Development of a methodology for systematic analysis of risk reduction by protective measures in tyre production machinery

M. Compare[1,2], E. Zio[1,2,3,4,*], E. Moroni[5], G. Portinari[6], T. Zanini[6]

[1]Dipartimento di Energia, Politecnico di Milano, Italy
[2]Aramis s.r.l., Italy
[3]Chair on System Science and the Energetic Challenge, Foundation Electricité de France, Ecole CentraleSupelec, France
[4]Department of Nuclear Engineering, College of Engineering, Kyung Hee University, Republic of Korea
[5]I.C.E.P.I. – Istituto Certificazione Europea Prodotti Industriali, Piacenza, Italy
[6]Pirelli Tyre S.p.a., Italy
[*]Corresponding author: enrico.zio@polimi.it

Abstract: ISO/TR 14121-2: 2012 considers three factors to describe the likelihood of the occurrence of an incident scenario: the frequency of exposure of persons to the hazard, the probability of occurrence of the hazardous event and the technical and human possibilities of avoiding harm. The assessment of these factors can be quite controversial, especially when it concerns the amount of risk removable by protective measures: their mapping onto the risk factors is not always clear and this can lead to non-conservative over-estimations of the risk reduction. We propose a methodological framework compliant with ISO 12100 to systemically carry out repeatable risk analyses in support to the design of industrial machinery in which protective measures can be introduced to reduce risk. The methodology first proposes a scheme for identifying the contribution of PMs to the reduction of risk in a machinery under design. Then, the methodology classifies the protective measures and builds a clear mapping between these classes and the risk factors they impact on. This helps decision makers to identify the protective measures guaranteeing that the residual risk is acceptable. The methodology is applied to a real case study concerning a curing machine for tyre vulcanization, where it has proven to be beneficial for the clarity of the analysis and its repeatability.

Key Words: Risk Assessment, ISO 12100: 2010, ISO/TR 14121-2: 2012, Risk reduction, Protective Measures.

Acronyms

HZ	Hazardous Zone, i.e., any space within and/or around machinery in which a person can be exposed to a hazard [21]
HS	Hazardous Situation, i.e., circumstance in which a person is exposed to at least one hazard. The exposure can immediately or over a period of time result in harm [21]
LD	Limiting Device, i.e., device preventing a machine or hazardous machine conditions from exceeding a designed limit [21]
MUP	Movable Upper Part, i.e., part of the machine that is opened for the green tyre loading and the cured tyre unloading; it is closed and locked during the curing process [15]
PM	Protective Measure, i.e., measure intended to achieve risk reduction, implemented by either the machine designer or user [21]
SPE	Sensitive Protective Equipment

Symbols

Cl	Scenario likelihood. According to ISO 12100, Cl=f(Pr,Fr,Av). According to ISO/TR 14121-2: 2012, Cl=Pr+Fr+Av.
Pr	Probability of occurrence of the hazardous event
Se	Scenario Severity
Fr	Frequency of exposure of persons to the hazard
Av	Technical and human possibilities of avoiding harm
$\boldsymbol{Op^i}$	i-th operation performed by operators, $i = 1, \dots, n$
$\boldsymbol{H^j}$	j-th hazard related to the machine operation, $j = 1, .., m$
$\boldsymbol{HS^{i,j}}$	Hazardous situation related to i-th operation and j-th hazard
$\boldsymbol{S_s^{i,j}}$	s-th scenario related to the i-th operation and j-th hazard, $s = 1, \dots, s_{i,j}$
$\boldsymbol{E_s^{i,j}}$	Hazardous event $E_s^{i,j}$ of $S_s^{i,j}$, $s = 1, \dots, s_{i,j}$
$\boldsymbol{Se_s^{i,j}}$, $\boldsymbol{Fr_s^{i,j}}$, $\boldsymbol{Pr_s^{i,j}}$, $\boldsymbol{Av_s^{i,j}}$	Risk factor scores for scenario $S_s^{i,j}$ before the protective measure introduction
$\overline{\boldsymbol{Se}}_s^{i,j}$, $\overline{\boldsymbol{Fr}}_s^{i,j}$, $\overline{\boldsymbol{Pr}}_s^{i,j}$, $\overline{\boldsymbol{Av}}_s^{i,j}$	Risk factor scores for scenario $S_s^{i,j}$ upon the protective measure introduction

1 Introduction

ISO 12100: 2010 [21] is the reference standard for carrying out risk analyses of machinery of different industrial fields. According to the engineering practice of many industries ([4], [5], [16],[29], [37]), ISO 12100: 2010 defines risk as the combination of two attributes (acronyms are taken from [21] and [27]):

a) *Severity* (Se), which is a rough quantification of the effect of the analyzed incident scenario. In the risk matrix in Appendix 1, which is derived from [27], this risk attribute is qualitatively expressed by integer numbers ranging from 1, for minor consequences, to 4, for severe consequences.
b) *Likelihood* (Cl), which is a coarse estimation of the aleatory uncertainty regarding the occurrence of the incident scenario. ISO 12100: 2010 states that Cl is a function (e.g., the sum, product, etc.) of the following three sub-attributes:
    1) The frequency of exposure of persons to the hazard (Fr); in the risk matrix in Appendix 1 there are 5 exposure classes, which are assigned numerical values ranging from 1, in case of rare exposures with exposure time shorter than 10 minutes, to 5, for very frequent exposures.
    2) The probability of occurrence of the hazardous event (Pr); this is expressed by an integer numerical value between 1, for negligible probability, and 5, in case of very high probabilities.
    3) The technical and human possibilities of avoiding harm (Av); this attribute can take three possible values: 1, probable, 3, possible, and 5, impossible.

Once the risk of a scenario is assessed, i.e., the severity of its consequences and the probability of its occurrence have been estimated, it is checked against a pre-fixed risk matrix (e.g., Appendix 1 [21], [27]) to establish whether it is acceptable or not. If not, some risk reduction measures are suggested by risk analysts and machine designers, and their effectiveness verified through a new iteration of the risk assessment process.

In spite of the wide use of ISO 12100: 2010 in industrial practice, risk analysts still encounter difficulties when the three-factor scheme is adopted for assessing the risk likelihood and the impact of risk reduction measures. In fact, although three parameters allow capturing the scenario characteristics better than when using a single factor [17], nonetheless their assessment becomes quite controversial in some cases, due to the inherent ambiguities of the analysis [28].

The main objective of this work is the development of a methodological framework in support to the reference standards, which provides a structured way for applying the three-factor scheme to the risk analysis of machinery.

In spite of the relevance of this issue for industry, to the authors' best knowledge it has been addressed in the light of ISO 12100: 2010 standard by a few works (e.g., [7]) in case of two risk factors, only.

Notice that risk reduction measures are referred to as safety barriers or controls in some industrial contexts (e.g., Oil&Gas [39], Nuclear Energy [1], Aerospace [35]) and as Protective Measures (PMs) by ISO 12100: 2010, which is the reference standard of this work.

The remainder of the paper is organized as follows. Section 2 sketches the research method followed. Section 3 analyses the reference standardization framework. Section 4 provides a reasoning scheme to give more consistency to risk factor estimation and, on this basis, a methodology to systematically perform risk analysis. Section 5 proposes a classification of PMs. Section 6 outlines some considerations to map PM classes onto the risk factors. Section 7 proposes some procedures to estimate the impact of the PM classes onto the risk factors. Section 8 develops the risk modelling framework. Section 9 applies the proposed methodological framework to a case study. Section 10 analyses the results. Section 11 concludes the work.

2 Research method

The research method used in this work can be summarized as follows:

a) Analysis of the standardization framework. This analysis allows better positioning our work in the reference standardization context.

b) Design of the methodological framework. This is the outcome of a continuous interaction with expert risk analysts through which the proposed theoretical reasoning schemes have been iteratively checked against their practical applicability to industrial settings. These interactions have been structured as formal brainstorming sessions (e.g., [24]), involving researchers as facilitators and engineers from Pirelli with a long experience in risk management as active participants. The outcomes of every brainstorming were synthetized by the researchers to form the basis for discussion for the next brainstorming session. The methodological framework is made up of the following steps:

   1. Development of a reasoning scheme to unambiguously frame how the PMs enter the risk analysis.
   2. Classification of the PMs. In industrial practice, there are a large number of possible devices and technical and organizational solutions that can be installed as PMs in different situations, scenarios, etc. However, to build the general risk modelling framework we are concerned with, it is fundamental to work with a limited number of possible alternatives. Thus, a preliminary grouping or classification of the PMs is required.
   3. Mapping of PM classes onto risk factors. Every type of PM can reduce the scores of a subset of the risk factors, only. Then, at this step we select for each PM the corresponding factors that could be influenced.

4. Quantification of the impacts of PMs on risk factors. General considerations are drawn to support the analysts in estimating the score reduction that every PM yields on the affected risk factors.
5. Development of a risk-modelling framework to identify and model the risk scenarios originated from the set of operations carried out on the system under analysis.

c) Case study. A team of 3 engineers from Pirelli with a sound experience in risk analysis were first trained by the Pirelli experts involved in step b) on the developed methodological framework and, then, asked to apply it to the risk analysis of a tyre curing machine.

