Compliance inSight
Consulting Inc.

145 Deer Ridge Drive
Kitchener, ON N2P 2K9

T 519 • 650 • 4753

complianceinsight.ca
machinerysafety101.com

Evaluation Of Problems And Challenges In Csa Z434-14 Annex Dva Task-Based Risk Assessment Methodology

Douglas Nix, C.E.T., SM-IEEE

July 9, 2015

Abstract

Risk assessment is critical in the design of safe machinery. The methodology used must support the goal by providing a means to estimate risk that encompasses all of the relevant risk parameters. The risk parameters are defined in ISO 12100 [10], including the Severity of Injury and three probability terms, the Probability of the Hazardous Occurrence, the Frequency and Duration of Exposure, and the Possibility to Avoid or Limit Harm. Many tools are published that do not adequately reflect these parameters, including CSA Z434 [14], and ANSI RIA R15.06 [2]. This paper analyzes the problems inherent in this methodology and proposes a new system that meets the requirements and simplifies selection of functional safety Performance Levels or Safety Integrity Levels.

Keywords

Risk, risk assessment, risk reduction, risk control, robot, machinery, functional safety, safety integrity, safety function

DOI: 10.13140/RG.2.1.2929.3921

Contents

Introduction

This white paper is intended to address the long-standing issues persisting with the risk scoring methodology presented in CSA Z434, 2014 [1]. The issues addressed pre-date this edition of CSA Z434, going back to the origin of the method in ANSI RIA R15.06, 1999 [2].

Discussion at the technical committee level regarding these issues is often contentious. This paper sets out the problems inherent in the methodology, and proposes changes that address those problems.

Risk assessment is increasingly important in machine design, and in workplace risk control programs. Selection of a risk scoring tool that is comprehensive, effective, and follows widely accepted practices is important to the acceptance and effective implementation of risk control measures in the workplace. Canada has lagged behind the rest of the world in this area. Any improvement in approach that can be made will benefit workers, employers and the Canadian economy as a whole.

International Requirements

Background and History

The international requirements for machinery risk assessment and control have their origins in EN 1050 [3], the first widely accepted general standard on risk assessment. EN 1050 was published by the European Committee for Standardization (CEN), as part of the efforts to establish the CE Marking system in the European Union. It was one of the first standards harmonized under the EU Machinery Directive, along with EN 292-1 [4], and EN 292-2 [5]. EN 292 was eventually adopted into the ISO library of standards, and renumbered as ISO 12100-1 [6] and ISO 12100-2 [7]. EN 1050 was similarly adopted by ISO and renumbered as ISO 14121-1 [8], and a Technical Report, ISO/TR 14121-2 [9], was produced that provided supporting information on risk assessment methods and scoring tools. Eventually, ISO 12100-1, ISO 12100-2 and ISO 14121-1 were amalgamated into one standard, ISO 12100:2010 [10]. This is the document that sets the groundwork for machinery risk assessment methodology globally. Throughout the rest of this paper, this is the version of the standard that will be referenced, unless explicitly stated otherwise.

Purpose

The need to find a method to identify hazards, and rank them for control is the fundamental reason for machinery risk assessment. In the past, ranking was done exclusively based on the severity of injury. Called “Hazard Analysis”, this method failed to consider the probability aspects of risk that exist in the real world. Hazard analysis is now recognized as the second step in risk assessment, following Hazard Identification. Hazard Analysis is

now considered to encompass characterization of the hazard, and estimation of the likely severity of injury.

Using risk as the basis for ranking hazards provides a consistent and effective way to "bin" hazards, making prioritization of risk control efforts more straightforward.

Binning risks into a few broad bands helps to eliminate the "precision bias" that can creep into assessments. Precision bias is a mindset that places undue emphasis on the precision of the calculation, leading to overconfidence in the correctness of the results. This mindset can lead assessors into making incorrect assumptions about the accuracy of the assessment process, and this can lead to errors that result in workers being unnecessarily exposed to risk. Grouping risks into a few broad categories using an appropriately designed tool is one effective method of reducing the effects of "precision bias."

Methodology

The basic methodology in ISO 12100 requires that risk scoring tools address four risk parameters:

1. Severity of Injury (related to a particular hazard)
2. Frequency and/or duration of exposure to the hazard
3. Probability of the Hazardous Event
4. Possibility to avoid or limit harm

These factors are related graphically in Figure 1 [10, Fig.3].

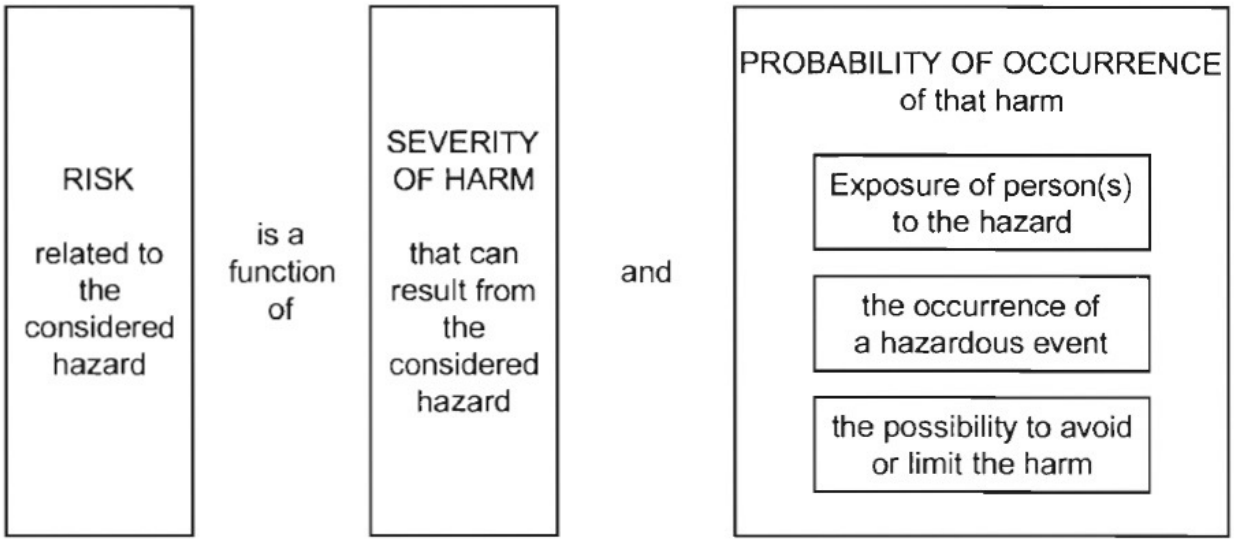


Figure 1 - Elements of Risk

Figure 1 does not represent any particular hierarchy in terms of the probability parameters, i.e., the Exposure parameter is not necessarily more significant than the possibility to limit harm. Figure 1 simply shows the parameters that should be considered and their general relationship. An alternate way to express the same concept is shown in Equation 1.

$$R\ f\ (S,P) \qquad \text{(Eq. 1)}$$

where

R represents Risk

S represents the Severity of Injury

P represents the aggregate Probability of Injury

The aggregate probability parameter can be further broken down as shown in Equation 2.

$$P\ f\ (Fr,Pr,Av) \qquad \text{(Eq. 2)}$$

where

Fr represents the Frequency or Duration of Exposure

Pr represents the Probability of the Hazardous Event

Av represents the possibility to Avoid or Limit Harm

Equation 3 shows equations 1 and 2 combined.

$$R\ f\ (S,Fr,Pr,Av) \qquad \text{(Eq. 3)}$$

These parameters can be combined in many ways, including arithmetic, i.e., as a product or a sum of the parameter values, or logically in the form of a decision tree. Mathematical treatments can include matrices that simplify the selection of a final risk value or a functional safety performance level [12] or safety integrity level [13].

