Safety Science 80 (2015) 252–263

Contents lists available at ScienceDirect

Safety Science

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

Developing a safety indicator to measure the safety level during design for safety

Leyla Sadeghi [a,*], Luc Mathieu [b], Nicolas Tricot [c], Lama Al Bassit [c]

[a] Laboratory of Design, Manufacturing and Control-LCFC-Arts et Métiers ParisTech, Metz, France
[b] Automated Production Research Laboratory-LURPA-ENS de Cachan, Cachan, France
[c] National Research Institute of Science and Technology for Environment and Agriculture-Irstea, Antony, France

ARTICLE INFO

Article history:
Received 14 April 2015
Received in revised form 26 July 2015
Accepted 5 August 2015
Available online 24 August 2015

Keywords:
Design for safety
Safety indicator
Safety assessment
Safety level

ABSTRACT

The objective of this study was to measure human safety when using a system during its design process. Safety is defined as no danger or no conditions that can create a risk. Based on this definition of safety, we established a safety indicator used at the earliest design phases based. The proposed safety indicator depends on two values indicating the presence or absence of danger and the level of importance of hazardous conditions. The power take-off drive shaft is used as a case study to illustrate and examine the proposed safety indicator.

1. Introduction

The main responsibility for making a machine safe lies in its design process (Caputo et al., 2013). The term "design for safety" captures this attempt to integrate safety knowledge into the design process (Sadeghi et al., 2013). Safety concerns accident prevention in a "working situation." It has often been argued that ideally, accident prevention should be integrated into the system's design, as opposed to modifying and repairing the existing system and adding new barriers (Khan and Abbasi, 1998). This means that hazards should be eliminated and risk reduced during early product design phases. Furthermore, safeguards and safety guides should be used to mitigate any residual risk.

In this context, Ghemraoui et al. (2009a) attempted to define safety objectives early in the product design process by proposing the innovative risk assessment design (IRAD) method. This method offers the mechanism for generating nontechnical design objectives when preparing the requirements and constraints list. However, IRAD does not yet guide designers to define what a safe design is. This requires addressing the measurement of safety during the design process. If early warnings reveal and manage safety in advance, the undesired event can be prevented (Øien et al., 2011). Based on Pahl et al. (2007), the design process is broken down into three design phases: the conceptual phase, the embodiment phase, and the detail phase. Measuring safety from the conceptual design phase to the detail design phase helps select the best safety solutions. Determining the level of safety could therefore be considered as a decision criterion during the safe-design processes to help designers choose the best solution in terms of safety.

An indicator can be considered any measurement that seeks to produce information on an issue of interest (Reiman and Pietikäinen, 2012). Safety indicators could be used to monitor the level of safety in a system to provide the necessary information for decision-makers about where and how to act (Hale, 2009). Safety indicators have been addressed in a special issue of *Safety Science* (Volume 47, 2009) and in several recent research articles (e.g., Øien, 2001a,b; Duijm et al., 2008; Osmundsen et al., 2008; Saqib and Tahir Siddiqi, 2008; Hale, 2009; Hopkins, 2009; Vinnem, 2010; Øien et al., 2011). The purpose of this paper is to establish a safety indicator that can be used in the design process.

The remainder of this paper is organized as follows. Section 2 is divided into three parts: the first part covers an overview of different concepts related to indicators, the second part briefly explains the past development of safety and risk indicators, and the third part discusses the research presented. Section 3 defines the safety indicator to measure safety at the earliest design phases. Section 4 describes this safety indictor. In Section 5, the power take-off drive shaft is used to demonstrate the applicability of the approach proposed. Finally, Section 6 includes the results, a brief discussion, and a conclusion.

* Corresponding author.

http://dx.doi.org/10.1016/j.ssci.2015.08.006
0925-7535/

2. Research background

2.1. Overview of safety and risk indicator concepts

According to (MIL-STD-882D, 2000), safety is "freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment." Based on this definition, safety could be viewed as the absence of unwanted events. (Aven, 2009) has listed eleven definitions of risk which are found between 1976 and 2008. Then, he proposed to divide risk definition into three categories:

– Risk is expressed by means of probabilities and expected values.
– Risk is defined as an event or a consequence.
– Risk is expressed through events/consequences and uncertainties.

Based on risk definition, safety essentially means the absence of risk (Hollnagel, 2008). Hollnagel believes the best way to ensure a state of safety is either to prevent something unwanted from happening or to protect against its consequences (Hollnagel, 2008). He states that in order to ensure safety by preventing something from happening, i.e., through the elimination of risks, first of all risks must be known or made known. So, safety and risk are inextricably linked concepts, since the presence of an induced absence of the other.