3 Analysis of the standardization framework

The primary objective of ISO 12100: 2010 is to provide an overall framework for designing machines that are safe for their intended use. It is a type-A standard, which gives basic concepts, design principles and general aspects that can be applied to any machinery. Then, ISO 12100: 2010 is at the basis of type B standards, which focus on a single safety aspect or type of safeguard that can be used across a wide range of machinery, and type C standards, which provide detailed safety requirements for a particular machine or group of machines.

Examples of type B standards include, among many others, EN/ISO 13849-1/2 [23], which provides the guidelines for designing the parts of the control system linked to machine safety, IEC/EN 62061: 2005 [19], which refers to systems using only electrical and electronic technologies, EN 982: 1996+A1: 2008 [13] and EN 983: 1996 + A1: 2008 [14] which define the rules for designing safe hydraulic and pneumatic components, respectively.

The general principles of ISO 12100: 2010 have been tailored to the specific design issues of plastics and rubber machines and tyre curing machines in type C standard EN 16474: 2015 [15], which is the reference framework for the case study considered.

To help the analysts to evaluate the risk upon the introduction of PMs, ISO 12100: 2010 has also been corroborated by the Technical Report ISO/TR 14121-2: 2012 [27], which provides examples of PMs applicable to a wide variety of machinery.

The structures of the all three types standards are broad, solid and give practical guidance for conducting attentive risk assessments and risk reduction analysis of machinery, from both general ([21], [27]) and specific ([15]) perspectives.

Nonetheless, in spite of the wide and long use of these standards in industrial practice, a fundamental issue still arises when the three-factor scheme is adopted for assessing the risk likelihood: their assessment becomes quite controversial in some cases, due to the inherent ambiguities of the analysis [28]. For example, the distinction between the likelihood of the event initiating the scenario and the frequency of exposure to the hazard can be ambiguous when the accident scenario stems from a human error activating the hazard (e.g., [37]). In these cases, assigning the same values to both Fr and Pr factors could result in an over-estimation of the risk, whereas providing estimations for one parameter only may be counter-intuitive. The factors' score estimation issue is even more emphasized when risk analysts have to estimate the amount of risk removable by the PMs: their mapping onto the risk factors is not always clear and this can cause a non-conservative over-estimation of the risk reduction (e.g., [9], [10]).

The objective of this work is to build a methodological framework that provides risk analysts with a structured approach to apply the three-factor scheme to the risk analysis of machinery. This contribution is intended to corroborate the available standardization framework.

4 Problem framing

In this Section, we build on ISO/TR 14121-2: 2012 ([27]) to propose a reasoning scheme to unambiguously frame how the PMs enter the risk analysis carried out for a machinery under design. The scheme is summarized in Figure 1.

The machinery maintenance and operation is threatened by hazards of different types (left-bottom part of the tree) related to the system functioning and operability: hazards related to energy (i.e., mechanical, thermal, electrical, etc.), materials (toxic, carcinogenic, etc.), etc. These hazards can lead to an Hazardous Situation (HS) only if any operator is present in the Hazardous Zone (HZ, i.e., the space where the operators can inadvertently activate an existing hazard and/or can be affected from the hazard activation) [41]. When a hazardous event occurs, which is typically a failure event, a human error, etc., then the hazardous scenario is activated, right-bottom part of the tree in Figure 1. The situation originating from the occurrence of both hazardous event and HS does not necessarily entail a harm. Rather, it is at the beginning of a sequence of events that can have harmful consequences. The severity of the scenario effects and the associated occurrence probability are at the basis of the final decision about the risk acceptability, according to the given risk matrix (see Appendix 1).

If the risk is not acceptable, then a second iteration of the risk analysis is performed to estimate the risk in the setting where PMs candidate to be implemented for risk reduction have already been installed in the system: in this second iteration, risk analysts have now to consider the system as different from that analyzed before the PM introduction. In this respect, it is worthy emphasizing that according to ISO 12100: 2010 the analysts must refer to the design of the machine without any PM when performing the first estimation of the risk, and consider one hazardous event per time (bottom-right part in Figure 1).
Figure 1 helps us to identify the risk attribute that the PMs impact on:

- The PMs impacting on Pr are those avoiding the hazardous event, which is at the beginning of a sequence of events possibly leading to the operator injury, should an operator be in the HZ. Notice that according to [21] and [27], Pr factor relates directly to the hazardous event, rather than to its causes. Then, to estimate the Pr factor value, we may need to seek for the combinations of possible causes that can lead to the hazardous event. This is typically done by building Fault Trees (e.g., [47]).
- The PMs reducing Fr are those impacting on the probability of being in an HS. To do this, we can reduce either the frequency of operator presence or the dimension of the HZ. With respect to the former approach, for example we can design the working procedures so that the operator is required to enter the HZ less frequently. With respect to the latter, we can operate on both the hazards, e.g., by reducing the hazard energy and, thus, the area affected by its activation, and the HZ extent, e.g., by reducing the portion of HZ with respect to the operator movement area.
- PMs that increase the possibility of avoiding the harm are those intervening to give the operator more chances to counteract the evolution of the scenario leading to his/her harm once this has already been activated.

  The scheme proposed in Figure 1 emphasizes that the hazardous event does not necessarily coincide with the harm. Rather, it is a deviation from the nominal system functioning, which, however, may be not sufficient to have harmful consequences. Indeed, provided that an operator is in HZ, additional events may be required to occur to have his/her injuries, even if the hazard has been activated. In turn, the PMs acting on Av can come into play only if the considered hazardous event does not immediately and surely lead to harm.
- PMs impacting on Se are those reducing the severity of the potential harm.

In the following, we assume that in case the PM acts on Av, Fr and Se, then in compliance with the rule of considering a single failure per time, we depict the hazard scenario by assuming that the PMs surely work and modify the scenario accordingly. When the PM impacts on Pr, we evaluate the probability of the event combining both the original hazardous event and the failure of the PM. The apparent inconsistency of considering the PMs as failed when appraising the probability of the initiating event and as perfectly working when considering the consequent scenario is justified by the following considerations. If we considered the scenario in which the introduced PMs do not work, then they cannot yield any effect on the hazard scenario and, thus, the only possible impact of the PM would be on the reduction of factor Pr. However, if we considered the case where the protection measures are perfectly working, then in the new system the original hazardous event could no longer occur. This way, the concept that PMs can have different reliability values would be disregarded. For this, we propose to consider the hybrid situation described above.

