources are always limited. Staffing and money are never adequate to attend to all risks. The greatest good to employees, employers and society is attained if available resources are effectively and economically applied to avoid, eliminate or control hazards and the risks that derive from them. . . . [S]afety professionals must be capable of distinguishing the more significant from the lesser significant. (pp. 55-56)

Learning about ISO 13849-1 and control systems can help safety professionals achieve this goal.

Overview of the 2006 Standard

The 1999 version of the standard provided the architecture for control systems, but it lacked any mechanism for verifying or validating that these

systems operated as intended. The 2006 version attempted to address this by requiring reliability calculations to validate system performance. The intent was to provide a reliable and verifiable safety control system.

ISO 13849-1 is not a simple standard; it is a broad, complex document. The authors make no attempt to explain the standard in detail in this article. Instead, let's review its most significant elements.

Scope & Strategy

The scope of ISO 13849-1 (2006) follows, with emphasis added to highlight changes from the 1999 version:

> **Scope**
>
> This part of ISO 13849 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), *including the design of software.*
>
> For these parts *of SRP/CS,* it specifies characteristics that *include the performance level required for carrying out safety functions.*
>
> It applies to SRP/CS, regardless of the type of *technology and energy* used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery.
>
> It does not specify the safety functions or *performance levels* that are to be used in a particular case.
>
> *This part of ISO 13849 provides specific requirements for SRP/CS using programmable electronic system(s).*

The significant changes specifically include the design of software, all types of technology and use of performance levels rather than categories.

The general strategy presented for design appears in Clause 4 of the standard as follows:

> The key objective is that the designer ensures that the safety-related parts of a control system produce outputs which achieve the risk reduction objectives of ISO 14121 [an earlier risk assessment standard that was combined into ISO 12100 in 2010)]. . . . The greater the dependence of risk reduction upon the safety-related parts of control systems, then the higher is the required ability of those parts to resist faults. This ability . . . can be partly quantified by reliability values and by a fault-resistant structure.

Key Terms

The standard defines several terms that form the basis for the reliability calculations:

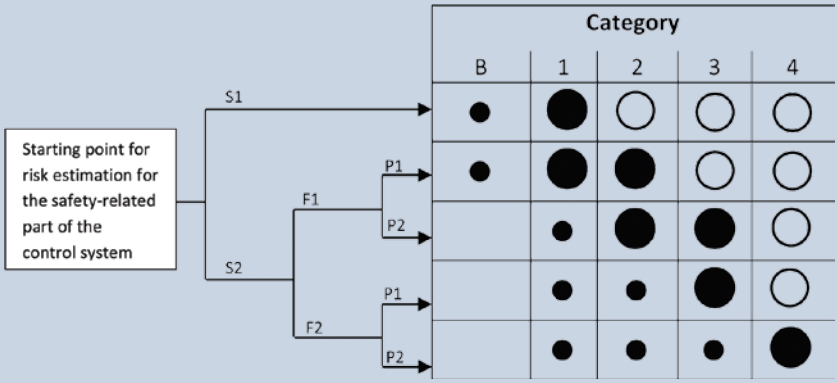
- **Category:** Classification of the safety-related parts of a control system with respect to their resistance to faults and their subsequent behavior in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability.
- **Common cause failure (CCF):** Failures of different items, resulting from a single event, where these failures are not consequences of each other.
- **Diagnostic coverage (DC):** Measure of the effectiveness of diagnostics; it may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.
- **Mean time to dangerous failure ($MTTF_d$).** Expectation of the mean time to dangerous failure.
- **Performance level (PL):** Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

Reliability Calculations

The calculated PLs correlate to the average probability of dangerous failures per hour ranging from 10^{-4} to 10^{-8} or less and are assigned PLs a-e (see the standard for the exact breakdown). To calculate the PLs, several parameters must be considered:

Figure 2

Possible Selection of Categories for Safety-Related Parts of Control Systems, ISO 13849-1 (1999)



Key

1 *starting point for risk estimation for the safety-related part of the control system (see 4.3, step 3)*

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 quite often and/or short exposure time
- F2 frequent to continuous and/or long exposure time

P *possibly of avoiding hazard or limiting harm*
- P1 possible under specific conditions
- P2 nearly possible