ISO 12100 allows users to pick any scoring tool that suits their purpose, as long as it addresses at least the four basic parameters, severity, frequency/duration, probability of the hazardous event, and possibility of avoiding or limiting harm. All of these factors are explored in more detail in ISO 12100.

The scoring tool selected is the measuring system that will be used to assess the relative degree of risk presented by the identified hazards and the related tasks that bring workers into proximity with the hazard.

Parameter Weighting

The weighting of the risk parameters is very important. Weighting refers to the amount of change in the output value, risk in this case, that occurs with each change in the parameters. For example, if all the parameters are weighted equally, then a single unit of change in any parameter will result in a single unit change in the output value of the scale.

In occupational health and safety (OHS) practice, severity of injury is normally given the highest weight. In the past, rather than assessing risk, "Hazard Assessment" or "Hazard Analysis" was used. This approach ignored the probability factors entirely, and looked only to the severity of injury as the basis for making safeguarding decisions. This approach severely limited the ability to make sound decisions, since a hazard that represented a fatality would always, at least theoretically, get the same treatment, even if workers were very rarely present, or were present all day.

The typical decision trees, like that given in CSA Z434 [1], or in ISO/TR 14121-2, Annex A [9], have severity scales that are weighted heavily toward severe injuries, with much less weight given to the probability factors, if they are included at all.

Measurement Scale Characteristics

Measurement theory defines measurement as "the assignment of numbers to individuals in a systematic manner as a means of representing properties of the individuals", [11]. Scaling theory shows that there are four basic characteristics that must be considered when developing or selecting a measurement scale:

a) Distinctiveness

b) Ordering magnitude

c) Equal intervals

d) Absolute zero

Distinctiveness is the characteristic that allows us to distinguish the difference between a higher value and a lower value using the scale. **Ordering magnitude** ensures that an individual with less of the measured characteristic is assigned a lower magnitude than individuals with a higher amount of the characteristic. **Equal intervals** requires that the scale have equal intervals so that the relative values assigned to individual measurements can be compared. Strictly speaking, an **Absolute Zero** should be defined, so that individuals that do not exhibit the measured characteristic can be assigned a zero value. Absolute zero is problematic in OHS related risk assessment, since zero probabilities rarely exist. The severity score can go to zero, but only when the hazard is permanently eliminated.

A scale is considered to be an organized series of measurements, measuring one particular characteristic or trait of something that is being observed. Numbers assigned to measurements are called *scale values*. Scales that are not tested against a set of observations to de-

termine validity are “scaled by fiat”, meaning that the scale has been set solely by definition. Scales set by fiat can result in incorrect conclusions, since there is no means of testing the scale against a set of observations for validity.

Qualitative, i.e., meaning “determined by quality” rather than quantity of an item, and semi-quantitative scales are most commonly used in estimating machinery risk. These methods are used to guide decision making in the absence of quantitative data that could be analyzed using mathematical techniques.

The two common characteristics, scale-by-fiat, and the qualitative or semi-quantitative nature of these methods, can lead to incorrect conclusions by users of the scales. Ensuring that the scales used are clear and as straightforward to use as possible, thereby avoiding interpretation or interpolation by users, will help minimize the potential sources of error, reducing confusion and improving the end result.

These principles of measurement set the basis for consistent evaluation of measurement scales. Scales should be continuous within their range, i.e., without mid-scale gaps, and should be defined to represent the measured characteristics as best possible.

Input Scales

The input scales should have at least two values in order to be considered a scale. The number of values, or divisions, on the scale should be enough to describe the expected quality being measured, while not being so great as to yield nearly indistinguishable values.

For the purposes of machinery risk assessment, qualitative scales are commonly used. These scales are defined to match the characteristics of the risk parameter being analyzed. For most scales, two to five divisions per scale is enough to describe the important characteristics of the parameter.

Scale weighting should also be considered. If one parameter needs to be given greater weight in determining the output value from the tool, then the definitions of the scale values should reflect that weighting. If a semi-quantitative scale is being considered, then appropriate numeric weights can be assigned to the scale divisions so that the parameter affects the output of the scale appropriately.

The scales should be continuous, and should ensure that lower or lesser characteristics are ranked lower on the scale versus those with higher or greater characteristics.

Output Scale

Output scales for machinery risk assessment should have enough divisions to adequately describe the risk, without having so many divisions that the output values become hard to distinguish from each other.

To help avoid “precision bias”, the minimum number of divisions that adequately describe all possible combinations of the input risk parameters should be the starting point. Once the effects of each parameter on the output is understood, the number of output scale division may be reduced if desired, and assuming that no loss of clarity is created. This kind of reduction is often accomplished by “binning” values into a series of groups, e.g. 0-20 = Low, 21-40 = Medium, etc. This approach assists in reducing precision bias, and in setting priorities for treatment.

Problems and Challenges

The risk assessment tool given in [1, Annex DVB], provides scales for three parameters: Severity, Exposure, and Avoidance. Each scale will be addressed individually.

The first problem with this tool is the absence of a scale for Probability of the Hazardous Event. This parameter is significant particularly when analyzing the probabilities associated with infrequent or long duration exposures like those common in maintenance and service tasks. The absence of a "Probability of the Hazardous Event" scale prevents assessment of hazards that cannot be controlled using control system based safety functions, like injuries caused by noise, vibration, or poor ergonomic design. Absence of the Probability of the Hazardous Event scale fundamentally handicaps the user’s ability to assess the likelihood of injury.

Absence of a Probability of the Hazardous Event scale makes this tool non-conforming to ISO 12100.

Severity Parameter

The Severity Parameter scale is reproduced in Table 1. The Severity of Injury scale was modified in the third edition of CSA Z434, with the addition of a third value to the scale. This change allows better differentiation between serious non-fatal injuries, and non-reversible or fatal injuries. This change improves the differentiation of values on this scale.