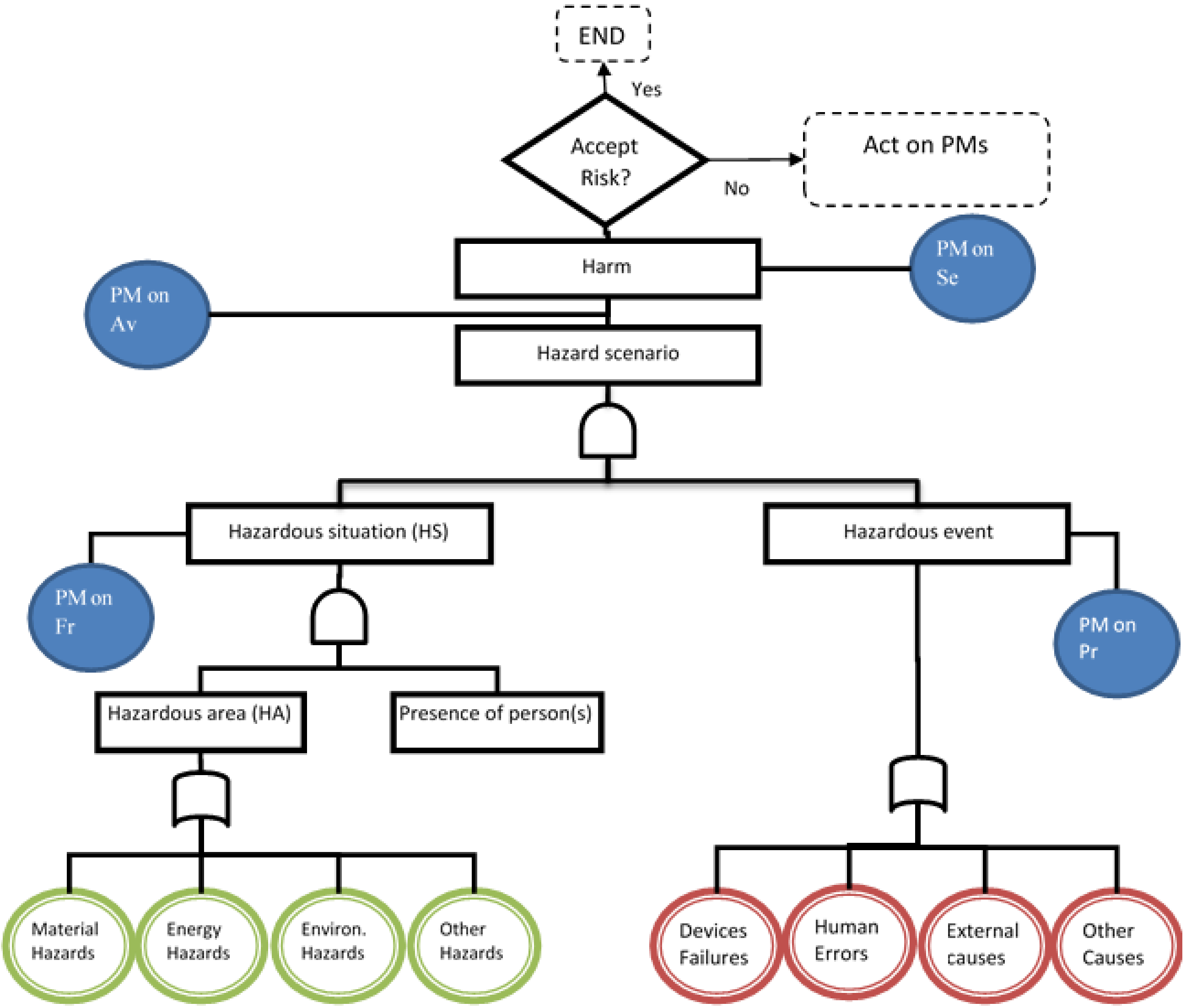


Figure 1: Synoptic of Hazard Analysis

5 Classes of PMs

Different ways have been proposed in the scientific literature to classify the PMs typically installed in industrial systems, which are reviewed in [44]. For example, in [18] an 11-classes classification is proposed, based on the consideration that any PM is characterized by three features: the main PM tasks, the cognitive effort to carry out these tasks and the type of support to the PM. According to IEC 61508, IEC 61511, ISO 13702 PM functions are classified as prevention, control and mitigation. The ARAMIS-project ([1], [43]) classifies PMs into four main categories, described by the action verbs 'to avoid', 'to prevent', 'to control' and 'to protect'. In [35] and [45], PM systems are divided into physical, technical, or human factors-organizational systems. Finally, a short review of the different perspectives for PM classification is given in [8], where another classification is proposed also.

We build on ISO/TR 14121-2: 2012 to propose a PM classification into the following five macro-categories (also in agreement to ISO 12100), which are further divided into the 18 classes listed in Table 1:

1) Hazard elimination by design. According to ISO/TR 14121-2: 2012, Section 8.2, this PM class contains all possible design methods for eliminating the hazards such as the substitution of hazardous materials and substances, usage of ergonomic systems, modification of physical features such as sharpness and shearing, to cite a few.
2) Risk reduction by design. ISO/TR 14121-2: 2012 and ISO 12100: 2010, Section 6.2, include in this class the design choices that make the machinery inherently more safe. In light of the reasoning scheme proposed in Section 4, we have grouped all the examples of PMs of this class in the ISO standards into the three following sub-classes:
    a. PMs reducing the level of the hazard (i.e., technologies and design precautions reducing the hazard energy, noise, radiation, toxicity, flammability, sharpness, etc.).
    b. PMs reducing the probability of hazard activation. These can be further divided into:
        i. PMs acting on the human factor (e.g., procedures for limiting the exposure to the hazard, aiding fault-finding, etc.).
        ii. PMs acting on the reliability of the equipment (e.g., provisions for stability, technologies and technical solutions to limit the degradation, redundancy, etc.).
3) Safeguarding. These PMs have been divided into six subclasses, differently from ISO/TR 14121-2: 2012 in the following points:
    a. Limiting Devices (LDs) have been further divided into Fixed and Activated, to highlight that the former do not need additional devices to guarantee the protection, whereas the latter need to be triggered by activating devices, which can have different reliability values.
    b. ISO/TR 14121-2: 2012 considers the following three sub-classes: SPE, Interlocking Guards and Devices of safety related functions. We have framed these PMs as Alarm Triggers to stress the fact that they yield a risk reduction only if they are coupled with the Activated LDs. This allows modeling the fact that, for example, the same switch for stopping the machinery can be activated by both a SPE and an Interlocking Guard.
4) Complementary. According to ISO/TR 14121-2: 2012, Section 8.4, these PMs have been divided into 5 classes (Table 1).

Information for use. According to ISO/TR 14121-2: 2012, the three sub-classes of this group of PM (Table 1) are taken from ISO 12100, Section 6.4.

Notice that building the procedure on ISO 12100: 2010 and ISO/TR 14121-2: 2012 entails inheriting all the safety principles behind them.

6 Mapping of safety device categories onto risk factors

The gray cells in Table 1 indicate the possible existing links between the identified PM classes and the four risk factors. This mapping differs from that proposed in ISO/TR 14121 [27]; the differences are explained through examples of concrete occupational PMs for machinery of the tyre industry, which is the object of the case study of Section 9, although the considerations outlined are general and applicable to other industries. In details, the PM classes are defined as follows.

Table 1: Mapping of safety device categories onto risk factors

Safety actions				Severity (Se) [injury]	Frequency (Fr) [exposure]	Probability (Pr) [occurence]	Possibility (Av) [avoidance]
Hazard Elimination by design	0		Elimination or Relocation of hazards	**Not Applicable**	**Not Applicable**	**Not Applicable**	**Not Applicable**
Risk reduction by design	1		Hazard level reduction	▨	▨	▨	▨
	2		Working procedures		▨	▨	▨
	3		Reliability Improvement			▨	
Safeguarding	4		Limiting devices (Fixed)	▨	▨	▨	▨
	5		Limiting devices (Activated)	▨	▨	▨	▨
	6		Fixed guards for prevention of access to HZ	▨	▨	▨	
	7	Alarm triggers	Interlocking Guards	▨	▨	▨	
	8		Sensitive protective equipment			▨	
	9		Devices of safety related functions			▨	
Complementary	10		Isolation and/or energy dissipation (isolation valve locking device, mechanical block, LOTO)	▨	▨	▨	▨
	11		Emergency stop			▨	▨
	12		Escape and rescue of trapped persons				▨
	13		Personal protective equipment	▨			▨
	14		Provisions for better handling of machines			▨	
Information for use	15		Pictograms			▨	
	16		Visual-Audible alarm			▨	
	17		Training on working and emergency procedures		▨	▨	▨

6.1 Elimination of hazards by design

When the hazard is eliminated or relocated, the analysis of the related risks becomes meaningless. Correspondingly, in Table 1 the estimation of the risk reduction values is indicated as not applicable to these PMs.

6.2 Risk reduction by design

These PMs are further divided into:

- Hazard Level Reduction. In [27], this PM is considered impacting mostly on Se: for example, small levels of energy generally entail light damages. Differently from [27], we consider possible effects also on the other three risk factors. In fact, according to the reasoning scheme proposed in Figure 1, a reduction of the available hazard level in principle can reduce the HZ and, thus, the Fr score. For example, reducing the pressure of a hot substance may reduce the area in which the operator could be injured by a leakage or blow up [17].

  Yet, the reduction of the hazard level can give the operator more time to escape from the HZ, thus reducing Av. For example, a reduction of the kinetic energy of a translating shuttle gives more time to recognize the HS and take counter-actions.

  Finally, the possible effect on Pr refers to the situations where the reduction of hazard level is beneficial for the probability of occurrence of the hazardous event. For example, reducing the temperature of a metal component subject to creep can improve its reliability.
- Working Procedures. This PM refers to the working procedure design phase, only, in which they are conceptualized. Indeed, to correctly estimate the effect of the working procedures on the hazard scenario, we need to take into account the actual capability of the operator in performing the designed working procedures, which depends on the PMs 'Training on working and emergency procedures': the final estimation of the real impact of the working procedures on the risk factors is that summarized by the Fault Tree in Figure 2, where an OR gate indicates that both working procedures and Training on Working and Emergency Procedures PMs have to properly function to ensure the achievement of the reduction scores.

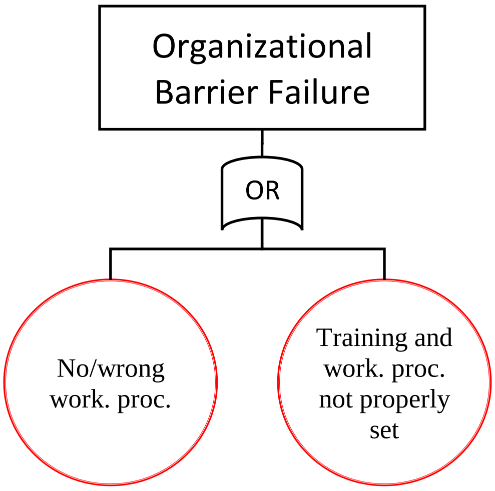

Organizational Barrier Failure
OR
No/wrong work. proc.
Training and work. proc. not properly set

Figure 2: Fault Tree representing the combination of 'Working Procedures' and 'Training on working and emergency procedures' PMs

  Working procedures can change the access frequency of the operator into the HZ and, thus, they allow reducing the Fr score. Moreover, the definition of a procedure compliant with applicable safety standards may contribute to reducing the probability of preventing operators from making errors. Then, these PMs can impact on Pr, as well. Finally, working procedures can also concern the emergency procedures, which can improve the operators' capability of avoiding the harm. For this, these PMs can act also on Av.
- Reliability Improvement. The installation of more reliable components prevents the occurrence of the failure event originating the hazard scenario, as it clearly emerges from the reasoning scheme in Figure 1. For this, the impact of these PMs is on Pr.

