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

Control system safety standards have also evolved from EN 954-1 but the term control reliability has been used in the U.S. for several years, but its meaning is unclear.

For a complete Table of Contents, see page 3
Control Systems Controversy: ISO 13849-1 continued from page 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 its meaning is unclear. As a result, there is ample opportunity for interpretation in the definition as it relates to a specific control system.

The term “functional safety” derived from the effort to evaluate the safety-related performance of control systems at the black box or functional level. This gave rise to the term “functional safety” and formed the basis for the standards that followed.

EN 954-1 (1996) and later 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 to monitoring, redundancy and self-checking.

Guidance on category selection is shown in Figure 1. In 2006, the new revision of ISO 13849-1 introduced a probabilistic determination of potential control system failures. The introduction to the 2006 standard 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 (PLs). These PLs are defined in terms of probability of dangerous failure per hour.”

The 2006 standard uses PLs as the metric used to discuss control systems (Figure 2).

Initially, the new ISO 13849-1 was published with great expectations. Over the ensuing years, the effort to introduce reliability calculations has met with resistance in industry. There are forces pushing to require the methodology of PLs as contained in ISO 13849-1 and forces resisting that effort. The problems can be summarized as the theory. Although apparently sound, it does not work easily in practice.

This article attempts to briefly highlight some of the more significant content of the standard, identify the primary controversies surrounding it and offer guidance to machinery suppliers and users on how to work with the current situation.

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

<table>
<thead>
<tr>
<th>Category</th>
<th>B</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred categories for reference points (see 4.2)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Possible categories that may require additional measures (see B.1)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Measures that can be over-dimensional for the relevant risk</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

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 Possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 nearly possible

**Overview of 2006 Standard**

Whereas the 1999 version of the standard provided the architecture for control systems, it lacked any real ability for verifying or vali-
dating that the operation of the system actually achieved the intended performance. The 2006 version of the standard attempted to address this situation by requiring reliability calculations to validate the system performance. The intent was to provide a reliable and verifiable safety control system.

ISO 13849-1 is a broad and complex document. This is not a simple standard. No attempt is made to explain the standard here in detail. Only the most significant highlights will be discussed.

**Scope & Strategy**

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

**1 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 in the scope include specifically the design of software, including all types of technology, and using PLs rather than categories.

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

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

**Necessary Definitions**

In discussing the standard, the following terms are important and defined in ISO 13849-1 because they form the basis for the reliability calculations that follow:

**Category**: classification of the safety-related parts of a control system in respect of 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, which 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 (MTTFd): 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.

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, the following parameters must be considered.

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

- the MTTFd value for single components [see Annexes C and D of ISO 13849-1 (2006)];
- the DC (see Annex E);
- the CCF (see Annex F);
- the structure (see Clause 6);
- the behavior of the safety function under fault condition(s) (see Clause 6);
- safety-related software (see 4.6 and Annex J);
- systematic failure (see Annex G);
- the 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 (MTTFd value for single components, DC, CCF, structure);

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

To comply with this standard, a machinery builder must convert circuit diagrams to logic flow diagrams. ISO 13849-1 provides two examples of converting a wiring diagram to a logic flow diagram in Annex I of the standard, one of which is excerpted in Figures 3 and 4.

More generally, the control system architecture can be translated into logic flow diagrams as noted by Collins and Miller (2009) in Figure 5.

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 relatively confusing without some explanation. The examples provided in the document are relatively simple designs, and most machinery is more complex for which little guidance is available in the standard.

In response to this problem of calculations and errors, the Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA) software program was developed by IFA, a German institute for research and testing of the German Social Accident Insurance. The software calculates the reliability values following the method of ISO 13849-1. The software download is available for free here. However, to use the software, the engineer needs to enter the data, so data availability remains a challenge even with the software.
Once the logic flow diagrams are constructed, the engineer then must calculate the probability of failure. This calculation is tedious but doable with the proper data. Every engineer has faced tedious problems. Many opportunities exist for computational errors and making the calculations takes time, but in the end, this is just math.

If doing the math were the most difficult part of ISO 13849-1, it would be completed. Engineers would wade through the problem and get it done. However, the fun only starts there. To calculate the PL, three parameters must be estimated: MTTF<sub>d</sub>, DC and CCF.