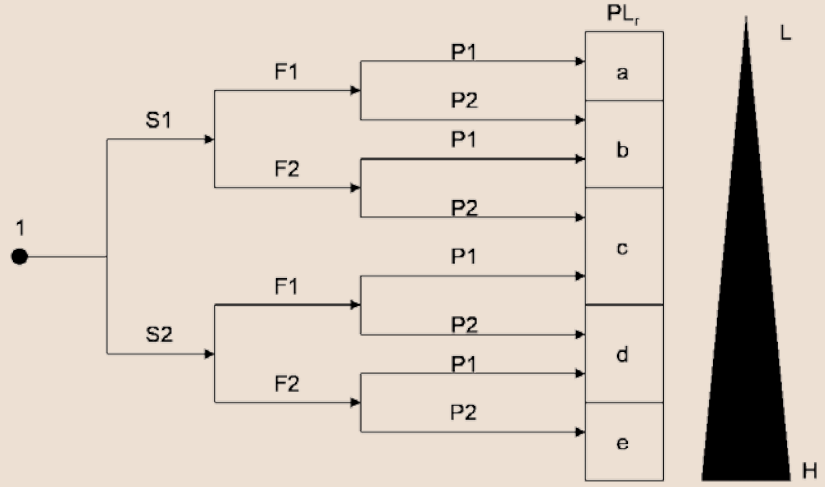
● **Preferred categories for reference points (see 4.2)**

• **Possible categories which may require additional measures (see B.1)**

○ **Measures which can be overdemensioned for the relevant risk**

Figure 3

Risk Graph for Determining Required PL_r for Safety Function



Key

1	*starting point for evaluation of safety function's contribution to risk reduction*
L	*low contribution to risk reduction/severity of injury*
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*

The PL of the SRP/CS shall be determined by the estimation of the following parameters:

- $MTTF_d$ value for single components (Annexes C and D in the standard);
- DC (Annex E);
- CCF (Annex F);
- structure (Clause 6);
- behavior of the safety function under fault condition(s) (Clause 6);
- safety-related software (Clause 4.6, Annex J);
- systematic failure (Annex G);
- ability to perform a safety function under expected environmental conditions.

These aspects can be grouped under two approaches in relation to the evaluation process:

a) quantifiable aspects ($MTTF_d$ value for single components, DC, CCF, structure);

b) nonquantifiable, qualitative aspects that affect the behavior of the SRP/CS (that is, behavior of the safety function under fault conditions, safety-related software, systematic failure and environmental conditions).

To comply with the standard, a machinery builder must convert circuit diagrams to logic flow diagrams. ISO 13849-1 provides two simple examples of converting a wiring diagram to a logic flow diagram in Annex I, one of which is illustrated in Figures 4 and 5 (p. 46). More generally, the control system architecture can be translated into logic flow diagrams (Figure 6, p. 47) as noted by Collins and Miller (2009).

Logic flow diagrams are considerably different from circuit diagrams. To perform the calculations, the circuit diagram must be morphed into a logic flow diagram. This involves some work, is not intuitively obvious and is confusing without some explanation. The examples provided in the standard are relatively basic designs; most machinery is more complex, and the standard provides little guidance in this regard.

In response, IFA developed the Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA). The free software (available at **www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp**) calculates the reliability values following the method specified in ISO 13849-1. To use the software, an engineer must enter the data, so data availability remains a challenge even with this tool.

Once logic flow diagrams are constructed, the engineer must calculate failure probability. Although this calculation is tedious, it is doable with the proper data. Certainly, the process presents many opportunities for computational errors and performing the calculations takes time, but in the end it is just math.

If doing the math were the most difficult part of ISO 13849-1, engineers would wade through the problem and get it done. However, this is only the beginning. To calculate the PL, three parameters must be estimated: $MTTF_d$, DC and CCF.

To estimate $MTTF_d$, an engineer must obtain reliability data from component suppliers. Many electronics controls suppliers have these data available, but hydraulic and pneumatic component suppliers are only beginning to develop these data. Obtaining such data on existing components can be even more difficult, if not impossible. When reliability data are unavailable, an engineer must estimate parameters. Although less preferred than using actual data, it can be acceptable if the standard provides reasonable estimate ranges.

To estimate DC, an engineer can use a look up table. Most of the values in the chart seem fairly reasonable because the values are specified or have a relatively narrow range. However, at least one example has a range that defies logic. "Cross monitoring of inputs without dynamic test" occurs quite often in machinery applications. The given DC range of 0% to 99% opens the value to interpretation, manipulation and error.

To determine the CCF estimate, several subparameters must be estimated and combined to achieve a rating. To pass, the total score must equal 65 or more (100 points maximum). The standard does not state the basis for the CCF score weighting. Furthermore, it is not clear why 65% is considered acceptable or why certain subparameters receive greater weighting than others. Users of the standard must simply accept that the weighting has validity.

Concerning this type of quantification, Manuele (2001) observes:

> Risk scorings begin with subjective judgments . . . and those subjective judgments are translated into numbers, not followed by any qualifying statements. What starts out as judgmental observations become finite numbers, which then leads to an image of preciseness. . . . Further, those numbers are multiplied or totaled to produce a risk score, giving the risk assessment process the appearance of having attained the status of science.