The definitions for this scale appear to adequately describe the characteristic being measured, and no overlaps or gaps appear to exist between the definitions.

Table 1 - Severity (S) Scale

Factor	Rating	Criteria
Injury Severity	Serious S3	Normally non-reversible: • fatality • limb amputation • long term disability • chronic illness • permanent health change If any of the above are applicable, the rating is SERIOUS
	Moderate S2	Normally reversible: • broken bones • severe laceration • short hospitalization • short term disability • loss time (multi-day) • finger tip amputation (not thumb) If any of the above are applicable, the rating is MODERATE
	Minor S1	First aid: • bruising • small cuts • no loss time (multi-day) • does not require attention by a medical doctor If any of the above are applicable, the rating is MINOR

Exposure Parameter

The Exposure Parameter scale is reproduced in Table 2. The Exposure parameter is unchanged from the second edition of CSA Z434, except that the definitions of the scale values have been slightly modified. The current scale definitions and the previous definitions are given in Table 2 for comparison.

Table 2 - Exposure (E) Scale

Factor	Rating	2014 Criteria	2003 Criteria
Exposure	High E2	• Typically more than once per hour • Frequent or multiple short duration Durations/situations which could lead to task creep and does not include teach, see NOTE 1 If any of the above are applicable, the rating is HIGH	Typically exposure to the hazard more than once per hour (see notes below)
	Low E1	– Typically less than or once per day or shift – Occasional short durations If either of the above are applicable, the rating is LOW	Typically exposure to the hazard less than once per day or shift (see notes below)
CSA Z434-14 3rd Edition **NOTE 1** – Exposure can be affected by either a change in the frequency that the task is performed or by the application of lockout to control the hazard by isolating the energy source that reduces exposure to the hazard. Lockout (control of hazardous energy) should be considered for interventions in order to avoid situations leading to task creep, and ultimately situations where the worker can be exposed to hazardous energy which is not adequately controlled. Determining frequency of access can require judgment decisions by the person(s) performing the risk assessment. Access can range from cyclical production to maintenance tasks associated with periodic maintenance.		**CSA Z434-03 2nd Edition** Notes: 1) Exposure can be affected by either a change in the frequency with which the task is performed or by the application of an index R2 risk reduction safeguard or application of lockout to control the hazard by removal of the energy source that reduces exposure to the hazard.	

This scale has only two divisions, with a large gap between the upper time boundary of E2 and the lower time boundary of E1. This is the single biggest single problem with the “E” scale, and can be seen clearly in Figure 2.

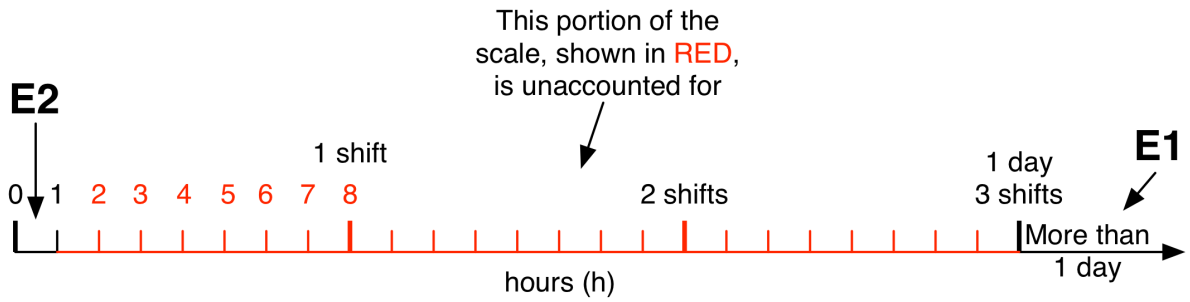


Figure 2 - CSA Z434 "E" Scale Gap

From Figure 2, it is clear that 23/24th of the the day used in the "E" scale is unaccounted for by the scale definition. This discontinuity leaves many tasks that happen more than once-per-day, but less than once-per-hour in limbo. Users are expected to somehow divine where in the undefined portion of the scale these tasks land, and then assess whether they are closer to an E1 or an E2!

Additionally, the definition for "E1" further confuses the matter by indicating that an E1 is "Typically less than or once per day or shift", while an E2 is "Typically more than once per hour". Definitions of this nature leave so much open to interpretation by users, that the likelihood of getting consistent results, even with the same group of people, is very low. One measure of the quality of a measurement scale is the ability to obtain consistent, comparable, results in a repeatable fashion. For example, a tape measure that provided a different measurement depending on who used it, or how recently they used it, would not be of much value.

Experience has shown that, given the choice, people will tend to opt for the choice leading to less work, or to achieving a low risk score that does not require any changes to the equipment or work practices. The design of the "E" scale makes this type of error very likely.

Note 1 is also problematic. The exposure parameter is useful for distinguishing which risk controls are most appropriate for a given hazard. Lockout is a risk control and should therefore not be considered in the initial assessment of the risk associated with a hazard. Failure to perform lockout, if selected as a risk control, will not effect the frequency of exposure to the area where a hazard could exist. It can effect the probability of a hazardous event, but the tool must have a scale to permit assessment of this parameter.

Avoidance parameter

The Avoidance Parameter scale is reproduced in Table 3. The avoidance scale provides an opportunity to assess the likelihood that a worker could avoid or limit the harm that might result from exposure to the hazard.

The scale definitions are continuous, and provide specific boundaries, e.g., insufficient clearance, 250 mm/s. This scale has a severe problem. If you consider A1 first, and find

any ONE of the criteria to be applicable then A1 could be selected even though the criteria of A2 is applicable as well.

If the criteria "may not perceive the hazard exists" is included in A2, there should be an opposite criteria in A1 such as "existence of the hazard can be easily perceived".

There is significant research [17], [18], and [19], that show that the 250 mm/s value assigned for avoidability is too fast. While this is outside the scope of this paper, it is worth noting that including specific factors like this in a scale definition can lead to errors in use and obsolescence if the thinking underpinning these factors changes.

Changes to these scale definitions are needed to improve this scale.

Table 3 - Avoidance (A) Scale

Factor	Rating	Criteria
Avoidance	Not Likely A2	• insufficient clearance to move out of the way • inadequate warning/reaction time • hazard is moving faster than reduced speed • (250 mm/s) • may not perceive the hazard exists If any of the above are applicable, the rating is NOT LIKELY
	Likely A1	• sufficient clearance to move out of the way • adequate warning/reaction time • hazard is moving at or less than reduced speed • (250 mm/s) If any of the above are applicable, the rating is LIKELY

Output Scale

The output of the CSA Z434 tool is given in terms of risk reduction priority, designated "PR". The scale is reproduced in Table 4. This scale is **NOT** in terms of risk, but rather results in specific recommendations for control measures. This feature moves this tool out of the realm of risk assessment, and into the realm of control measure selection. There is NO WAY to use this tool to determine residual risk, since the output is not in terms of risk.