To estimate MTTF<sub>d</sub>, the engineer must obtain reliability data from the component suppliers. Many electronics controls suppliers now have the data available. Hydraulic and pneumatic component suppliers are only beginning to develop the data. Obtaining such data on existing components can be even more difficult if not impossible. In instances where reliability data are unavailable, the engineer must estimate parameters. This is less preferred than actual data but can be acceptable if reasonable estimate ranges are provided in the standard.

To estimate DC, the engineer can use a “lookup table.” Most of the values in the DC chart seem fairly reasonable because the values are specified or have a relatively narrow range. At least one of the examples has a range that defies logic. “Cross monitoring of inputs without dynamic test” occurs frequently in machinery applications. The given DC range of 0% to 99% opens the value to interpretation, manipulation and error.

In terms of the CCF estimate, several identified subparameters must be estimated and added up to achieve a rating. The total score must add up to 65 or better to pass (100 points maximum). The basis for the CCF score weighting is not stated in the standard. More explicitly, it is not clear why 65% is considered acceptable or why certain subparameters receive greater weighting than others. Readers must accept on faith that the weighting has validity.

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

“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.”

The reliability of a component 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, the 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.

**Fault Exclusion**

The standard requires that “The ability to resist faults shall be assessed.” However, some faults can be excluded as noted in Clause 7.3:

**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.
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; and
- technical requirements related to the application and the specific hazard.

If faults are excluded, a detailed justification shall be given in the technical documentation.

What exactly is included in fault exclusion is not explicitly clear in the standard. In ISO meetings where discussions have occurred about this standard, the impression given is that fault exclusion is a basket of elements that are difficult to quantify or to estimate in terms of reliability or do not relate to system architecture and are thus excluded. Examples of faults that have been excluded from evaluations include:
- interlock key breaking off in the interlock switch;
- fasteners failing;
- workers bypassing or defeating an interlock, etc.

Yet anecdotal reports also indicated that these types of failures are exactly the kind that result in harmful events—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**

However, the challenges of complying with ISO 13849-1 are not limited to the design effort. The standard also applies to validation. Validation occupies a significant part of ISO 13849 to the extent that a separate standard, ISO 13849-2, was created to define the validation requirements. Validation involves more than just testing that the system works. Validation requires that a validation document be created in addition to performing and recording the validation.

**Discussion**

*What Problem(s) Does This Standard Address?*

The standard does not explicitly answer this question. The standard provides the requirements for control system safety-related performance, but nowhere does it identify the particular need for this standard. From a careful reading of the standard and the technical report, one can infer that the purpose of the standard is to prevent control system failures due to faults that occur from various sources. In particular, the 1999 technical report indicates two principle means to reduce risk:

1) reducing the probability of faults at the component level;
2) improving the structure of the system.

An implied problem with the 1999 standard is that it specifies architectures or structures without regard to the reliability or performance of the components. For example, in a processing plant, assume a pump is used to move material and that a Category 3 system is required. Category 3 requires redundancy, thus a second pump would be required to meet the requirements. But 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 this type of decision to be made. To comply with the standard, a second pump would need to be added. In the 2006 version, this situation could be avoided provided the PL of the pump system meets the requirements.

Both the 1999 and 2006 versions of ISO 13849-1 include the following intent in the introduction:

“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 upon which a control system can be evaluated. Whether it achieved the objective of being a “clear basis” remains doubtful.

*Is This Really a Problem?*

Assuming that the purpose of the standard is indeed to prevent control system failures due to faults that occur from various sources, one question arises: “Is this really a problem?” Little information is readily available to determine an answer.

Data on actual incidents related to control system failures is difficult to obtain because incident reports rarely include such information, and access to company incident reports is severely limited due to confidentiality. 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. 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, thus 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 state that extremely 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. These failures are typically excluded in the ISO 13849-1 calculations under Clause 7.3, Fault excludability. Other experts contend that control system failures occur and have resulted in harm to personnel. Companies that manufacture control systems are understandably silent on failures of their systems, if any have occurred. However, no indication of the magnitude of the problem, if it really exists, has been determined.

**WHAT THE MACHINE DIRECTIVE ACTUALLY REQUIRES**

Compliance with ISO 13849-1 is often driven by the need for CE marking a machine or to meet a user’s specifications. A common misconception is that to apply the CE mark, a machine must comply with the most current industry standards. This is not true. The actual requirements of the machinery directive state that CE marking certifies that the machine meets the essential health and safety requirements (EHSR) of the directive.