A component's reliability often depends significantly on how it is used in a design, thus a narrow range for a parameter cannot be provided in the standard. Where reasonable estimates are not available for the three parameters, an engineer must essentially guess at a value. For some parameters, the range for estimating is so broad as to make the calculations incredible. When guesses are used in the calculations and are then multiplied or totaled, Manuele's statement rings true.

To be clear, there is no indication that the reliability calculation in the standard is incorrect. The methodology uses sound math based on sound science. However, the calculations rely on good inputs, and the inputs are not necessarily robust. Incorrect or manipulated inputs can lead to falsely positive outputs. This makes performing the calculations a challenge, and verifying that the calculations and inputs are correct is an even greater challenge.

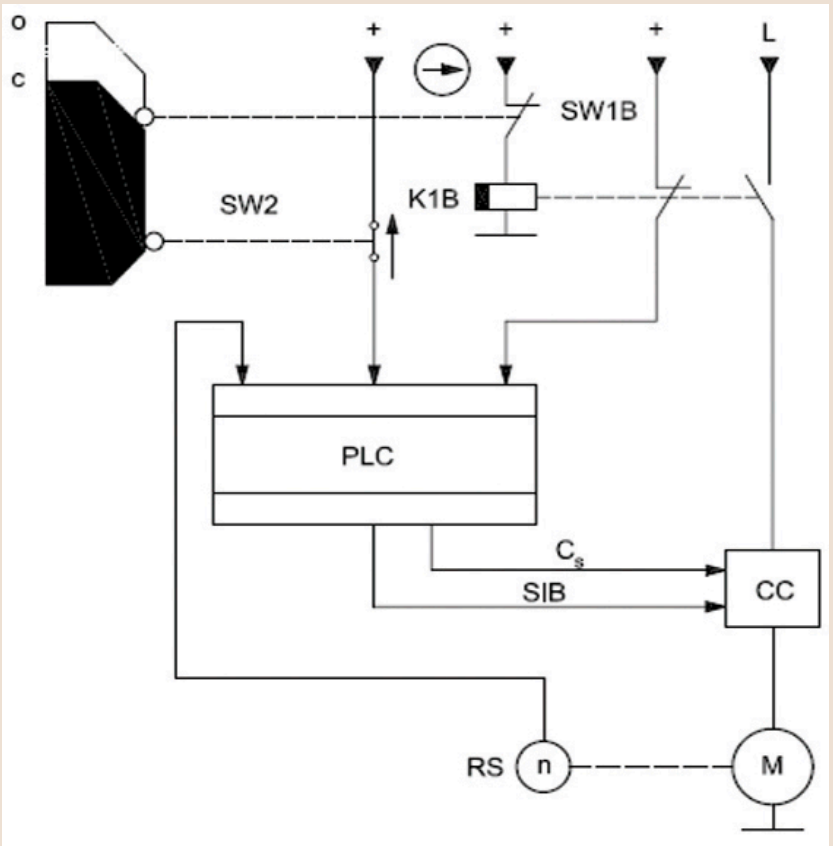
Fault Exclusion

The standard states, "The ability to resist faults shall be assessed." However, as noted in Clause 7.3, some faults can be excluded:

> **7.3 Fault Exclusion**
>
> It is not always possible to evaluate SRP/CS without assuming that certain faults can be excluded. For detailed information on fault exclusions, see ISO 13849-2 (2008).
>
> Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault. Fault exclusion can be based on:
>
> •the technical improbability of occurrence of some faults;
>
> •generally accepted technical experience, independent of the considered application;
>
> •technical requirements related to the application and the specific hazard.
>
> If faults are excluded, a detailed justification shall be given in the technical documentation.

The standard is not explicit on what exactly is included in fault exclusion. During meetings on this standard, the general impression has been that fault exclusion is a collection of elements that is difficult to quantify or estimate in terms of reliability, or does not relate to system architecture and is, thus, excluded. Examples of faults that have been excluded from evaluations include interlock key breaking off in the interlock switch; fasteners failing; and workers bypassing or defeating an interlock. However,