This output scale is an attempt to map risk onto the hierarchy of controls. One of the fundamental aspects of the Hierarchy of Controls is that ALL control measures are applicable to all levels of risk, and the Hierarchy requires that each level in the Hierarchy be exhaust-

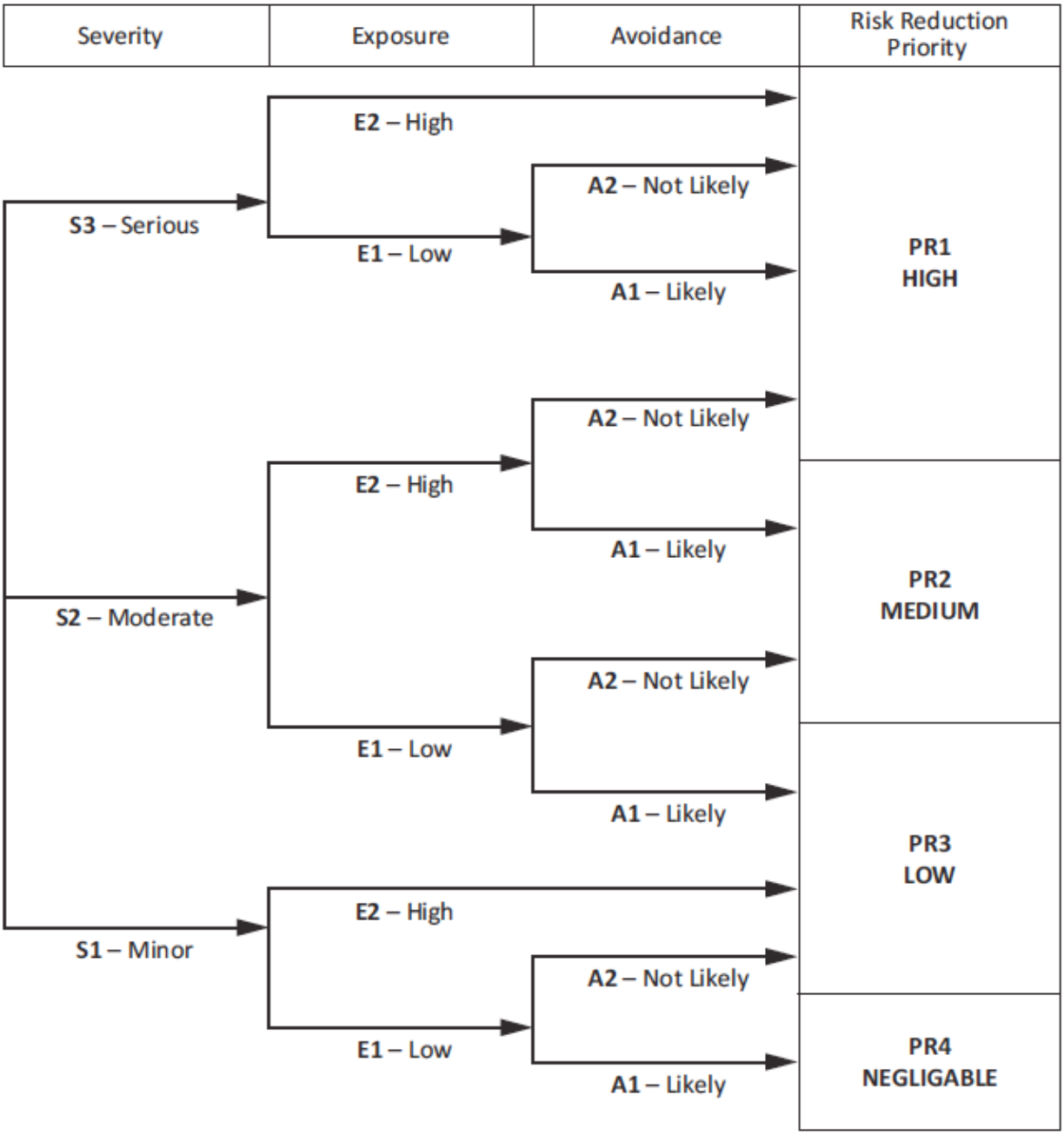
ed before moving to the next lower level. This table appears to exclude the use of some levels of control to some risks, an inappropriate interpretation of the hierarchy.

Table 4 - Risk Reduction Prioritization

<table>
<tr><th>Risk Reduction Priority</th><th colspan="3">Safeguarding Measures</th></tr>
<tr><td>PR1
HIGH</td><td rowspan="4">Inherently safe design measures
Hazard elimination or hazard substitution</td><td rowspan="2">Risk reduction by safeguarding</td><td>Fixed guard preventing access; engineering controls preventing access to the hazard, or stopping the hazard, e.g., interlocked guards, light curtains, safety mats, or other sensitive protective equipment implemented to meet a functional safety performance</td></tr>
<tr><td>PR2
MEDIUM</td></tr>
<tr><td>PR3
LOW</td><td rowspan="2">Complementary protective measures</td><td>Non-interlocked guards, clearance, procedures and equipment</td></tr>
<tr><td>PR4
NEGLIGIBLE</td><td>Awareness means</td></tr>
</table>

The use of four bins would appear to be reasonable, until the effect of each parameter is observed in Table 5 [1, Table DVA.1].

Table 5 - Decision Tree



As can be seen by following through each parameter, the S3 parameter has no effect on the outcome of the assessment. As such, it could be eliminated from the tool, or the output scale revised so that selection of S3 results in a higher order risk ranking.

No explanation is provided for the exclusion of the "A" parameter in the S3 > E2 chain, or in the S1 > E2 chain. This shows that these parameters are not considered significant in distinguishing the various degrees of risk resulting from the combinations of parameters, and results in some parameters being ignored.

The attempt to map directly from risk parameters to the Hierarchy of Controls is a significant error in the design of this system, resulting from a desire to simplify the selection of control measures as much as possible.

Probability of the Hazardous Event Scale

This scale is absent from the CSA tool as previously mentioned. This parameter is used to account for situations where exposure to the hazard does not immediately lead to injury. There are many factors that can influence this parameter, including:

- reliability and other statistical data,
- available incident history,
- near-miss history,
- comparison of risks from similar hazards

Both technical and human sources of exposure should be included when assessing this parameter. Human factors analysis, including cognitive loading, training frequency, and other factors can be significant contributors to this parameter.

Because reliability of safety-related control functions have an impact on this parameter, a tool that does not account for the probability of the hazardous event misses a key linkage to functional safety. The safety related control function PL [12] or SIL [13] has direct impact on the probability of the hazardous event, where risk mitigation relies on the safety function. Failure of a gate interlock, a light curtain, or a robot axis limit switch, can result in an immediate and potentially catastrophic, increase in risk.