In 2009, Guide to the Application of the Machinery Directive 2006/42/EC was published with the following guidance:

**§87 The Definition of “Harmonized Standard”**

Harmonized 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 harmonized standard, a machinery manufacturer remains free to apply alternative specifications. The voluntary nature of harmonized standards is intended to prevent technical standards from being an obstacle to the placing on the market of machinery incorporating innovative solutions.

For the control system, the guide and the directive do not specify that ISO 13849-1 must be used to meet the EHSRs. Machinery suppliers and users are free to use any standard they choose in meeting the EHSRs. Industry standards are often used to demonstrate compliance with the EHSRs. But suppliers remain free to use EN 954-1 categories for CE marking rather than the PLs of ISO 13849-1 as long as they meet the EHSRs. Different industries have diverged from this path and have required complying with ISO 13849-1 as a condition of complying with the industry standards.

**PRODUCTS 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, but impacts every supplier that sells machinery in the U.S. market. The very mechanism in the EU intended to reduce supplier liability may greatly increase supplier liabilities in the U.S.

In the event of an injury that can be remotely related to the failure of a control system, the plaintiff attorney will claim that the machine was defective because the control system failed and that the failure caused the plaintiff’s injury. This claim can be made without solid proof that any failure of the control system occurred 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 the claim, the machine supplier will need to demonstrate that the control system did not fail, that the failure did not cause the injury or that the control system met the requirements of the standard. The last option is by far the most challenging. The 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 may hire an expert witness of its own 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.

Generally speaking, juries that get confused tend to hand out money. If the machinery supplier cannot clearly, simply and easily explain the control system operation and how it met the standard, the jury will likely get confused. As noted throughout this article, ISO 13849-1 has ample opportunities for confusion, even to engineers let alone a jury of one’s peers. Having two opposing experts arguing about the details of ISO 13849-1 will most assuredly confuse a jury.

A machinery supplier will need to defend its designs using the standard(s) to which it uses in design and to which it claims conformance. A supplier conforming to ISO 13849-1 (2006) will thus need to defend its design without confusing the jury. The supplier conforming to EN 954-1 or to ISO 13849-1(1999) will enjoy a much greater likelihood of not confusing a jury. Categories can be explained, but PLs and their justification much less so. Given the history, complexity and potential confusion surrounding ISO 13849-1 (2006), machinery suppliers with products liability concerns may seriously wish to consider foregoing ISO 13849-1 or confirming compliance by doing the calculations but omitting statements of compliance from all sales, marketing and similar documentation.

**WHERE IS THE VALUE?**

This is a fair question that is not easily answered. One possible answer comes from Figure 6. This figure demonstrates how different architectures can be combined with DC and MTTFd to achieve a required PL.

For example, Figure 6 shows that depending on the mix chosen, a PLd 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, even though Figure 6 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 end users are tending to require Category 3 and PLd machines. In these instances, the “value” of the ISO 13849-1 methodology becomes unavailable and adds cost to developing the machinery.

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

There appears to be little appetite in the international community to open ISO 13849-1 for a technical revision. Although the current standard introduced no small amount of chaos, it appears to be somewhat stable chaos at the moment. There is interest and activity in developing guidance information to assist small and medium-sized companies in how to appropriately apply the standard.

**How Control Systems Relate to 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 attempt to apply the risk assessment for the machine to the control system or vice versa. Doing so will only tend to confuse participants. Many hazards on a machine are unrelated to control systems—fall hazards from elevated work, slips, trips, ergonomic hazards from lifting, bending, twisting, fire hazards, chemical exposures, noise, etc. PLs and categories have no meaning with these hazards unrelated to control systems.

Attempting to merge the machinery risk assessment and the control system specification is unwarranted and will likely further confuse readers.

**What Matters Most**

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 to reduce risk. Machinery suppliers and users need to keep this goal in mind and to apply ISO 13849-1 and other standards where and when the standards help reduce risk.