Figure 4
Wiring Circuit Diagram From ISO 13849-1 Example

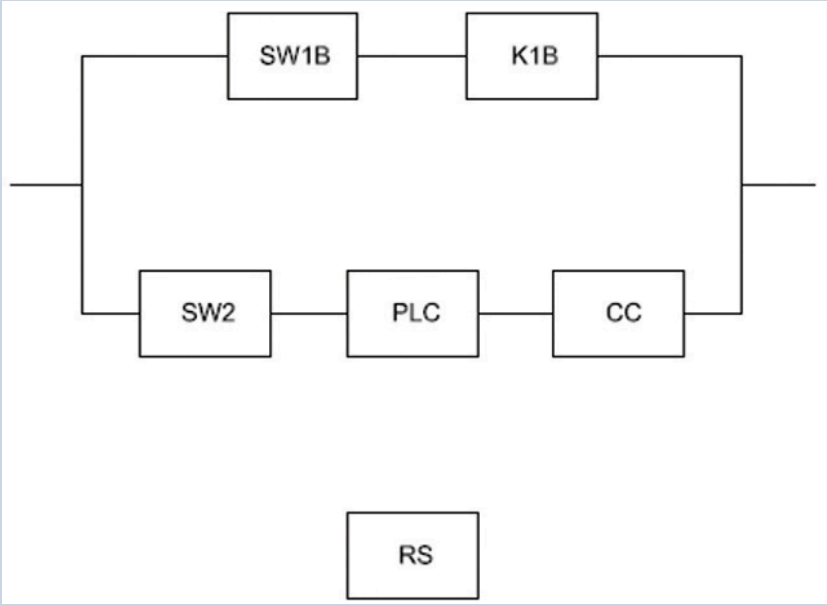


Key

PLC	*programmable logic controller*	*C_s*	*stop function (standard)*
CC	*current converter*	*SIB*	*safe impulse blocking*
M	*motor*	*K1B*	*switch (NC)*
RS	*rotation sensor*	*SW2*	*switch (NO)*
o	*open*		
c	*close*		

Figure 5

Logic Flow Diagram From ISO 13849-1 Example



SW1B and K1B guild up the first channel, SW2, PLC and CC build up the second channel; RS is only used to test the current converter.

Key

SW1B	*interlocking device*
K1B	*contactor*
SW2	*switch*
PLC	*programmable logic controller*
CC	*current converter*
RS	*rotation sensor*

anecdotal reports suggest that these types of failures are exactly the kind that result in harmful events—and far more frequently than other failures of control systems.

Software Reliability

The requirements for software safety include the following: "The main objective of the following requirements is to have readable, understandable, testable and maintainable software."

When coupled with the validation requirements, ISO 13849-1 can present a costly problem. If software is not coded with these requirements in mind, the validation and testable elements may be problematic. These requirements could necessitate recoding the software, a potentially expensive solution, or adding safety hardware to validate the software outputs, which also adds costs.

Validation

Efforts to comply with ISO 13849-1 are not limited to the design effort. The standard also applies to validation. Validation occupies a significant part of the standard; in fact, a separate standard, ISO 13849-2, was issued to define the validation requirements. Validation involves more than just testing that the system works. It requires creation of a validation document in addition to performing and recording the validation.

Discussion

What Problem(s) Does This Standard Address?

The standard does not specify the problems it aims to address. It provides the requirements for control system safety-related performance, but it does not identify a particular need for this standard. From a careful reading of the standard and the technical report, one can infer that the standard aims to prevent control system failures due to faults that occur from various sources. In particular, the 1999 technical report indicates two principal means to reduce risk: 1) reduce the probability of faults at the component level; and 2) improve the system's structure.

An implied problem with the 1999 standard is that it specifies architectures or structures without regard to component reliability or performance. For example, suppose that a pump is used to move material in a processing plant and that a Category 3 system is required. Since Category 3 requires redundancy, a second pump would be required to meet the requirements. However, assume that the first pump is oversized and reliable since it is only operating at less than half its capacity at full load. This is because the company stocks only one pump size to minimize and simplify spare parts inventory. Based on the pump's reliability and performance, a single pump should be sufficient. The 1999 version of the standard does not provide a means for such a decision to be made, but the 2006 version includes such provisions, as long as the pump system's PL meets the requirements.

The introduction of both the 1999 and 2006 versions of ISO 13849-1 state this intent:

> This part of ISO 13849 is intended to provide a clear basis upon which the design and performance of any application of the SRP/CS (and the machine) can be assessed, for example, by a third party, in house or by an independent test house.

The standard certainly achieved the objective of providing a basis on which to evaluate a control system. Whether it achieved the objective of being a "clear basis" remains doubtful, however.

Is This Really a Problem?

Assuming that the standard's purpose is, indeed, to prevent control system failures due to faults that occur from various sources, one must ask an ob-

vious question: Is this really a problem? Unfortunately, little information is readily available to determine an answer.

Data on actual incidents related to control system failures are difficult to obtain because incident reports rarely include such information and access to company incident reports is limited due to confidentiality concerns. For example, an incident report might include a statement that "the machine continued to run" or "did not stop" when a door or gate was opened, but the report would not likely identify this as a control system failure. Also, control system failures may not be determined until well after an incident occurs, so the incident report may not include this type of information. Finally, incident investigators may not have the expertise or experience to correctly identify or explain a control system failure.