Functional Safety Mapping

CSA Z434-14 provides mapping between the Risk Reduction Priority scale and the Performance levels defined in ISO 13849-1 [12]. The mapping is reproduced in Table 6.

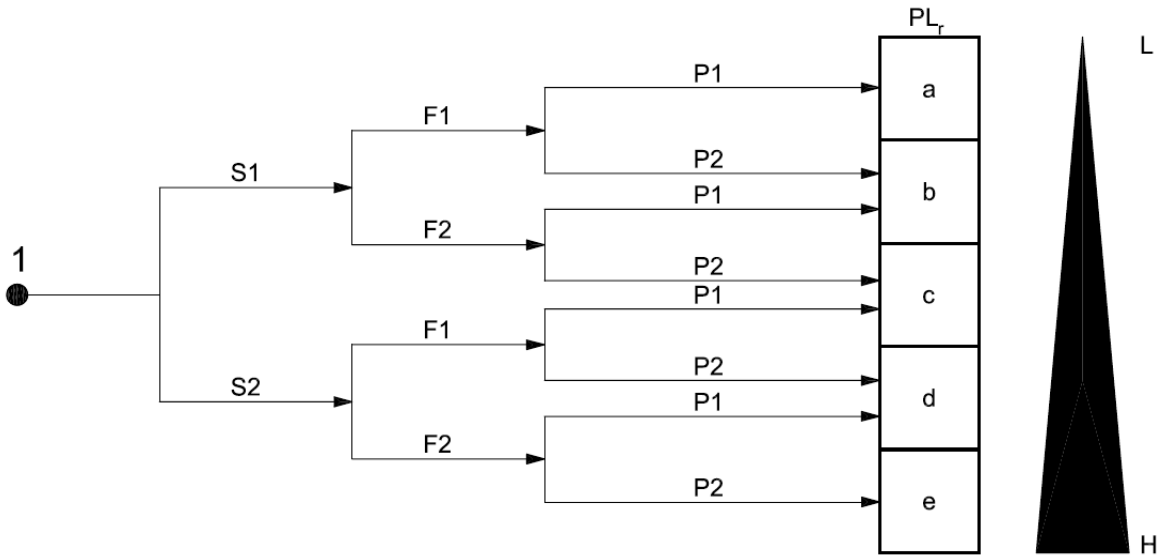
Table 6 - Minimum Functional Safety Performance [1, Table DVA.4]

Risk Reduction Priority	Functional Safety Performance Requirement for Safeguards Utilizing SRP/CS	
	Performance Level (PL)	Structure
PR1	d	3
PR2	d	2
PR3	c	2
PR4	b	1

The validate the mapping given in Table 6, a comparison with the “Risk Graph” in ISO 13849-1 [12, Annex A] was done. The Risk Graph is shown in Figure 3. In order to map the parameters, the definitions of the scales were compared, and the mapping shown in Table 7 was used. The results of the comparison are shown in Table 8.

Table 7 - Risk Parameter Mapping

CSA Z434 Risk Parameter	ISO 13849-1 Risk Parameter
S3	S2
S2	S2
S1	S1
E2	F2
E1	F1
A2	P2
A1	P1



Key

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

Risk parameters:

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

Figure 3 - ISO 13849-1 Risk Graph

Table 8 - Functional Safety Requirements

CSA Z434					ISO 13849-1			
S	**E**	**A**	**PR**	**PL**	**S**	**F**	**P**	**PL**
S1	E1	A1	PR4	b Cat 1	S1	F1	P1	a
S1	E1	A2	PR3	c Cat 2	S1	F1	P2	b
S1	E2	X	PR3	c Cat 2	S1	F2	P1	b
S2	E1	A1	PR3	c Cat 2	S1	F2	P2	c
S2	E1	A2	PR2	d Cat 2	S2	F1	P1	c
S2	E2	A1	PR2	d Cat 2	S2	F1	P2	d
S2	E2	A2	PR1	d Cat 3	S2	F2	P1	d
S3	E1	A1	PR1	d Cat 3	S2	F1	P1	c
S3	E1	A2	PR1	d Cat 3	S2	F1	P2	d
S3	E2	X	PR1	d Cat 3	S2	F2	P2	e
S3	E2	X	PR1	d Cat 3	S2	F2	P2	e

Note: “X” in Table 8 indicates that the parameter is not used.

As can be seen, the two approaches yield differing results in a number of cases. For example:

1. CSA PR4 results in a requirement for PL_b, Category 1, while the ISO method results in PL_a. PL_a can be achieved with Category B or 1 architectures. This decision on the part of the Z434 TC can be explained as an abundance of caution, since Category B architecture can be achieved in a single channel configuration with any components that are rated for the circuit conditions.

2. CSA PR3 results in PL_c, Category 2, while the ISO method results in PL_b. PL_b can be achieved with Category B through 3 architectures which include both single and dual channel designs with varying degrees of diagnostic capability.

3. In the case where S3, E1, A1 = PR1, PL_d, Category 3, the ISO method results in PL_c.

4. CSA PR1 results in PL_d, Category 3, while the ISO method results, for high frequency exposures (P2) in PL_e. The differnce between PLd and PLe is a full factor of magnitude in reliability, $PL_d = 10^{-7}$ failures/hour, $PL_e = 10^{-8}$ failures/hour of operation.

While the CSA Z434 TC made decisions that, with the exception of example 4, yield more conservative results, the overall result of this mapping is that machines built to the Canadian approach will have different Performance Levels than the same machine built using the ISO methods. This will result in confusion for integrators and machine builders, as well as users. Canadian standards that require a higher level of reliability than required by the International standards could be interpreted as a technical barrier to trade. This could result in suppliers ignoring the Canadian market in order to avoid the increased cost of unique designs for a small market. The result is that Canadian companies will have fewer choices of suppliers, and higher machinery costs.

Problem Summary

Summarizing the problems found with the CSA Z434 tool, in no particular order:

- the Severity Scale value "S3" has no effect on the output of the tool compared to "S2"
- the Exposure Scale has a large discontinuity that requires users to interpret the scale for intermediate values that fall into the discontinuity
- the Avoidance Scale parameter is not used in all branches of the decision tree
- the Output Scale is not in terms of risk, and is insufficiently granular to express all possible combinations of parameters.
- The limited effect of the higher two Severity divisions could be explained by weighting, however the lack of divisions representing all possible combinations begs the question "Why have this division at all?"
- The design of the tool limits the ability to do risk assessments
- The design of the scales drives the user to very conservative results, with the result being more expensive and complex solutions where they may not be warranted.
- Based on the identified problems, the design of this tool cannot be considered to be valid.
- The risk mapping to functional safety requirements yields results inconsistent with ISO methods, creating another area of confusion for users of the CSA method, without yielding any better results than would be achieved using the ISO methods directly.