For machinery suppliers that have been building machinery for some time without control system failures, even less incentive exists to deviate from past successes simply to comply with ISO 13849-1. Focus on reducing risk rather than strictly compliance because a compliance-only focus may inadvertently increase risks (Kopps, 2006). If a company has a successful track record of control system performance, continue building machinery with the existing control systems. It may be beneficial to run the numbers and to determine the performance levels of the machinery, but do not let the standard dictate the control system design if doing so increases risk.

**What to Do**

For the time being, the best approach may be to not rush to any major changes. There need not be a hurry to change, particularly if the changes create more havoc and chaos than the problems they intend to solve. This is especially true given the uncertainty of whether the problems exist at all. 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.

Do not jettison categories. Categories work. Categories provide the architecture or structure in the ISO 13849-1 standard, and the marketplace understands categories. Categories will not go away.

The uncertainty related to the liability aspects of this standard are another reason to move slowly. ISO 13849-1 will likely increase products liability risk in the U.S.

If a customer requires machinery built to a PL, then the supplier may need to work with ISO 13849-1 (2006). Even then, discussing the implications and the uncertainties with the customer may be worthwhile. Sometimes customers write a specification without fully appreciating the implications of the request and with discussion can better understand the issues. In those circumstances, alternate solutions may be available.

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 calculations on the performance without an outright statement of conformance to ISO 13849-1. The supplier could do the math and perform the necessary calculations to know the PL but not commit to conformance or nonconformance with the standard. This approach could limit products liability exposure.

At this point, little doubt exists that PLs of ISO 13849-1 will become common and understood in time. Machinery users and suppliers will gain familiarity with the system, the requirements and the challenges as the standard is used. However, there is no immediate need or requirement to use ISO 13849-1. Given the controversial factors surrounding the standard, there appears to be little incentive to rush to compliance.

**CONCLUSION**

Many challenges are associated with ISO 13849-1 and its use. The standard is complex, which has led to confusion and misunderstandings of its use and opportunities for application errors even from its original publication. The problems can be summarized as the theory. Although apparently sound, it does not work easily in practice. Characterizing the situation as chaotic has some semblance of truth.

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 to the calculation are often subjectively determined and in some cases so broadly applied that the credibility of the answers can be questioned.

Perhaps the greatest challenge in ISO 13849-1 is that lack of clarity on whether it 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.

In many respects, the current situation with ISO 13849-1 is complete chaos and a predictable result of the rushed document development of the 2006 standard. Some engineers who really dig into the standard have found value in it, particularly by enabling less costly solutions in meeting higher PLs. Other engineers have dug in and have been completely frustrated and dismayed at the poor value derived—the time required does not justify the “benefits” obtained. Still other engineers are working with the standard without significant problems. Time will tell how this plays out.

**REFERENCES**


Bruce W. Main, P.E., CSP, is president of Design Safety Engineering, Inc. He served on the advisory committees for the Institute for Safety Through Design and Prevention through Design and is a member and/or chair of several industry committees on risk assessment. He is the convener (chair) of Technical Committee 199, Working Group 5 responsible for the ISO 12100 safety of machinery international standard. He is also the primary representative to the B11 Committee (machine tool industry) on behalf of ASSE. Main is a member of several professional engineering and safety organizations, having authored numerous articles, papers and books, including Risk Assessment: Basics and Benchmarks. He is a frequent lecturer on risk assessment and safety through design to industry and educational institutions. Main holds mechanical engineering degrees from the Massachusetts Institute of Technology and the University of Michigan as well as an M.B.A. from the University of Michigan.

C. Fred Hayes is director of technical services at PMMI and president of Hayes & Associates. He is responsible for monitoring all standards activity affecting packaging machinery manufacturers, helps revise the ANSI/PMMI B155.1 standards, serves on the B11 (machine tools) accredited standards committee and is a U.S. delegate to ISO Technical Committee 199, Safety of Machinery. For approximately 30 years, he was an owner of Hayes Machine Company, Inc., a manufacturer of cartoning machines, where he held various engineering and executive positions. Since 1972, he has been involved in writing safety and sanitation standards for packaging machinery through ASME and the PMMI B155.1 committee. In addition, Hayes presents hazard identification and risk assessment seminars to packaging machinery manufacturers and is an expert witness in liability litigation involving packaging machinery. Hayes holds degrees in Mechanical Engineering and Engineering Administration from Michigan State Technological University.

*Reprinted with permission. Originally published in Risk Assessment: Challenges and Opportunities (2012).*