Anecdotal information on control system failures is mixed. Many experts involved in incident investigations or accountable for occupational injuries report that few incidents relate to control system failures and that far more relate to poor system design; personnel bypassing or defeating control systems; mechanical failure of attaching hardware; broken interlock switches; or similar causes. Such failures are typically excluded in the ISO 13849-1 calculations under clause 7.3 (fault exclusion). Others contend that control system failures occur and have led to employee injuries. Companies that manufacture control systems are understandably silent on their control system failures. However, the magnitude of the problem, if it truly exists, has not been determined.

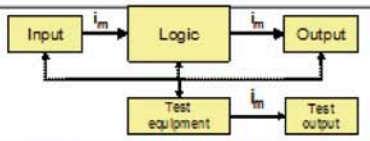
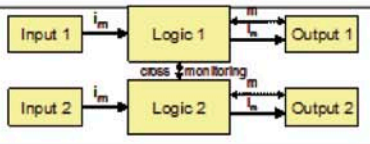
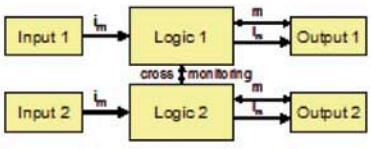
Photos 1 and 2 (p. 48) show an example of a control system problem. This interlock switch controls an access gate to a robot cell. The interlock switch is secured to the door frame and the key is (or was) retained by a cable attached to the gate door. Presumably, the key was secured to the door to prevent the key from inadvertently walking away in someone's pocket, as this would prevent the system from running. In use, however, the key was not removed from the gate prior to opening and eventually the cable failed.

Data on actual incidents related to control system failures are difficult to obtain because incident reports rarely include such information and access to company incident reports is limited due to confidentiality concerns. Also, control system failures may not be determined until well after an incident occurs, so the incident report may not include this type of information.

In this case, a single mechanical fault in the control system led to a loss of the safety function and noncompliance with ISO 13849-1, Category 3. In many cases, the control system effort focuses on only the electrical aspects and misses simple yet

Figure 6

Categories, Description & Logic Diagrams

Category B	When a fault occurs it can lead to the loss of the safety function	
Category 1	When a fault occurs it can lead to the loss of the safety function, but the $MTTF_d$ of each channel in category 1 is higher than in category B. Consequently the loss of the safety function is less likely.	
Category 2	Category 2 system behavior allows that: the occurrence of a fault it can lead to the loss of the safety function between the checks; the loss of the safety function is detected by the check.	
Category 3	SRP/CS to category 3 shall be designed so that a single fault in any of these safety-related parts does not lead to the loss of the safety function. Whenever reasonably possible the single fault shall be detected at or before the next demand upon the safety function.	
Category 4	SRP/CS to category 4 shall be designed so that a single fault in any of these safety-related parts does not lead to the loss of the safety function, and the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, at end of a machine operation cycle. If this detection is not possible an accumulation of undetected faults shall not lead to the loss of the safety function.	

Photos 1 and 2 show an access door controlled by an interlock switch with broken cable.

significant mechanical installation problems such as that shown in Photos 1 and 2. The problem illustrated in this example involves implementation of the control system rather than design. ISO 13849-1 does not address implementation even though many real-world problems occur as a result of implementation challenges.

What the Machine Directive Actually Requires

Compliance with ISO 13849-1 is often attached to the need to apply CE marking to a machine or to meet a user's specifications. A common misconception is that applying the CE mark requires compliance with the most current industry standards. This is not true. The Machinery Directive states that CE marking certifies that the machine meets the directive's essential health and safety requirements (EHSRs). This is an important distinction because it affects costs significantly. Decisions to upgrade or conform to the most current standards should be made knowing what is actually required.

Guide to the Application of the Machinery Directive 2006/42/EC contains the following guidance:

> § 87 The definition of "harmonised standard"
>
> Harmonised standards are essential tools for applying the Machinery Directive. Their application is not mandatory. . . .
>
> Even when a given essential health and safety requirement is covered by a harmonised standard, a machinery manufacturer remains free to apply alternative specifications. The voluntary nature of harmonised standards is intended to prevent technical standards being an obstacle to the placing on the market of machinery incorporating innovative solutions.

For the control system, neither the guide nor the directive specify that ISO 13849-1 must be used to meet the EHSRs. Machinery suppliers and users are free to use any standard they choose to meet the EHSRs. Often, industry standards are used to demonstrate compliance with the EHSRs. But suppliers remain free to use EN 954-1 categories for CE marking rather than the ISO 13849-1 PLs as long as they meet the EHSRs. However, some industries have diverged from this path and require ISO 13849-1 compliance as a condition of complying with industry standards (e.g., industrial robots).

Product Liability

ISO 13849-1 presents some significant concerns related to products liability in the U.S. This is not just a concern for U.S. machinery suppliers, it also affects every supplier that sells machinery in the U.S. market. Ironically, the mechanism in the EU intended to reduce supplier liability may increase supplier liabilities in the U.S.