Proposed Changes

1. Reject the CSA Z434 methodology completely, and follow the ISO methodology. This promotes harmonization, reduced confusion, and results in reduced barriers to trade without sacrificing user safety.

2. Adopt the Risk Scoring methodology shown below.

Risk Scoring Methodology

The algorithm used to determine the risk level is unique to this paper. Tables 9 and 10 show the final scoring matrix. Details of the method follow the Tables.

Table 9 - Risk Scoring Matrix

	Probability of Injury Class [Pr x (Fr+Av)]				
Severity	**3-10**	**11-20**	**21-30**	**31-40**	**41-50**
4	12-40	44-80	84-120	124-160	164-200
3	9-30	33-60	63-90	93-120	123-150
2	6-20	22-40	42-60	62-80	82-100
1	3-10	11-20	21-30	31-40	41-50

Table 10 - Approximate Risk Ranges

Approximate Risk Ranges				
1-10	11-20	21-100	101-150	151-200
Very Low	Low	Moderate	High	Very High

Note that there are overlapping areas between the approximate risk ranges. User judgement is required in these areas to determine if the risk should be scored in the lower of the two ranges. Risks should be prioritized based on the level of severity, i.e., two risks are scored at 90. One has a severity score of 3, the other a severity score of 4. This risk with severity level 4 should be binned into the “High” risk bin, rather than “Moderate”, based on the higher severity level.

Scoring Algorithm

The Risk Scoring Algorithm is weighted to give the Severity and Probability of the Hazardous Event parameters greater effect on the final risk score than either the Frequency and Duration of Exposure or Possibility of Avoidance parameters. The weighting was chosen in this way to prioritize risks with high-severity of injury consequences, and to give the Probability of the Hazardous event greater impact. In continuous exposure conditions, i.e., when Pr = 100 %, the Frequency (Fr) and Possibility to Avoid (Av) parameters become dominant, as would be expected based on observation of real-world work conditions. In other words, when a worker is continually exposed to the hazardous situation (Pr ap-

proaches 1), then the frequency of interaction with the hazard, Fr, and the worker's ability to avoid or limit harm during those exposures, Av, are what determine the likelihood of injury.

The Probability of the Hazardous event is very significant in OHS applications. This parameter can be used to account for a number of real-world effects, including:

- Predictability of the behaviour of component parts of the machine relevant to the hazard in different modes of use (e.g. normal operation, maintenance, fault finding).
- Probability of unexpected start-up of the machine
- Reliability of the Safety Related Control System
- Non-routine, non-repetitive tasks, such as unexpected repairs

The basic algorithm is shown in Equation 4.

$$R = Se \bullet [Pr \bullet (Fr + Av)] \qquad \text{(Eq. 4)}$$

where

R represents Risk

Se represents the Severity of Injury

Pr represents the Probability of the Hazardous Event

Fr represents the Frequency and Duration of Exposure

Av represents the Possibility to Avoid or Limit Harm

The sum of the Fr and Av terms limits their overall impact on the final risk score when Pr is less than 1, and aggregates them since they normally occur together in the real world. The Pr term multiplies the impact of the (Fr,Av) term based on the likelihood that a person will be exposed, and the whole probability term is multiplied by the Se term to derive the Risk score.

The use of the Pr term must be carefully considered. The probability of occurrence of hazardous event should be estimated independently of other related parameters Fr and Av. A worst-case assumption should be used for each probability parameter to ensure that risk is not inadvertently scored lower than it should be. To prevent this occurring, task-based analysis is strongly recommended to ensure that proper consideration is given to estimation of the probability of occurrence of the hazardous event.

"**Very high**" probability of occurrence of a hazardous event should be selected to reflect **normal production** constraints and worst case considerations. If the hazard being ana-

lyzed is due to the normal operation or motion of the machine, then it is 100% probable that it will occur, and should be scored at the highest level. Positive reasons (e.g. well defined application and knowledge of high level of user competences) are required for any lower values to be used.

The probability factors are calculated first, to provide a series of risk classes, which are then combined with severity in matrix form. This is done to simplify the risk matrix.

Equation 4 is shown in a matrix form in Table 9, with approximate risk bands shown in Table 10. These risk bands provide five "bins" that will generally group the assessed risks, helping to avoid precision bias. Note that there is significant overlap at the edges of the bands. This is also reflective of real-world conditions, as there are no well-defined break points between risk bands in real life.

Risk Parameter Scale Definitions

The parameter definitions are adopted from [13, Annex A]. Guidance for using the parameters is provided in [13], and reproduced here.

Severity (Se) Parameter

Severity of injuries or damage to health can be estimated by taking into account reversible injuries, irreversible injuries and death. Consider the most probable degree of injury expected for the exposure, i.e., slip and fall injuries can be fatal, but not all are fatal all the time. A fall to the same level is less likely to cause a fatality, than a fall to a lower level 20 m below.

Choose the appropriate value of severity from Table 11 based on the most probable consequences of exposure to the hazard, where:

4 means a fatal or a significant irreversible injury such that it will be very difficult to continue the same work after healing, if at all. Includes significant lost time, more than 1 month;

3 means a major or irreversible injury in such a way that it can be possible to continue the same work after healing. It can also include a severe major but reversible injury such as broken limbs. Includes limited duration lost time, where more than 1 week but less than one month is lost;

2 means a reversible injury, including severe lacerations, stabbing, and severe bruises that requires attention from a medical practitioner. Includes lost time where 1 week or less is lost;

1 means a minor injury including scratches and minor bruises that require attention by first aid. No lost time.

Table 11 - Severity Parameter Weights

Consequences	*Severity (Se)*
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Probability of occurrence of harm

The probability of the occurrence of harm is the aggregate probability of an injury occurring. The probability of the occurrence of harm parameter (P), is made up of three probability parameters: Probability of the Hazardous Event (Pr), Frequency and Duration of Exposure (Fr), and the Possibility to Avoid or Limit Harm (Av), Equation 2.

$$P \; f \; (Pr, Fr, Av) \qquad \text{(Eq. 2)}$$

Each of the three parameters of probability of occurrence of harm (i.e. Pr, Fr, and Av) should be estimated independently of each other. A worst-case assumption needs to be used for each parameter to ensure that the assessed risk is not scored lower than it should be. Generally, using some form of task-based analysis is strongly recommended to ensure that proper consideration is given to estimation of the probability of occurrence of harm.

Probability of occurrence of a hazardous event

Generally, consider whether the machine or material being processed has the propensity to act in an unexpected manner.