6.3 Safeguarding

These PMs are introduced when the risk cannot be reduced by design measures and are divided into:

- LD such as overloading and moment limiting devices, over-speed switches, temperature and pressure limiting switches, etc. These mainly apply to energy hazards and guarantee that they cannot exceed pre-fixed thresholds. Being the main function of these devices the reduction of hazard energy, they impact on the four parameters, analogously to the hazard level reduction PMs: according to the reasoning scheme proposed in Figure 1, a reduction of the available hazard energy can reduce both the extent of the harm (i.e., reduction of Se score) and the HZ (i.e., reduction of Fr score); it can give the operator more time to escape from the HZ (i.e., reduction of Av score). With respect to the probability of occurrence of the hazardous event (i.e., reduction of Pr score), LDs can work as PMs preventing the hazard activation, for example when triggered by a SPE.

  LDs are here divided into two further classes, depending on whether they are fixed or activated by other PMs:
    - Fixed LD (e.g., mechanical fuses, leak before break rings, etc.).
    - Activated LD (e.g., safety switches) which are commanded by signals sent by control devices.

The main difference between the two sub-classes is in their reliability models, as it emerges from Figure 3. Namely, upon the introduction of PMs impacting on Pr, the hazardous event can be framed as the top event of a Fault Tree connecting in AND logic the original initiating event and the failure of the selected PMs. Now, the failure of the Fixed LD is a basic event directly linked to the AND gate (Figure 3(a)), whereas in case of Activated LD the PM failure can be caused by two events (OR gate): either the Activated LD failure or the failure of the device triggering the alarm (Figure 3(b)). The triggering device can be not only a PM of classes 7-9 in Table 1, but also a transducer monitoring the hazard level, which is used by the machinery control system for the normal machinery operation (e.g., pressure transducers, temperature transducers, etc.). Then, in the reliability modelling of the PM, one has to consider the different reliability values of the activating devices.

Notice that according to [33], the score of an AND gate can be conservatively estimated as the minimum of the scores of its inputs, whereas for an OR gate, the score can be estimated as the maximum of the scores of its inputs.

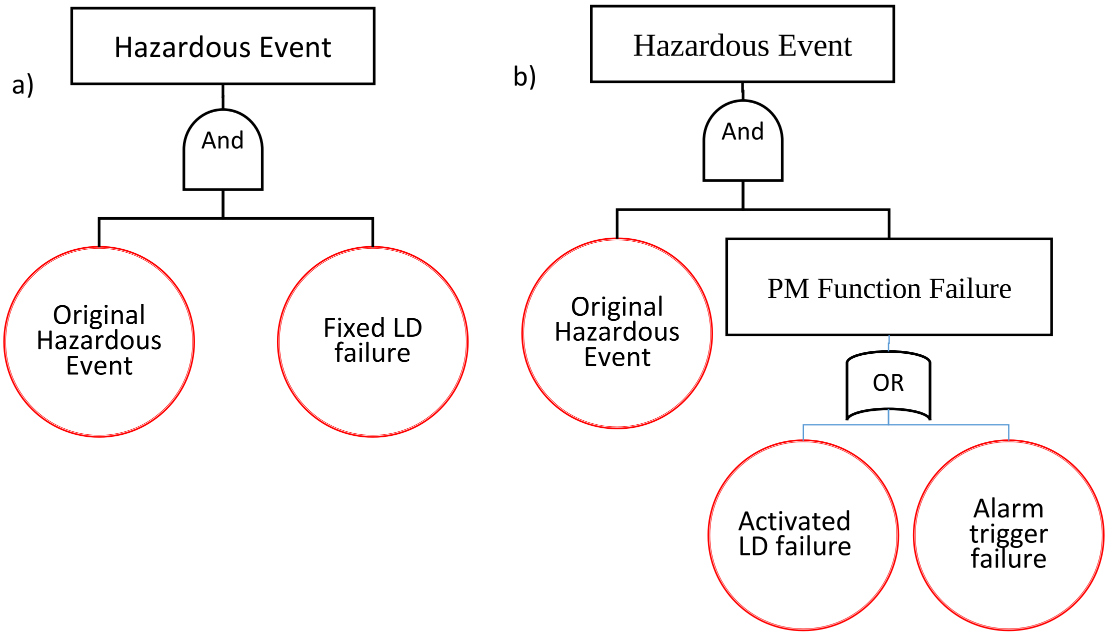


Figure 3: Fixed devices (a) and activated devices (b)

- 'Fixed guards for prevention of access to HZ' are guards affixed so that they can only be opened or removed by the use of tools such as by screws, nuts, welding, or by destruction of the affixing means. Their main function is, thus, twofold: i) to prevent the operator from reaching and activating the hazard: this reduces the probability of triggering the hazardous event and can also limit the extension of HZ; ii) to prevent the activated hazard from reaching the operator, thus reducing the severity of the consequences. For this, we consider that the fixed guards can impact on Pr, Fr, and Se, although in [27] these PMs are considered impacting mostly on Fr, with little effect, if any, on Se.
- Alarm triggers. In this PM class we include interlocking guards, Sensitive Protective Equipment (SPE) and control devices of safety-related functions. These are coupled with the Activated LDs of class 6.
    - Interlocking guards perform the following functions [21]:
        - The hazardous part of the machine "covered" by the guard cannot operate until the guard is closed. If a guard locking device is installed, then also the guard must be locked for the system to operate.
        - If the guard is opened while hazardous machine functions are operating, a stop command is triggered. In case of guard locking, this also means that the guard remains closed and locked until the risk due to the hazardous machine functions "covered" by the guard has disappeared.
        - When the guard is closed and possibly locked, the hazardous machine functions "covered" by the guard can operate. The closure and locking of the guard does not by itself start the hazardous machine functions. A start function is required to send this starting signal.

      Then, interlocking guard PMs on one side send the signal to reduce or eliminate the hazard and, thus, they impact on Pr, as the hazard requires the additional failure of these devices to be activated. On the other side, apart from this triggering function, interlocking guards are made up of mechanical PMs, which have the same function of the 'Fixed Guards', i.e., separating the machine operators from the HZ. Thus, these PMs can impact on Fr and Se, as well.
    - SPE is a PM for detecting persons or parts of persons going beyond a predetermined limit, which is also refereed to as tripping, and sensing the presence of a person in some specific positions; this information is sent to the control system, which can contain the hazard. Thus, SPE performs the same function of the interlocking guards, although with different technologies. In this respect, differently from interlocking guards, SPE does not physically isolate the space where the hazard is from that of the operator. For this, it has no impact on Fr and Se.
    - Devices of safety related functions, such as hold-to-run devices, limited movement control device, etc. These PMs are similar to SPE, the main difference being that here there is an active control of the operator in triggering the signal to de-energize the hazard. Accordingly, they impact on the same risk factors.

As mentioned before, in our framework the alarm trigger PMs must be coupled with Activated LDs; this is modelled by considering that the installation of the former entails that of the latter, the final effect being the combination of the two PMs arranged in OR gate (Figure 3).

6.4 Complementary PMs

These PMs are divided into:

- Isolation and/or energy dissipation PMs, such as isolation valves, locking devices, Lock-Out Tag-Out (LOTO), etc., which are typically used to allow maintenance operators performing their activities in safe conditions. They can be framed as LDs and, thus, they can impact on the four risk factors. In [27], these PMs are considered impacting mostly on Fr.

- Emergency stop PMs can operate upon the initiation of an accident scenario or other anomalous conditions. For this, according to [27] their main impact is on Av. Also in this case, the emergency stop PM is usually associated to a PM reducing the hazard energy, the difference being that the emergency stop is activated on condition, only. The probability of sending the signal is accounted for by Pr (see Figure 3).
- Escape and rescue of trapped persons PMs increase the possibility of avoiding harm. In [27], these PMs are also associated to a reduction in the exposure frequency, which is not consistent with the reasoning scheme proposed in Figure 1. Thus, the impact on Fr is here neglected.
- Personal protective equipment such as hands, feet and eyes protection, protective hearing devices, hard hats, etc., allow increasing the possibility of avoiding harm while reducing its severity, should its avoidance be not possible.
- Provisions for better handling of machines allow reducing the probability of having operator errors. For this, their impact is mainly on Pr.

Notice that all the complementary PMs are strictly dependent on the Training on Working and Emergency Procedures. To give account to this relationship, the same reasoning scheme for the working procedure PM applies: the two PMs must be arranged in an OR gate.