If an injury can be remotely related to control system failure, the plaintiff attorney will likely claim that the machine was defective because the control system failed and that this failure caused the plaintiff's injury. Such a claim can be made without solid proof that the control system failed or that it actually caused the injury. In attempting to prove the claim, the plaintiff attorney will likely hire an expert witness who will develop an opinion that the machine was defective because the control system did not meet the requirements of ISO 13849-1 (2006).

To defend such a claim, the machine supplier must demonstrate that the control system did not fail, that the failure did not cause the injury or that the control system met the standard's requirements. The last option is the most challenging. A claim that the control system was defective creates the need to defend the system design. The machinery supplier may defend the claim using its own engineers or hire an expert witness to refute the plaintiff's expert's opinions. Note that in the EU, the court hires an expert to assist the judge. In the U.S., each party hires experts individually and the jury must sort through the differing opinions offered.

If the machinery supplier cannot clearly, simply and easily explain the control system operation and

how it met the standard, the jury will likely be confused. (Remember, engineers find some elements of ISO 13849-1 confusing; jury members likely will as well.) Having two opposing experts arguing about the details of ISO 13849-1 will only add to the confusion.

A machinery supplier must then defend its designs using the standard(s) to which it designs and to which it claims conformance. In the authors' opinion, a supplier conforming to EN 954-1 or ISO 13849-1 (1999) will enjoy a much greater likelihood of not confusing a jury than will one conforming to ISO 13849-1 (2006). Categories can be explained, but PLs and their justification are less straightforward. Given the history, complexity and potential confusion, the authors suggest that machinery suppliers with products liability concerns may wish to consider foregoing ISO 13849-1 (2006) or simply confirming compliance by performing the calculations but omitting statements of compliance from sales, marketing and similar documentation.

Where Is the Value?

Questions about the value derived from compliance are not easily answered. Figure 7 presents one possible answer. This figure demonstrates how different architectures can be combined with DC and $MTTF_d$ to achieve a required PL.

For example, the chart shows that depending on the mix chosen, a PL_d can be achieved using Category 3 or Category 2 architecture. The Category 2 architecture can provide a significant difference in costs, particularly on larger projects. However, although Figure 7 suggests that a Category 2 architecture can be adequate, customers often specify the architecture based on their experiences with the 1999 standard. This occurs in the packaging machinery industry where users tend to require Category 3 and PL_d machines. In these instances, the value of the ISO 13849-1 methodology becomes unavailable and it simply adds to product development costs.

If there is value in performance levels and ISO 13849-1, the market will recognize it and machinery suppliers and users will determine how to integrate its requirements into their machinery. Given the background and history of ISO 13849-1 as outlined in this article, simply adopting this standard because it is the newest version may create as many problems in machinery development as it attempts to solve.

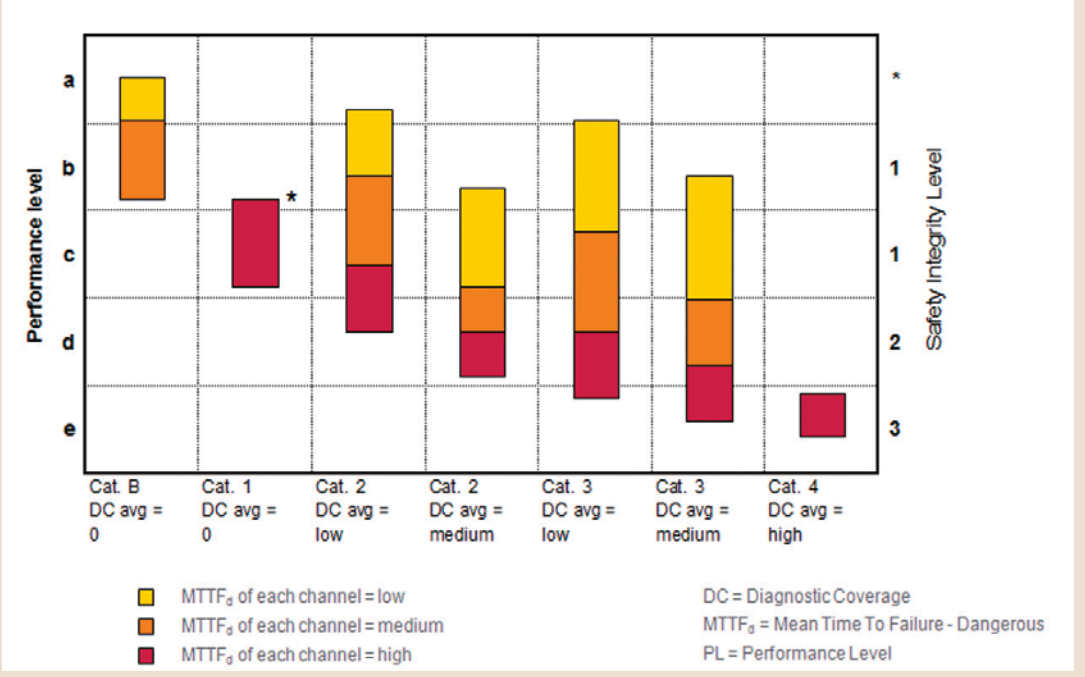
Presently, the international community is not likely to open ISO 13849-1 for a technical revision. However, there is interest and activity in developing guidance to help small and medium-size companies appropriately apply the standard.