Machine behaviour will vary from very predictable to not predictable, but unexpected events cannot be discounted. Predictability is often linked to the complexity of the machine function. This parameter can be estimated by taking into account the :

- Predictability of the behaviour of component parts of the machine relevant to the hazard in different modes of use (e.g. normal operation, maintenance, fault finding).
- Probability of unexpected start-up of the machine
- Reliability of the Safety Related Control System
- Non-routine, non-repetitive tasks, like unexpected repairs

This will necessitate careful consideration of the control system regarding the risk of unexpected start up. Do not take into account the protective effect of any Safety Related Control System (SRCS). This is necessary in order to estimate the amount of risk that will be exposed if the SRCS fails. Protective effects can be assessed when the risk reducing effects of the potions of the Hierarchy of Controls are considered.

It is also important to take into account intended and foreseeable human behaviour when interacting with the machine relevant to the hazard. Some factors to consider include:

- stress (e.g., due to time constraints, work task, perceived damage limitation); and/or
- lack of awareness of information relevant to the hazard. This will be influenced by factors such as skills, training, experience, and complexity of machine/process.

A task analysis will reveal activities where total awareness of all issues, including unexpected outcomes, cannot be reasonably assumed.

Select the appropriate row for probability of occurrence of hazardous event (Pr) of Table 12.

Table 12 - Probability of Occurrence of the Hazardous Event (Pr) Weighting

Probability of Occurrence	***Probability (Pr)***
Very high*	5
Likely	4
Possible	3
Rarely	2
Negligible	1

* "**Very high**" probability of occurrence of a hazardous event should be selected to reflect **normal production** constraints and worst case considerations. Positive reasons (e.g. well defined application and knowledge of high level of user competences) are required for any lower values to be used.

Frequency and duration of exposure (Fr)

Consider the following aspects to determine the level of exposure:

- need for access to the danger zone based on all modes of use, for example normal operation, maintenance; and
- nature of access, for example: manually feeding material, setting, lubrication.

It should then be possible to estimate the average interval between exposures and therefore the average frequency of access.

It should also be possible to foresee the duration, for example if it will be longer than 10 min.

Where the duration is shorter than 10 min, the value may be decreased to the next level. This does not apply to frequency of exposure ≤ 1 h, which should not be decreased at any time.

Select the appropriate row for Frequency and Duration of Exposure (Fr) from Table 13.

Table 13 - Frequency and Duration of Exposure (Fr) Weighting

Frequency of Exposure	***Duration >10 min***
≤ 1 h	5
1 h to ≤ 1 day	5
> 1 day ≤ 2 weeks	4
> 2 weeks ≤ 1 year	3
> 1 year	2

Probability of avoiding or limiting harm (Av)

This parameter can be estimated by taking into account aspects of the machine design and its intended application that can help to avoid or limit the harm from a hazard. These aspects include, for example

- sudden, fast or slow speed of appearance of the hazardous event;
- spatial possibility to withdraw from the hazard;
- the nature of the component or system, for example a knife is usually sharp, a pipe in a dairy environment is usually hot, electricity is usually dangerous by its nature but is not visible; and
- possibility of recognition of a hazard, for example electrical hazard: a copper bar does not change its aspect whether it is under voltage or not; to recognize if one needs an instrument to establish whether electrical equipment is energized or not;
- ambient conditions, for example high noise levels can prevent a person hearing a machine start;

- presence of any Complementary Protective Measures, i.e., emergency stop, enabling devices, hold-to-run controls, etc.

Select the appropriate row for probability of avoidance or limiting harm (Av) of Table 14.

Table 14 - Possibility to Avoid or Limit Harm (Av) Weighting

Possibility	***Weight***
Impossible (Probability approaches 0%)	5
Rarely (Probability < 50%)	3
Probable (Probability approaches 100%)	1

The Risk Matrix presented in this paper is consistent with sound scaling theory, provides an output in terms of Risk, and provides a means to map risk to functional safety Performance / Safety Integrity Levels that is consistent with ISO 13849-1, Amd. 1 when published in 2015.

Functional Safety Mapping

The risk scoring methodology discussed above uses risk parameter scales that are unchanged from their source in IEC 62061. This provides a unique advantage, in that direct parameter mapping is automatically provided. No additional mapping from the risk scoring methodology to the functional safety integrity level scoring is required, only recalculation using the IEC 62061 algorithm.

For example, consider a risk scored as follows:

Se = 4, Irreversible: death, losing an eye or arm

Pr = 5, Very high

Fr = 5, ≤ 1 h

Av = 3, Rarely (Probability < 50%)

Substituting into Equation 4, the risk score would be

$$R = 4 \times [5 \times (5+3)] = 160$$

Determining the required SIL using the IEC 62061 matrix provides the following.

Table 15 - SIL Selection Matrix [13, Table A.6]

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

To determine the Class (Cl), Equation 65 is used.

$$Cl = Fr + Pr + Av \quad \text{(Eq. 5)}$$

Substituting into Eq. 5:

$$Cl = 5 + 5 + 3 = 13$$

Using Table 15, the SIL selection matrix, SIL 3 is located at the intersection of Se 4 and Cl 11-13, as shown below. This would not be an unreasonable reliability requirement for this severity of risk.

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

If the functional safety requirement is preferred in PL, reference to Table 15 provides this direct mapping. Using Table 15, SIL 3 maps to PL_e.

Table 15 - Relationship between performance level (PL) and safety integrity level (SIL) [12, Table 4]

PL	SIL (IEC 61508-1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

Conclusions

The methodology used in RIA R15.06, CSA Z434, and the second edition of CSA Z432 has been problematic for many years. The gap in the E scale, and the output in terms of safeguarding measures, along with the confused validation method provided in the standards have created much confusion for users. Ongoing development in machinery risk assessment methods internationally have lead to increasingly useful risk models, coupled with the hierarchy of controls and more recently, functional safety requirements, have outstripped the old models proposed by the RIA and CSA documents.

Revision or replacement of these models to eliminate the gaps, correct the misunderstandings, and provide better guidance to users is due. Small changes to the old models are not enough to correct the problems.

Harmonization with international models will eliminate technical barriers to trade, and facilitate both the export of Canadian built machinery to the rest of the world, and the import and use of machinery from other markets in Canada. Further delays in meeting our harmonization goals do not serve Canada's manufacturers, the users of CSA machinery standards, or our country's national economic interests.

Definitions

functional safety

part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities [16. 3.1.9]

harm

physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment [16. 3.1.1]

hazard

potential source of harm [16, 3.1.2]

hazardous situation

circumstance in which a person is exposed to at least one hazard
NOTE The exposure can result in harm immediately or over a period of time. [16, 3.1.3]

hazardous Event

event that can cause harm

NOTE A hazardous event can occur over a short period of time or over an extended period of time. [16, 3.1.4]

hazard zone (danger zone)

any space within and/or around machinery in which a person can be exposed to a hazard. [12, 3.12]

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

[12, 3.1.23]

required performance level (PL_r)

performance level (PL) applied in order to achieve the required risk reduction for each safety function

[12, 3.1.24]

risk

combination of the probability of occurrence of harm and the severity of that harm [16, 3.1.5]

tolerable risk

risk which is accepted in a given context based on the current values of society [16, 3.1.6]

residual risk

risk remaining after protective measures have been taken [16, 3.1.7]

safety

freedom from unacceptable risk [16, 3.1.8]

safety function

function to be implemented by an E/E/PE safety-related system, other technology safety related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the equipment under control (EUC), in respect of a specific hazardous event (see 3.4.1) [16, 3.5.1]

safety integrity

probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

NOTE 1 - The higher the level of safety integrity of the safety-related systems, the lower the probability that the safety-related systems will fail to carry out the required safety functions.