6.5 Information For Use

These PMs are communication links such as texts, words, signs, signals, symbols, diagrams, which are used separately or in combination to convey information to the user for the correct and safe use of the machinery and inform and warn him/her about the associated risks. There are three types of information for use PMs:

- Pictograms, which serve as alerts to operators. Given the reasoning scheme in Figure 1, the effect of these PMs is on Pr, only. In [27], these PMs are considered impacting on Av.
- Visual-Audible alarm, which alert the operators to the execution of a hazardous procedure. These PMs improve the capability of the operators of detecting HSs and, thus, they impact on Av.
- Training on Working and Emergency Procedures, which can be framed in combination with complementary PMs to see their impact on Av and Pr, as trained operators have more chances to avoid errors and recover from their effects. Moreover, training can avoid the operators to access an area in the presence of hazardous conditions. For this, Training on Working and Emergency Procedures can impact on Fr, as well.

Notice that the Information For Use PMs are all expected to bring a negligible effect in preventing human errors when the operators have to execute repetitive actions, whereas they may have a large impact on visitors or non-expert operators. In this respect, future research work will focus on the exploitation of the results of the Human Reliability Analysis engineering filed (e.g., [32]) to more attentively estimate the reduction score of these PMs, by accounting for their possible influencing factors such as comfort of the working conditions, duration of the working sessions, experience of the operators, etc.

7 Quantitative impacts of safety devices on risk factors

In the following sub-Sections, considerations are outlined in relation to the quantification of the reduction in risk factor scores yielded by PM installation. These are presented through examples of occupational PMs for machinery of the tyre industry, although their application is more general. The aim is not to give general, numerical methodologies, which is infeasible as shown by the many and diverse standards that had to be issued to tailor general principles to the specific industries and contexts of application.

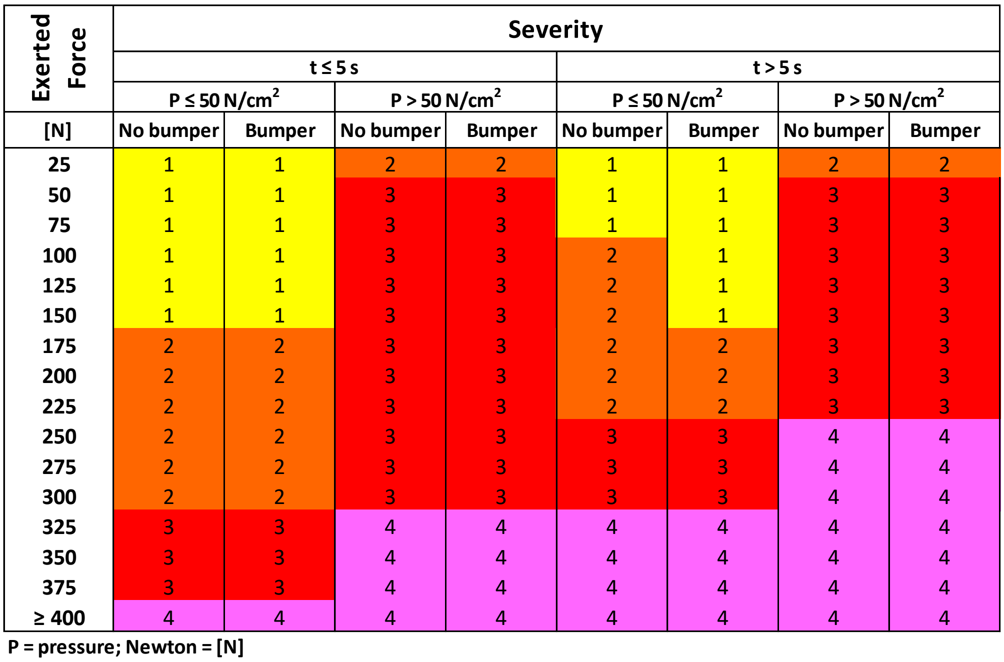
7.1 Factor Se

The Se score reduction heavily depends on the type of hazard originating the scenario. With respect to the PM classification in Table 1, the reduction in the Se score for energy hazards brought by de-energization (i.e., PMs 1, 4, 5 and 10) and physical isolation (i.e., PMs 6 and 7) can be estimated based on crude mappings of the removed energy into the severity of the harm, whereby we can assume that the final value of Se is always 1 if the PMs yield a complete de-energization or isolation of the hazard. For example, Figure 4 shows the findings of a preliminary phase of a study that Pirelli intends to carry out to link the severity of harm by crashing or shearing to the forces and pressures exerted by a moving mechanical element. This tentative mapping builds on UNI EN 953: 2009, and it is not applicable to estimate the harm severity of scenarios where kinetic energy is not negligible.

To wit, Figure 4 first column tells us that if a force exerted for less than 5 seconds is reduced from 400N to 225N, then in the setting in which no bumper is positioned on the leading edge of the part exerting the force corresponding to a pressure smaller than 50N/m^2, we can apply a reduction of 2 scores to the initial estimation of the Se factor (from Se=4 to Se =2).

For other hazards, different mappings can be used. For example, in [19] the effects of the electrical current on human beings have been thoroughly investigated and some threshold values for the electrical power supply features (i.e., voltage, current, etc.) have been derived to distinguish the safe operations from the hazardous ones.

With respect to the thermal hazards, many studies have been conducted to establish the effect of hot and cold temperatures on human body and psychology, both in the short term and in the long term (e.g., [3], [6], [25], [22], [26]). These can be at the basis of the development of Tables similar to that represented in Figure 4. This complex issue will be addressed in future research work.



Exerted Force	Severity							
	t ≤ 5 s				t > 5 s			
	P ≤ 50 N/cm^2		P > 50 N/cm^2		P ≤ 50 N/cm^2		P > 50 N/cm^2	
[N]	No bumper	Bumper	No bumper	Bumper	No bumper	Bumper	No bumper	Bumper
25	1	1	2	2	1	1	2	2
50	1	1	3	3	1	1	3	3
75	1	1	3	3	1	1	3	3
100	1	1	3	3	2	1	3	3
125	1	1	3	3	2	1	3	3
150	1	1	3	3	2	1	3	3
175	2	2	3	3	2	2	3	3
200	2	2	3	3	2	2	3	3
225	2	2	3	3	2	2	3	3
250	2	2	3	3	3	3	4	4
275	2	2	3	3	3	3	4	4
300	2	2	3	3	3	3	4	4
325	3	3	4	4	4	4	4	4
350	3	3	4	4	4	4	4	4
375	3	3	4	4	4	4	4	4
≥ 400	4	4	4	4	4	4	4	4

P = pressure; Newton = [N]

Figure 4: Mapping of pushing energy onto Se score

7.2 Factor Fr

Also for Fr, score reduction depends on the type of hazard considered. We give some examples for systemically approaching the estimation of reduction scores for Fr for energy hazards. According to the reasoning scheme proposed in Figure 1, the PMs that de-energize the hazard (i.e., 1, 4, 5 and 10) reduce the score of factor Fr depending on the extension of the energy reduction. That is, if de-energization is complete, then whichever the initial Fr score is, it has to be set to 1 upon the PM introduction, as the extension of HZ reduces to 0. On the other hand, in case the de-energization is not complete, the effect of the PM on Fr depends on the extent of the HZ reduction yielded by the limitation of the hazard energy. The relation between hazard energy and HZ depends on the particular energy hazard analyzed, and it must be derived case by case, for example by applying qualitative preference programming approaches (e.g., [30], [46], [42]). These methodologies can be used to establish a relationship between the reduction in the Fr score and that of HZ. This allows estimating the score to be subtracted from the initial appraisal of Fr with more repeatability and objectiveness.

Figures 5 and 6 show two examples of how the reduction of the hazard energy could be linked to that in the Fr score. These Figures are made up of two parts: in the bottom part, a link is established between the energy reduction, vertical axis, and the percentage of reduced HZ, horizontal axis. For example, Figure 5, bottom, shows the situation where HZ does not reduce with hazard de-energization, till the energy reduces to zero. This may be the situation concerning the kinetic energy of a translating shuttle: the extension of HZ is not impacted from a reduction in the shuttle speed, unless this reduces to zero. Figure 6 shows a situation in which the hazard de-energization entails a reduction of HZ, which is mapped into the reduction of the Fr score.

In the upper part of both Figure 5 and Figure 6, the reduction of HZ related to the percentage of energy reduction is linked to the reduction in the Fr score. Namely, the condition of no shrinkage of HZ is assigned score 0 (i.e., no reduction of Fr score), whereas its complete reduction is assigned score 4 (i.e., maximum reduction of Fr): every other percentage value of HZ reduction is scored according to these two reference points, possibly through set-valued scores, to give the risk analysts more flexibility. For example, score {0, 1} is assigned to a reduction of HZ of 20%, given that its effect is much closer to null reduction than complete reduction.

Notice that the values in Figure 5 and Figure 6 are for illustration, only. For every case study, a dedicated analysis should be performed to tune the values in Figure 5 and Figure 6.

With respect to the interlocking guards, these do not completely isolate the space in which the hazard is located. For this, the effect of these PMs needs to be carefully evaluated case by case, and it cannot be larger than a reduction of 2 Fr scores.

Fixed guards reduce the HZ and, thus, they can reduce or even eliminate the frequency of access. The extent of the reduction depends on the specific case study. Based on this estimation, one can exploit the upper parts of Figures 5 and 6 to link the reduction of HZ to that in the Fr score.