Control Systems & Risk Assessment

The risk assessment for a machine should be separate from the risk assessment for a control system. ISO 13849-1 only addresses the safety-related parts of the control system and only applies once the risk assessment for a machine has determined that a control system is needed as a risk reduction measure. There is no reason to apply the risk assessment

Figure 7

Relationship Between Categories, DC_{avg}, $MTTF_d$ of Each Channel & PL



What matters most in the safety of machinery is reducing risk. Efforts that concentrate on compliance with standards often lose sight of this fundamental goal. Machinery suppliers and users need to keep this goal in mind and apply ISO 13849-1 and other standards when and where the standards help reduce risk.

for the machine to the control system, or vice versa. Doing so would only confuse participants.

Many hazards on a machine are unrelated to control systems (e.g., fall hazards from elevated work; slips and trips; ergonomic hazards from lifting/bending/twisting). PLs and categories have no meaning with these hazards, thus attempting to merge the machinery risk assessment and the control system specification is unwarranted. See ISO TR 22100-2 (2013) for further clarification.

Companion Standard

ANSI B11.26, Functional Safety for Equipment–Application of ISO 13849, provides guidance to understand and implement safety control functions and is a companion standard to ISO 13849-1. ANSI B11.26 illustrates safety control circuit design concepts and works to close the gaps between ISO 13849-1 requirements and the understanding of electrical, pneumatic and hydraulic safety circuits. The standard includes detailed annexes for understanding PLs and category block diagrams and detailed, nonvendor specific, schematic diagrams that are based on actual circuitry/products that have been successfully implemented in commerce.

ANSI B11.26 helps readers understand the activities required to:

1) Conduct a risk assessment.

2) Identify those hazards for which a safety-related control system will be used to reduce risk.

3) Define the safety function (what needs to happen).

4) Determine the risk reduction required for each safety function (category, PL_r, control reliability, SIL).

5) Design the SRPCS that make up each safety function. This also encompasses determining the failure modes to be managed; selecting the safeguarding device and/or complementary equipment; choosing the appropriate input device implementation; and selecting the appropriate output device implementation.

6) Evaluate the effectiveness of that system for the desired results. To achieve this, one must calculate the PL achieved of each safety function taking into account structure category, $MTTF_d$, DC, CCF. In addition, one must verify that $PL_d > PL_r$ for each safety function.

ANSI B11.26 is a technical document intended to help control engineers in implementing ISO 13849-1.

Reducing Risk Is Key

What matters most in the safety of machinery is reducing risk. Efforts that concentrate on compliance with standards often lose sight of this fundamental goal. Machinery suppliers and users need to keep this goal in mind and apply ISO 13849-1 and other standards when and where the standards help reduce risk. If a standard points to a solution that does not make sense, one should stop, conduct a risk assessment, develop a sensible solution that achieves acceptable risk and document the reasons for the decision. One should not simply blindly follow any standard.

For suppliers that have been building machinery for some time with no control system failures, few incentives exist to deviate from past successes simply to comply with ISO 13849-1. The authors recommend focusing on reducing risk rather than strictly on compliance because a compliance-only focus may inadvertently increase risks (G. Kopps, personal communication, 2006).

A company with a successful track record of control system performance should continue building machinery with the existing control systems. It may be beneficial to perform the calculations and determine the PLs of the machinery, but one should not allow a standard to dictate control system design if doing so increases risk.

A Prudent Course of Action

The best approach is to not rush to any major changes. This is especially true given the uncertainty of whether the problems even exist. Although control system failures may be a significant issue in complex machinery systems, most machinery applications do not have this concern or a notable history of failures.

It is also important to not simply jettison categories. Categories work. They provide the architecture or structure in the ISO 13849-1 standard, and are understood in the marketplace. They are not going away. The uncertainty related to the liability noted earlier is another reason to move slowly.

If a customer requires machinery built to a PL, then a supplier may need to work with ISO 13849-1 (2006). However, even then, it may be worthwhile to discuss the implications and the uncertainties with the customer. Sometimes, a customer writes a specification without fully appreciating the implications of the request and a discussion can clarify expectations and identify possible solutions.

