Safety Science 101 (2018) 248–259

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Validation of the impact of architectural flaws in six machine risk estimation tools

Yuvin Chinniah[a,*], François Gauthier[b], Barthélemy Aucourt[a], Damien Burlet-Vienney[c]

[a] Department of Mathematics and Industrial Engineering, Polytechnique Montréal, Montreal, Canada
[b] Department of Industrial Engineering, Université du Québec à Trois-Rivières (UQTR), Trois-Rivières, Canada
[c] Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), Montreal, Canada

ARTICLE INFO

Keywords:
Risk assessment
Risk estimation tool
Safety of machinery
Flaws in risk estimation tools

ABSTRACT

To address the hazards inherent in industrial machinery, machine designers and users must conduct risk assessments and use risk reduction measures. Machine risk estimation plays a crucial role in choosing and prioritizing risk reduction methods (e.g., level of performance required for the safety-related control system). A large number of machine risk estimation tools exist, and each tool has its own specific parameters and architecture. Flaws in a tool may bias risk estimation and lead to the adoption of inappropriate or insufficient risk reduction methods. An earlier study identified potential flaws in risk estimation tool parameters and architecture and proposed construction rules. In this paper, potential flaws in the architecture of six tools are tested by 25 machine safety experts. Four scenarios involving industrial machines and representing different risk levels were used for that purpose. The experimentation served to validate the potential flaws which were the impact of (i) a non-uniform distribution of risk levels, (ii) greater relative weight given to one parameter, (iii) discontinuity in risk levels and (iv) an overly sensitive risk matrix. Construction rules for machine risk estimation tools that should help improve inter- and intra-user repeatability, making the tools more reliable and robust, are proposed. The recommendations can potentially guide users of risk estimation tools when choosing, designing or using a tool. The results of this study will also help improve national and international standards in machinery risk assessment.

1. Introduction

1.1. Background

The use of industrial machinery commonly involves exposure to mechanical, electrical, thermal, chemical, noise-related, vibration-related and biological hazards, as well as hazards resulting from failure to respect basic ergonomic principles (ISO 12100, 2010; Bluff, 2014; ANSI B.11 TR3, 2000). The European Machine Directive and regulations in other countries require machinery designers to conduct risk assessment and reduction (Directive 2006/42/EC). The advantages of machinery risk assessment are numerous: hazards are identified effectively and better risk reduction measures can be implemented, injuries and deaths are prevented, fines and criminal prosecution are avoided, regulatory compliance is ensured and productivity is increased. In fact, used appropriately, a risk assessment ensures a successful health and safety management system and a safe working environment (Gadd et al., 2004). Investigation reports of serious or fatal accidents involving machinery often point to poor risk assessment or a complete lack of it (Chinniah, 2015; Backström and Döös, 2000; Lind, 2008). This kind of situation does nothing to address an absence or lack of risk reduction measures, or the use of inappropriate means of risk reduction.

Standard ISO 12100 (2010), on the principles of machine safety risk assessment and reduction, defines risk as a combination of two key parameters: the severity of the harm that could occur and the probability of occurrence of that harm. This probability consists of (i) the frequency and duration of exposure to the hazard, (ii) the probability of occurrence of the hazardous event and (iii) the possibility of avoiding or limiting the harm. A variety of risk estimation tools and methods based on these parameters have been developed over the years (e.g., Forteza et al., 2016; Burlet-Vienney et al., 2015). Each tool responds to a specific need or context and can be used to reduce risks (Etherton, 2007; Etherton et al., 2008).

Risk estimation tools have different architectures and recommendations have been issued regarding the design of such tools (Chinniah et al., 2011; Gauthier et al., 2012). For instance, a tool based

* Corresponding author.
E-mail addresses: yuvin.chinniah@polymtl.ca (Y. Chinniah), Francois.Gauthier@uqtr.ca (F. Gauthier), barthelemy.aucourt@polymtl.ca (B. Aucourt), Damien.BurletVienney@irsst.qc.ca (D. Burlet-Vienney).

http://dx.doi.org/10.1016/j.ssci.2017.09.015
Received 21 February 2017; Received in revised form 2 August 2017; Accepted 19 September 2017

Severity of harm / Probability of occurrence of harm	Catastrophic	Serious	Moderate	Minor
Very likely	High	High	High	Medium
Likely	High	High	Medium	Low
Unlikely	Medium	Medium	Low	Negligible
Remote	Low	Low	Negligible	Negligible

Fig. 1. Risk matrix from ANSI B11.TR3 (2000).