NOTE 2 - There are four levels of safety integrity for systems (see 3.5.6).

NOTE 3 - In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) which lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, the safety integrity of a system also depends on many factors which cannot be accurately quantified but can only be considered qualitatively.

NOTE 4 - Safety integrity comprises hardware safety integrity (see 3.5.5) and systematic safety integrity (see 3.5.4)

NOTE 5 - This definition focuses on the reliability of the safety-related systems to perform the safety functions (see IEV 191-12-01 for a definition of reliability).

[16, 3.5.2]

safety integrity level (SIL)

discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE - The target failure measures (see 3.5.13) for the four safety integrity levels are specified in tables 2 and 3 of IEC 61508-1.

[16, 3.5.6]

safety–related part of a control system (SRP/CS)

part of a control system that responds to safety-related input signals and generates safety-related output signals

NOTE 1 The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

NOTE 2 If monitoring systems are used for diagnostics, they are also considered as SRP/CS.

[11, 3.1.1]

safety requirements specification

specification containing all the requirements of the safety functions that have to be performed by the safety-related systems

NOTE - This specification is divided into the

- safety functions requirements specification (see 3.5.9);

- safety integrity requirements specification (see 3.5.10).

[16, 3.5.8]

verification

confirmation by examination and provision of objective evidence that the requirements have been fulfilled

NOTE 1 - Adapted from IS0 8402 by excluding the notes.

NOTE 2 - In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PES and software), by analysis and / or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

EXAMPLE Verification activities include

- reviews on outputs (documents from all phases of the safety lifecycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;

- design reviews;

- tests performed on the designed products to ensure that they perform according to their specification;

- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

[16, 3.8.1]

validation

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

NOTE 1 - Adapted from IS0 8402 by excluding the notes.

NOTE 2 - In this standard there are three validation phases:

- overall safety validation (see figure 2 of IEC 61508-1);

- E/E/PES validation (see figure 3 of IEC 61508-1);

- software validation (see figure 4 of IEC 61508-1).

NOTE 3 - Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system. Therefore, for example, software validation

means confirming by examination and provision of objective evidence that the software satisfies the software safety requirements specification.

[16, 3.8.2]

Acknowledgements

I offer my sincere appreciation to Mr. Tom Doyle, my longtime colleague and friend, and instructor at Conestoga College in Kitchener, Ontario, Canada. Risk assessment is rarely a solo endeavour, and Tom's collaboration, focused, helpful reviews of the manuscript, and constructive criticism made this paper much stronger.

I also acknowledge Dr. Yuvin Chinniah, Professor at École Polytechnic de Montréal for reviewing the manuscript and suggesting some useful papers related to "safe operating speeds" used with industrial robots. Dr. Chinniah is a colleague on the CSA Z432 Safety of Machinery Technical Committee, and is the Chair of the Canadian Mirror Committee to ISO TC199, Safety of Machinery.

I also acknowledge my colleague Mr. Réal Bourbonnière, ing., of Consultation Réal Bourbonnière, for reviewing and commenting on the manuscript, and for our interesting conversations on the applications of risk assessment and functional safety.

Together we are more than the sum of our parts!

References

[1] Industrial robots and robot systems. (ISO 10218-1:2011, MOD / ISO 10218-2:2011, MOD). CSA Z434. Canadian Standards Association (CSA). Toronto. 2014.

[2] American National Standard for Industrial Robots and Robot Systems — Safety Requirements. ANSI RIA R15.06. American National Standards Institute (ANSI). Washington, DC. 1999.

[3] Safety of Machinery: Principles for risk assessment. EN 1050. European Committee for Standardization (CEN). Brussels. 1997.

[4] Safety of Machinery: Part 1 - Basic Terminology, Methodology. EN 292-1. European Committee for Standardization (CEN). Brussels. 1991.

[5] Safety of Machinery: Part 2 - Technical Principles and Specifications. EN 292-2. European Committee for Standardization (CEN). Brussels. 1991.

[6] Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology and methodology. ISO 12100-1. International Organization for Standardization (ISO). Geneva. 2003.

[7] Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles. ISO 12100-2. International Organization for Standardization (ISO). Geneva. 2003.

[8] Safety of Machinery – Risk Assessment – Part 1: Principles. ISO 14121-1. International Organization for Standardization (ISO). Geneva. 2007.

[9] Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods. ISO/TR 14121-2. International Organization for Standardization (ISO). Geneva. 2007.

[10] Safety of machinery — General principles for design — Risk assessment and risk reduction. ISO 12100. International Organization for Standardization (ISO). Geneva. 2010.

[11] M. J. Allen, W. M. Yen. Introduction to Measurement Theory. Brooks/Cole Publishing Company. Monterey, California. 1979.

[12] Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design. ISO 13849-1. International Organization for Standardization (ISO). Geneva. 2006.

[13] Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems. IEC 62061. International Electrotechnical Commission (IEC). Geneva. 2005.

[14] Industrial Robots and Robot Systems - General Safety Requirements. CSA Z434. Canadian Standards Association (CSA). Toronto. 2003.

[15] Safety aspects — Guidelines for their inclusion in standards. ISO Guide 51. International Organization for Standardization (ISO). Geneva. 2014.

[16] Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations. IEC 61508-4. International Electrotechnical Commission (IEC). Geneva. 1998.

[17] A. Sugimoto, 'Limits of industrial robot teaching speeds through operation tests.', in A collection of papers contributed to conferences held by the Machinery Institute of Japan., Tokyo, 1984, pp. 844-845.

[18] Y. Beauchamp, T. Stobbe, K. Ghosh and D. Imbeau, 'Determination of a Safe Slow Robot Motion Speed Based on the Effect of Environmental Factors', Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 33, no. 419, 1991.

[19] W. Karwowski, T. Plank, M. Parsaei and M. Rahimi, 'Human Perception of the Maximum Safe Speed of Robot Motions', Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 31, no. 2, pp. 186-190, 1987.

[20] Y. Chinniah, F. Gauthier, S. Lambert and F. Moulet, 'Experimental Analysis of Tools Used for Estimating Risk Associated with Industrial Machines, Report R-684', Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), Montréal, 2011.