His definition is based on Gray and Wiedemann (1999). According to Øien et al. (2011) this aspect could be, e.g., safety or risk. This indicator definition proposed (Øien et al., 2011) by is based on the combination of two definitions: "an indicator is a measurable/operational definition of a theoretical variable (Hellevik, 1999)" and "an indicator is a measure used to describe the condition of a broader phenomenon or aspect of reality (Gray and Wiedemann, 1999)".

Several terms are used for indicators, for example "safety performance indicators," "risk indicators," and "safety indicators." (Øien et al., 2011) defined a risk indicator as "a measurable/operational definition of a risk influencing factor." Based on (Vinnem, 2010), risk indicators must be observable and quantifiable, sensitive to change, transparent and easily understood, robust against manipulation, and valid. Based on (OECD, 2003) as mentioned in (Øien et al., 2011), "A safety performance indicator is a means for measuring the changes over time in the level of safety (related to chemical accident prevention, preparedness and response), as the result of actions taken."

The main purposes of safety indicators are to monitor the level of safety in a system, to motivate action, and to provide the necessary information for decision-makers about where and how to act (Hale, 2009). Hopkins (2009) discusses two dimensions of safety indicators: personal safety versus process safety, and leading versus lagging indicators. Personal safety involves avoiding cuts, trips, and falls on the part of employees; hence it does not include management of process hazards.

The objective herein is to include human safety during the design phase; therefore, we focus on the safety indicator. In this paper the term "safety indicator" is defined as a means for measuring the presence and the importance of hazardous conditions during design phases which reflect a level of human safety.

2.2. Indicator development

Øien et al. (2011) gave an overview of research on safety indicators. They believe the research on indicators started with the need to measure safety or risk. Based on Tarrants (1980), they explain that the term "indicator" in the safety field is rather new: although safety measures were undertaken in the 1980s and before, these attempts used terms such as "index," "rate," and "measurements.".

Hopkins (2009) discusses two dimensions of safety indicators: personal safety versus process safety, and leading versus lagging indicators. In response to Hopkins, safety indicators were addressed in a special issue of *Safety Science* (Volume 47, 2009).

Harms-Ringdahl (2009) believes that the usually formal aspects of safety management are measured, based on a top-down model coming from major hazard companies. Based on his article, (Harms-Ringdahl, 2009), indicators could address the following areas:

– "Nature and characteristics of the hazards.
– Technical safety features – which are in place and their performance.
– Formal safety organisation systems – which are in place and how they perform.
– Informal safety issues.
– Communication and co-operation issues as discussed by OECD (2003).
– Absolute values (evaluated or measured), or trends (the changes of performance over time).
– Economic consequences and probability for different outcomes."

Coulibaly et al. (2008) proposed an approach to provide indicators for maintainability and safety prediction in the early design phases. They expressed the safety indicator for a given design solution by the multiplication of two values: the risk factor that indicates the presence or absence of a risk and the risk index, which concerns its qualification and quantification.

2.3. Discussion

Although the recent discussions, referred to above, include some interesting viewpoints, there have been few attempts, if any, to structure one safety indicator to be applied in the design process. The safety indicator best suited to our needs is presented in Coulibaly et al. (2008). This indicator was developed to be applied during design. Hazardous conditions are also included. However, this indicator has the following drawbacks:

– It can only be applied in the embodiment design phase. However, safety needs to be measured from the conceptual design phase to the detail design phase.
– It is based on an expert's estimation of different numerical values entering its expression such as the severity and the probability of occurrence of the hazardous event. However, it is preferable not to consult an expert if possible to obtain the most objective indicator possible.
– While Coulibaly et al. (2008) indicate the probability of the hazardous event depends on the reliability of humans and the inherent reliability of the system, they do not relate their maintainability and safety indicators, neither indicators to calculate the reliability of humans. We consider that the probability of occurrence of a hazardous event is not a function of system reliability but is also related to its design quality.
– In Coulibaly et al. (2008), the presence of a safeguard is not specifically addressed. Here, we consider the safeguard as a system in itself and we attempt to assess the system's safety level with and without its safeguard.

We have therefore chosen to base this study on the safety indicator proposed by Coulibaly et al. (2008), which best adapts to meeting the criticisms above. Our safety indicator could be calculated from the conceptual design phase in the design for safety