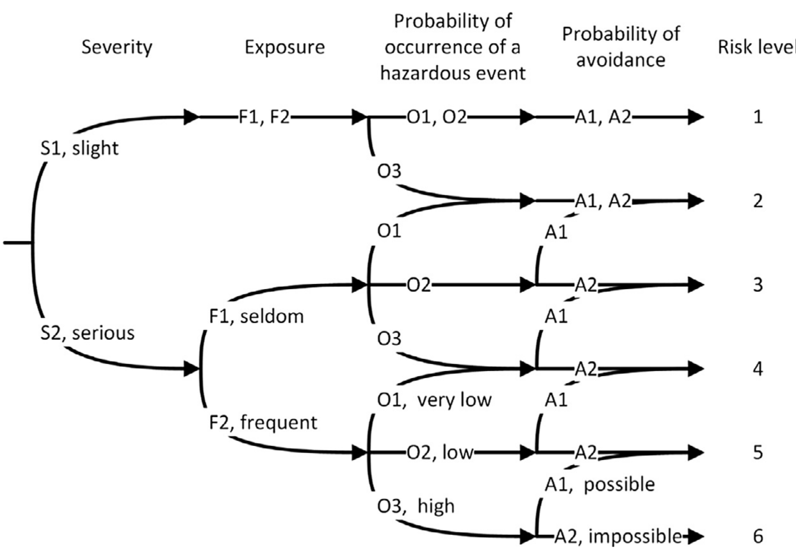

Fig. 2. Risk graph from ISO 14121.TR2 (2007).

on a logical model has been developed for managing accident risks related to the moving parts of machines (Aneziris et al., 2013). Tools often take the form of matrices or graphs and can be used to determine a risk level from risk estimation parameters (e.g., severity of harm, duration of exposure). Two tools derived from machine safety standards are presented in Fig. 1 (risk matrix) and Fig. 2 (risk graph) (ANSI B.11 TR3, 2000; ISO 14121.TR2, 2007). For the risk matrix, two parameters are used: the severity of the harm and the probability of occurrence of that harm. The two parameters have four levels each. The tool's architecture results in 16 possible combinations and four risk levels (high, medium, low, negligible).

The risk graph has four parameters, as defined in standard ISO 12100 (2010). The severity of the harm (SI and S2), exposure (F1 and F2) and the probability of avoiding harm (A1 and A2) each have two levels. The probability of the hazardous event occurring has three levels (O1, O2 and O3). The tool's architecture leads to six risk levels or indices, with 1 being the lowest and 6 the highest.

The risk graph presented in Fig. 2 is based on a decision tree where each node represents a risk parameter (severity, exposure, probability of occurrence of a hazardous event and possibility of avoidance) and where each branch from a node represents a class of the parameter (e.g., S1 or S2). The path on the risk graph is followed from the starting point. At each joint the path continues on the appropriate branch in accordance with the selected class. The final branch points at the risk level associated with the combination of classes that have been chosen. The end result is an estimation of risk qualified with a number 1 to 6. For instance, a combination of S1, F1 or F2, O1 or O2 and A1 or A2 gives 1. A combination of S2, F1, O3 and A1 gives 3.

The risk graph presented in Fig. 3 is different since it has three levels for severity of harm (S1, S2 and S3) as well as 14 levels for risk (1 to 14). For instance, a combination of S1, F1 or F2, O3 and A2 gives 6. A combination of S2, F2, O2 and A1 gives 7. A combination of S3, F2, O1 and A2 gives 10.

1.2. Literature review and research objective

Applying risk estimation tools to machine safety requires interpreting information that is often qualitative, generally using an ordinal scale, as described by Stevens (1946). The tools' ease of use and the speed at which they provide results contribute to their popularity (Hubbard and Evans, 2010). They offer a simple, effective approach, along with a clear framework for the systematic examination of hazardous situations (Ni et al., 2010). They are perceived as being easy to develop, explain and use (Thomas et al., 2014). Duijm (2015) notes that risk matrices are simple tools for classifying and prioritizing undesirable events.

As Ale et al. (2015) point out, however, a problem does arise with such matrices when a quantitative result is sought, but the input data are qualitative. Other shortcomings are related to the fact that the matrices do not help with identifying risks, nor with ensuring the certainty of results. Indeed, many risk estimation tools lack precision or detail (Chinniah et al., 2011). For instance, a qualitative verbal scale of the type *Highly unlikely*, *Unlikely* and *Likely* is used in some tools to determine the probability of occurrence of harm. As no further precision is provided, it is hard for the user to determine the exact scope of each term. This type of construction can create biases in the estimating process and significantly influence the final result (Duijm, 2015; Carey and Burgman, 2008; Christensen et al., 2003; Cox, 2008; Patt and Schrag, 2003). Problems inherent in qualitative ordinal scales are described in the literature (Franceschini et al., 2004; Hubbard and Evans, 2010; Smith et al., 2009; Woodruff, 2005; Duijm, 2015).

Thus, different risk estimation tools can arrive at different determinations of levels of risk for a given situation (Charpentier, 2003; Parry, 1999). Excessive dispersion in the risk estimation results may lead to inappropriate risk reduction measures being implemented, such as when determining the performance level required (PLr) of a safety-related control system (Hietikko et al., 2011). In standard ISO 13849 on the design of safety-related control systems, the PLr is estimated by a