Finally, working procedures determine the theoretically exposition of the operator to the hazard; their impact on the exposure frequency and, thus, on factor Fr strongly depends on the analyzed situation. To guide the analysts in finding the correct value, we refer to the scale considered in ‘Exposure Frequency’ column of the risk matrix in Appendix 1.

To wit, a change in the working procedures that reduces the frequency of exposure from 1/h to 1/year reduces the Fr score from 5 to 2.

However, working procedures are always accompanied with Training and Emergency Procedures measures, ‘Training on Working and Emergency Procedures’ PMs being the weakest of the two in the logic structure of Figure 2. For this, the final effect of working procedures on Fr cannot be larger than a reduction of 1-2 points.

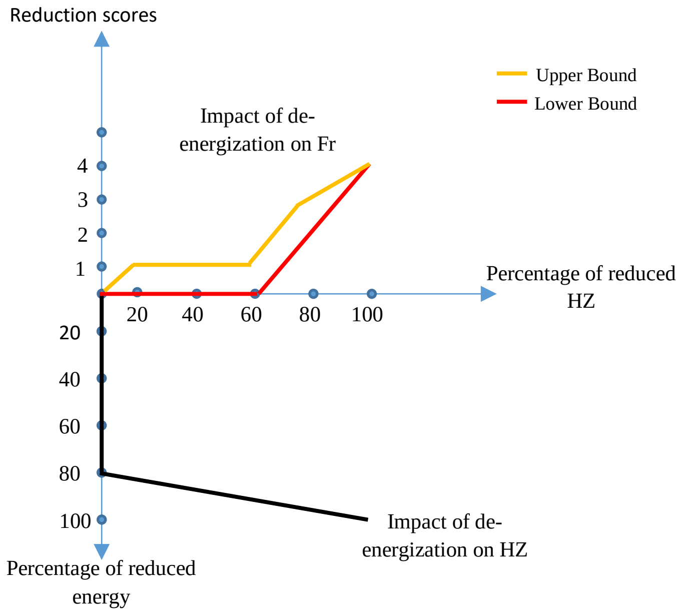


Figure 5: Fr score reduction vs reduction of HZ: situation in which HZ reduces only if the energy hazard is completely removed.

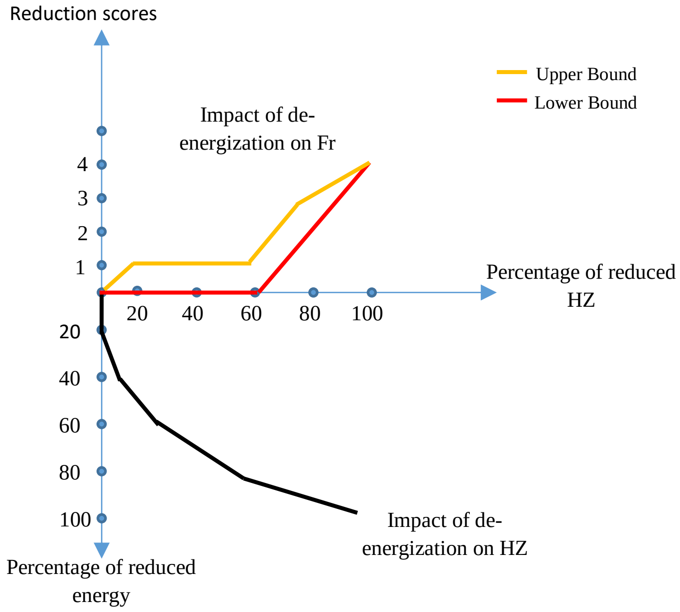


Figure 6: Fr score reduction vs reduction of HZ

7.3 Factor Pr

In this Section, we outline some suggestions to help the risk analysts to provide objective and repeatable estimations of the reliability of the PMs, which determine the probability score.

When PMs relying on electro-mechanical sensors are introduced in the system, we can use the Performance Level (PL) index ([23]), which relates to the probability that the PM performs the required safety function. This is the case of activated LD coupled with PMs 7, 8, 9, 11 in Table 1. The PL level of a safety device, which is certified based on attentive reliability and risk analyses, ranges from level 'a', worst in class, to level 'e', best in class. Then, we can assign Pr {0, 1} to devices of classes PL a and b, and linearly decreasing scores to the other PL levels up to PL ‘e’, which yields a 4-score reduction in Pr.

In compliance with [27], the risk matrix in Appendix also defines for every outcome of the preliminary evaluation of risk, the minimum PL requirement for the barrier to be installed in the system to reduce the Pr score.

The Pr score reduction of the other PMs has to be analysed case by case. However, to give the analysis more objectiveness and repeatability, we can rely on techniques used in decision science to elicit value or utility functions from decision makers (e.g., [46]). For example, the reduction score can be assigned by trading off the reliability of the candidate PM against those of the PLa and PLe PMs. To wit, consider the question:

> “Is the reliability difference between the candidate PM and a PM classified as PLa more or less significant than that between the candidate PM and a PLe PM?”

Answering this question allows identifying the range of possible Pr reduction scores: in the set {0, 1} if the answer is ‘less’, in {3, 4} if the answer is ‘more’ and in {1, 2} otherwise.

Yet, a limited Pr score reduction capability can be assigned to the Pictograms and Training PMs; in these cases, Pr score reduces by 1, at most, only in case of not repetitive operations.

A final comment seems in order about the lack of numerical threshold values defining the probability classes (e.g., Pr=1 if the probability of occurrence of the considered hazardous event is smaller than 10^{-5}), as for example in the case of factor Fr. On the one hand, the definition of these thresholds would simplify the estimation of the Pr reduction extent, which only requires to compare the probability of the hazardous event with the threshold values. On the other hand, the estimation of the probability values is not as simple as for the frequency factor, as it may require developing more or less complex models that rely on parameters that are difficult to know such as those of the failure distribution functions or the probabilities of human errors.

7.4 Factor Av

According to ISO 12100: 2012, the operator capability of avoiding injuries depends on different factors such as the level of preparation of the persons exposed to the hazard (e.g., skilled, unskilled), how quickly the hazardous situation can lead to harm (suddenly, quickly, slowly), the means of risk awareness (e.g., by general information, in particular, information for use, by direct observation, through warning signs and indicating devices, in particular, on the machinery), human ability to avoid or limit harm (e.g., reflex, agility, possibility of escape), practical experience and knowledge (e.g., of the machinery, of similar machinery, etc.).

These factors can be framed as contributions to the total time T_{Av} available to counteract the scenario originated from the hazard activation. We propose to coarsely estimate T_{Av} as the sum of two contributions: the mean time available for recognizing the HS, $T_{detection}$, and the mean time available to avoid injury, $T_{counteract}$.

From this perspective, the PMs can impact Av in three ways:

1. Improve the operator capability in recognizing the HS: training on working and emergency procedures, and visual-audible alarms favour this ability.
2. Increase the time available to counteract the evolution of the accident scenario: for some energy hazard types, the PMs de-energizing the hazard can operate in this way; for example,

the reduction of the speed of a moving part gives more time to recognize its movement and leave the hazardous zone.

3. Increase the operator quickness to counteract the activated hazard: training on emergency procedures can yield this effect, together with complementary PMs.

These three PM effects are lumped together in the following formula:

$$T'_{Av} = q(T_{detection} + \beta T_{counteraction}) \tag{1}$$

where T'_{Av} is the total equivalent time to avoid the injury upon the implementation of the PMs, q encompasses the improvement in the operator quickness in doing the emergency actions, β quantifies the gain in the time to make counter-actions. The formula in Eq. (1) is justified as follows. The quickness gain q maps the calendar time onto an equivalent time scale. For example, doubling the speed for doing the same counter-actions brings the same effect of doubling time T_{Av} available to avoid harm before PM installation. The quickness effect also encodes the improvement in the operator's capability of detecting the HS: the better this capability, the more prompt the detection.

To the authors' best knowledge, systemic studies for the quantitative modelling of factor Av are lacking. In this respect, the approach proposed in this Section is an attempt to provide risk analysts with a structured basis to estimate the Av reduction score.

The increment of the time available to answer to the risky situation is taken into account separately, by coefficient β. For example, a reduction in an hazard energy that doubles the time to leave HZ leads to doubling the time available to counteract the scenario. This has the same effect of doubling the time $T_{counteraction}$ the operator has to perform the actions to avoid the failure, and can be further amplified by the increase in the quickness q.

To assign a score to Av, times $T_{Av} = T_{detection} + T_{counteraction}$ and T'_{Av} must be evaluated against the time required for a safe managing of the activated hazard. For example, Figure 7 shows the situation in which if the time available to avoid injury is larger than 5 seconds, then the operator will safely implement counter-actions. The safe zone is thus defined as the combinations of $T_{detection}$ and $T_{counteraction}$ such that $T_{detection} + T_{counteraction} > 5$. A time interval between 3 and 5 seconds allows partially avoiding operator injuries (Middle Area in Figure 7). Finally, it is improbable to avoid harm if T_{Av}< 3 seconds.