For example, if a control system design has a successful track record in terms of safety and reliability, the customer may be able to accept use of that design and performance calculations without an outright statement of conformance to ISO 13849-1. The supplier could perform the necessary calculations to know the PL, yet not commit to conformance with the standard. This approach could limit product liability exposure as well.

The standard's PLs will likely become common and understood in time as machinery users and suppliers become familiar with the system, the requirements and the related challenges. However,

since there is no immediate need or requirement to use ISO 13849-1, there is also little incentive to rush to compliance.

Because they are international, ISO standards are often perceived as being superior, but this may not always be the case. This perception is likely driven by the desire to become globally common. This sentiment applies to machinery suppliers wishing to sell one design globally and also to users who wish to move equipment around the globe without modifications.

It is also important to note that ISO standards only include requirements for machinery suppliers. Requirements for machinery users cannot be included because the individual EU countries have workplace regulations that are the province of each country, a limitation that ANSI standards in the U.S. do not encounter.

Conclusion

Safety professionals have more to do with less time and resources than ever before. Life would be much easier if a safety audit were as simple as opening the electrical control panel, verifying that controls are the right color, then closing the doors and checking the audit box. Unfortunately, control systems are not so simple. No simple checklist exists and one cannot know whether the control system is safe enough without examining the details. Even high-quality components can be and have been combined in poor designs to yield poor (and expensive) results.

People expect industry standards to be scientifically engineered to provide the right answer and, thus, often perceive that complying with the standard, whatever it may be, achieves acceptable risk. While this is often the case, industry standards are consensus documents and not precise engineering analyses.

ISO 13849-1 presents many challenges. The standard is complex, which has caused some confusion and misunderstandings of its use, and it presents many opportunities for application errors. As noted, the theory, although apparently sound, does not work easily in practice.

The standard calls for a calculation of the reliability of the control system and its components based on the system architecture in a manner that can be verified. However, the input parameters for the calculation are often subjectively determined and in some cases so broadly applied that the credibility of the answers can be questioned.

The standard's methodology is based on sound math and science. However, the calculations rely on good inputs, and those inputs often are not so robust. As a result, the calculations are difficult to perform, and verifying that the calculations and inputs are accurate is an even greater challenge. Safety professionals will be well served to know of these challenges.

Perhaps the greatest challenge is the lack of clarity about whether the standard truly addresses the primary causes of injuries, control system failures, poor design or actions that bypass, defeat or break hardware mounting for control systems, which tend to be excluded from the calculations.

Some engineers who dig into the standard report finding value in it, particularly by enabling less costly solutions in meeting higher PLs. Others report deriving poor value because the time required does not justify the "benefits" obtained. Still others apply the standard with no significant problems. Time will tell how this plays out. **PS**

References

ANSI. (2014). Functional safety for equipment: Application of ISO 13849 (ANSI B11.26). New York, NY: Author.

BGIA Institute for Occupational Safety and Health of the German Social Accident Insurance. (2008). Functional safety of machine controls: Application of EN ISO 13849. Retrieved from **www.dguv.de/medien/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf**

Collins, D. & Miller, M. (2009). Understanding ISO 13849-1. Presentation at PMMI Safety Conference, July 14-15, Chicago, IL.

European Commission. (2006). Machinery directive 2006/42/EC. Retrieved from **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:EN:PDF**

European Commission for Standardization. (1996). Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design (EN 954-1). Brussels, Belgium: Author.

IFA. SISTEMA: Safety integrity software tool for the evaluation of machine applications. Retrieved from **www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp**

International Electrotechnical Commission (IEC). (2005). Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems (IEC 62061). Geneva, Switzerland: Author.

International Organization for Standardization (ISO). (1999). Safety related parts of control systems (ISO 13849-1-1999). Geneva, Switzerland: Author.

ISO. (2000). Guidelines for the use and application of ISO 13849-1 (ISO TR 13849-100-2000). Geneva, Switzerland: Author.

ISO. (2003). Safety of machinery—Basic concepts and general principles for design, Part 1: Basic terminology and methodology (ISO 12100-1). Geneva, Switzerland: Author.

ISO. (2006). Safety-related parts of control systems (ISO 13849-1-2006). Geneva, Switzerland: Author.

ISO. (2008). Safety of machinery—Safety-related parts of control systems, Part 2: Validation (ISO 13849-2-2008). Geneva, Switzerland: Author.

ISO. (2013). Safety of machinery—Relationship with ISO 12100; Part 2: How ISO 12100 relates to ISO 13849-1 (ISO 22100-2). Geneva, Switzerland: Author.

Manuele, F.A. (2001). *Innovations in safety management: Addressing career knowledge needs.* New York, NY: John Wiley & Sons.

Manuele, F.A. (2013). *On the practice of safety* (4th ed.). New York, NY: John Wiley & Sons.