Figure 7 also shows the possible effects of PM introduction: the initial situation in which T_{Av}=1.5+1=2.5s and Av=5 is modified by q =2, $\beta = 2$ into T'_{Av}=7s, which corresponds to Av=1. Notice that the values in Figure 7 are illustrative.

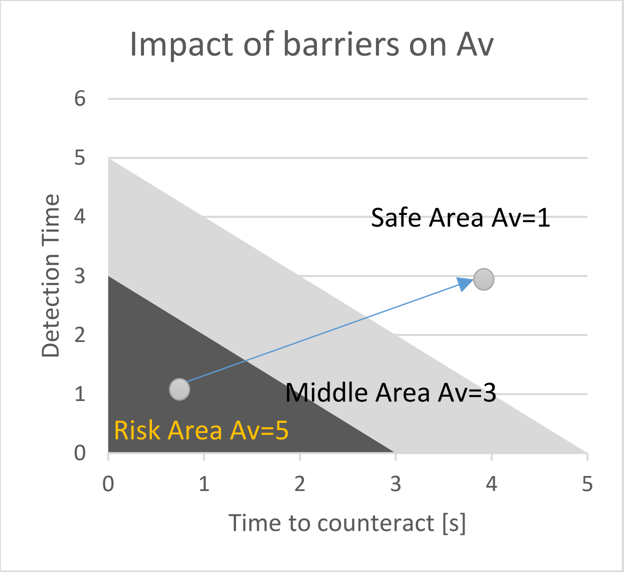


Figure 7: Time to leave HZ vs Av reduction score

8 Development of a risk-modelling framework

The goal of this step is to develop a procedure to model the risk scenarios originated from the set of operations carried out on the system under analysis. First, every hazard $H^j, j = 1, \dots, m$ needs to be identified. To do this, we start from the checklists available in the literature ([11], [24]).

Every hazard is then mapped into the operator activities (Op^i), $i = 1, \dots, n$. The risk analyst, then, has to check whether an HS $(HS^{i,j})$ could originate from the combination of Op^i and H^j. For every feasible HS, the possible pairs $(E_s^{i,j}, S_s^{i,j})$ of hazardous event $E_s^{i,j}$ and corresponding scenario $S_s^{i,j}$, $s = 1, \dots, s_{i,j}$ need to be considered (Figure 8).

	H^1	H^2	…	H^m
Op^1	$HS^{1,1} \rightarrow$ $\{(E_1^{1,1}, S_1^{1,1}), \dots, (E_{s_{11}}^{1,1}, S_{s_{11}}^{1,1})\}$			
Op^2		$HS^{2,2}$ $\rightarrow \{(E_1^{2,2}, S_1^{2,2}), \dots, (E_{s_{2,2}}^{2,2}, S_{s_{2,2}}^{2,2})\}$		
…				
Op^n	$HS^{n,1}$ $\rightarrow \{(E_1^{n,1}, S_1^{n,1}), \dots, (E_{s_{n,1}}^{n,1}, S_{s_{n,1}}^{n,1})$			$HS^{n,m}$ $\rightarrow \{(E_1^{n,m}, S_1^{n,m}), \dots, (E_{s_{n,m}}^{n,m}, S_{s_{n,m}}^{n,m})$

Figure 8: Mapping between operator activities and hazardous events

Every pair $(E_s^{i,j}, S_s^{i,j})$ is assigned the initial score values $Se_s^{i,j}$, $Fr_s^{i,j}$, $Pr_s^{i,j}$, $Av_s^{i,j}$, according to the reasoning scheme of Figure 1, considering the design of the machine without any PM.

Finally, a mapping between every pair $(E_s^{i,j}, S_s^{i,j})$ and the type of PMs applicable should be sketched, and the corresponding risk factors values $\overline{Se}_s^{i,j}$, $\overline{Fr}_s^{i,j}$, $\overline{Pr}_s^{i,j}$, $\overline{Av}_s^{i,j}$ estimated after the PM implementation. The considerations drawn in Section 7 can provide the analysts with a structured approach to carry out this part of the risk analysis. On this basis, the decision maker can finally select the minimal set of PMs to make the risk acceptable.

9 Case study

We consider a case study concerning a tyre curing machine. Expert risk analysts from Pirelli Tyre have analysed two risk scenarios with the methodology presented above and recognized its valuable contribution to performing solid and structured risk analyses, with improved repeatability.

Tyre curing machines are used for vulcanisation of tyres and are made up of fixed and movable parts that can be locked together, inside which a curing process ensures that the green tyre assumes its final shape, characteristics and performances [15]. The curing process consists in performing controlled temperature cycles, while an inflatable rubber, named bladder, pushes the green tyre against the mould at controlled pressure level in an environment with specific mixtures of curing fluids. We assume that every curing cycle lasts almost 20 minutes.

The machine is made up of two independent cavities, which allow curing two green tyres per time. Every cavity has dedicated movable parts, which load the green tyre on its seat and un-load the cured tyre at the end of the vulcanization process.

A detailed description of a tyre curing machine can be found in [15], in which the hazards related to the operation of tyre curing machines are analysed and PMs are proposed.

Building on [15], for illustration we consider $m = 2$ hazards and only $n = 1$ operation. Namely, Op^1 is the loading of the green tyre, before it is automatically loaded from the stand onto the mould. Op^1 is performed almost every ten minutes and requires the operator to walk on Area 1 (Figure 9) to approach the green tyre stand and, then, exit from this area.

The two hazards taken form [15] are:

- H^1= Kinetic Energy and Difference of Potential Energy of the movable upper part of the machine.
- H^2= Pressure Energy in the bladder when the tyre curing machine is above the semi-closed position.

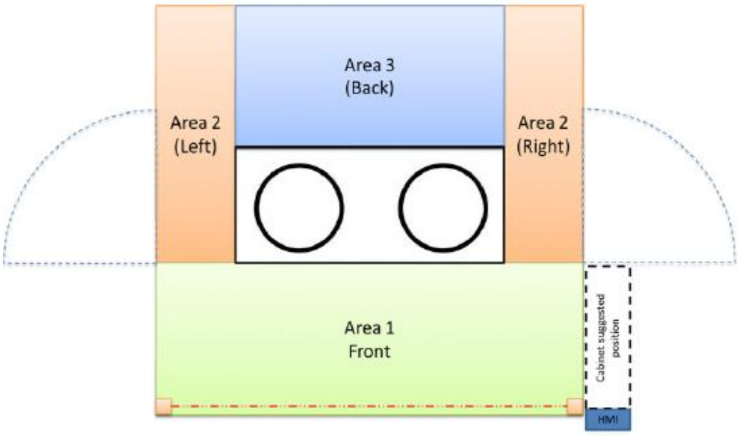
There are many other operations during which the operators are exposed to the considered two hazards, such as the process supervision activities, the activities performed by the quality technicians to analyse the steps of the curing process, the tuning activities carried out at the initial set-up of the curing machine, the ordinary maintenance activities, etc. For brevity, the large number of hazards and activities related to the operation of the tyre vulcanization machine are not listed in this work and their analysis is not reported.

Notice that according to ISO/TR 14121-2: 2012, we consider the summation operator to lump together the three Cl sub-attributes ([9]). This way, Cl varies from 3 to 15.

9.1 Energy of the movable upper part of the machine

The movable upper part (MUP) closes the mould and assures its tightening by exerting a force of almost 250 tons: this prevents the mould opening when the bladder internal pressure reaches almost 30 bars to stamp the tyre. The MUP closing phase lasts almost 30 seconds.

The operator enters Area 1 (Figure 9) to approach the green tyre stand to accomplish Op^1. The HZ is the portion of Area 1 including the space along the ride of the MUP, where human bodies would be crushed, and its surrounding zone, from which the open MUP is reachable by an inattentive operator. In Figure 9, HZ is indicated by the uncoloured central zone. However, entering the HZ does not necessarily lead to an HS. Rather, the HS we are concerned with, $HS^{1,1}$, occurs when Op^1 is carried out simultaneously to the closing of the MUP. To assign a frequency to $HS^{1,1}$, we can perform some naïve calculations, with the final aim of identification of a class factor in the 1 to 5 scale of possible values. Namely, we consider that the operator accesses HZ twice in every cycle, for almost 5 seconds each. If we assume that these accesses are uniformly distributed over the 20-minute (i.e., 1200 seconds) cycle duration, the probability of entering HZ while the MUP is not closing can be roughly estimated as the portion of the cycle duration in which the MUP is not moving: (1200s-30s)/1200s= 0.975. Now, consider that there are two cavities and, then, there are two operator accesses in every cycle. Then, the estimated probability value, i.e., 0.975, must be squared to estimate the probability of avoiding overlaps between Op^1 and MUP in every cycle. This means that the probability of having an operator access simultaneous to the MUP closing within a 20 minute cycle is 1-((1200s-30s)/1200s)^2=1-0.975^2≅ 0.05. Finally, to calculate the frequency of $HS^{1,1}$, we can consider that there are three cycles per hour. Thus, the probability of Op^1 overlapping the MUP closing phase within a 1 hour machine operation interval is the complement to one of the probability of avoiding the overlap in three cycles. If we assume that the overlap events are independent on each other, it turns out that the final probability of Op^1 overlapping the MUP closing phase is 1-(1-0.05)^3=0.15 in 1 hour. That is, the frequency of $HS^{1,1}$ is once every seven hours. According to the risk matrix in Appendix, we set $Fr_1^{1,1}$=5. However, the report [27], from which the risk matrix is derived, assumes that if the exposure to the hazard lasts less than 10 minutes then the we can use the next lower frequency level. Thus, the final score is $Fr_1^{1,1}$=4.



- GT is loaded from area 1;
- Cured tire is discharged in automatic from area 3;
- Access from area 2 are for maintenance purpose only;

Figure 9: layout of the curing machine

The hazardous event $E_1^{1,1}$activating the hazard scenario $S_1^{1,1}$ is the lack of attention of the operator, which leads him/her to stumble or to make an improper movement and, then, to put some body part under the MUP. This is conservatively estimated to be a rare event and, according to Table 4 in Appendix 1, $Pr_1^{1,1}$=2. There are many other events $E_s^{1,1}, s > 1$, associated with $HS^{1,1}$ such as the inadvertent activation of the MUP. For brevity, these events are not analysed.

We assume that the operator immediately recognizes the HS (i.e., $T_{detection} = 0$) and that he/she will certainly not succeed in removing the limb from the MUP movement area to avoid harm if the time available for counteractions is $T_{Av} = T_{counteraction} < 9s$, whereas it is almost certain that he/she will avoid harm if the time for counteraction implementation is longer than 15s (i.e., half of the MUP closing time). Experts of the tyre industry conservatively assume that the time required to escape from the MUP is 10s; then, $Av_1^{1,1} = 3$ (see Table 4 in Appendix 1).

In conclusion, the likelihood of the scenario is $Cl_1^{1,1} = Fr_1^{1,1} + Pr_1^{1,1} + Av_1^{1,1}$=4+2+3=9. The consequences of the crunching can lead to the operator death or to serious injury (Figure 4). Then, $Se_1^{1,1}$=4. Thus, checking these factor values against the risk matrix in Appendix 1, we can see that the risk is not acceptable, and additional PMs are required to be installed to reduce the risk.

To do this, we perform a mapping between $(E_1^{1,1}, S_1^{1,1})$ and the 18 classes of PMs, to select those applicable to $S_1^{1,1}$ and quantify the reduction in the risk scores brought by the single PM.

Notice that the estimations of both Cl and Se are equal to those given in [15] for the same risk scenario: although the proposed methodology does not change the outcomes of the analysis, it always brings an added value, which lies in that the structured reasoning followed to analyse the scenario makes the risk analysts more aware and confident on the final results.

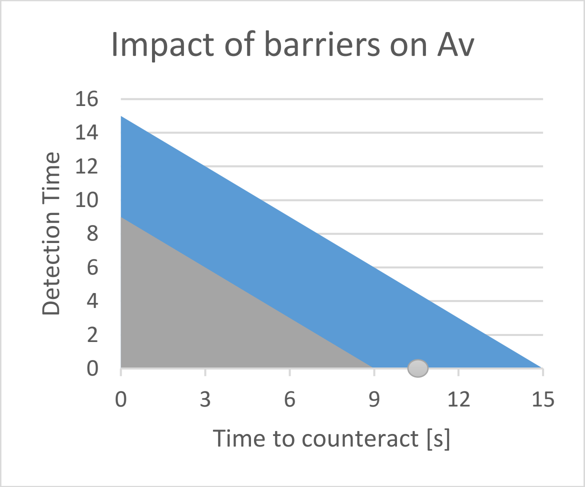


Figure 10: Av factor score for $(\boldsymbol{E_1^{1,1}}, \boldsymbol{S_1^{1,1}})$

9.1.1 Risk reduction by design

The kinetic energy and the difference of potential energy hazards are necessary for the tyre curing process; then, hazard energy reduction PMs are not applicable to the analysed scenario.

The impact of Working Procedures on risk is discussed in Section 9.1.4, together with the training PM.

Finally, with respect to the Reliability Improvement PM, this is considered not applicable to the considered scenario, as it is originated by a human error, whose probability cannot be reduced by designing a tyre vulcanization machine with more reliable components.

9.1.2 Safeguarding

Fixed guards cannot be installed on the front area of the curing machine: given the relatively large frequency of operator entrance-exit actions in Area 1 for green tyre loading, fixed guards would strongly affect the machine operability.

Fixed LDs are not applicable to the scenario under analysis, as they would not allow the MUP movement.

Activated LDs stop the moving upper part and, thus, de-energize the hazard. However, this de-energization is not complete, as only the kinetic energy is removed, whereas the difference of potential energy still remains active and can cause injury, should the upper part inadvertently fall. Although Figure 4 is not applicable to estimate the harm severity of the impacts, nonetheless the weight of the MUP, which is larger than 5.5 Tons, is such that even if we neglect the kinetic energy of the falling upper part, the load conditions always lead to a severe injury or death. Then, the application of the PM does not yield a reduction in the severity score, whereby $\overline{Se}_1^{1,1} = 4$.

To estimate the reduction in $Fr_1^{1,1}$ due to the activated LDs, we can rely on Figure 5: the score does not change, as HZ is not reduced once the MUP is stopped in an elevated position. Then, $\overline{Fr}_1^{1,1} = 4$.

With respect to the avoidance factor, assuming that the activation time for the activated LD is negligible, its effect is on factor q, which increases to infinite the time available to safely remove the limb from the MUP moving space. Accordingly, $\overline{Av}_1^{1,1}$= 1.

With respect to the probability of occurrence of the hazardous event, its reduction depends on both the intrinsic failure probability of the Activated LDs and the failure probability of the alarm triggers, which are arranged in OR configuration (Figure 3). With respect to alarm triggers, it is worth noticing that the installation of interlocking guards is not recommended when the frequency of the operations requiring the interlocking guard opening is high, as in the present case. The high frequency of operation also undermines the practical applicability of the devices controlled by the operators as alarm triggers for activated LDs, as it is not credible that an operator different from the one loading the green tyre is always available to trigger the alarm. Then, the only trigger applicable to this case study is the SPE.

As mentioned above, the final effect on Pr is driven by the minimum among the two contributions, which is the alarm trigger. In this regard, a requirement for the performance level of the safety functions implemented for risk reduction is established in [27], for every entry of the risk matrix (see Appendix 1). Accordingly, in the analysed failure scenario we are compelled to install a PLd safety function, which yields a reduction of at least 3 points in the Pr factor. To conclude, also in this case, $\overline{Pr}_1^{1,1}$=1, as the risk factors cannot be smaller than 1.

9.1.3 Complementary

Isolation and/or energy dissipation PMs are not applicable to the MUP, as there is no device capable of isolating or dissipating aside the difference of potential energy of the MUP.

Emergency stop. The probability of stopping the evolution of the hazard scenario through the activation of the Emergency stop is very small, as this relates to the situation in which an additional operator is not far from the Emergency stop button and immediately recognizes the emergency situation. For this, we assume that the Av score reduction is negligible and that the emergency stop has no effect on the probability of activating the scenario.

Escape and rescue of trapped persons: this PM is not applicable, as the scenario analysed does not concern operator trapping.

Personal protective equipment impacts on neither Se, as no protection available in industrial practice can reduce the extent of the harm, nor Av, as there is no equipment that can improve the operator capability of leaving the moving space of the machine.

Provisions for better handling of machines cannot reduce the Pr value, due to the fact that the hazardous event is unintentional and mainly due to a momentary lack of attention, rather than to an error in the procedure execution.

9.1.4 Information for use

Pictograms, Visual-Audible alarm and Training on working and emergency procedures are judged to yield a negligible effect on the probability of this scenario. For this, $\overline{Pr}_1^{1,1}$=2. This is due to the fact that, as mentioned before, Information For Use PMs are all expected to bring a negligible effect in preventing distractions when the operators have to execute many times repetitive actions.

With respect to the working procedures, it seems reasonable to assume that the operator tumbling initiating event $E_1^{1,1}$ cannot be prevented by changing working procedures, since operation Op^1 is very simple and the hazardous event relates to an unintentional action of the operator. However, working procedures are requested such that the operator can access the front area (Figure 9) only when the MUP is closed. This would render impossible the occurrence of the hazard scenario and, thus, reduce $\overline{Fr}_1^{1,1}$ to 1. As mentioned before, however, the final reduction of the score depends on the effectiveness of the training procedures (PM 17 in Table 1), which mitigate the reduction in the Fr score. We assume that the final score is $\overline{Fr}_1^{1,1} = 2$, with a reduction of two points.

The effect on Av of the Training on Working and Emergency Procedures PM is also negligible, as there is no particular procedure to improve the operator escaping from the machine moving space.

9.1.5 Results

To conclude, the application of the working procedure PM together with the activated LD make the risk of the scenario acceptable, as Se=4, whereas Pr=min(2,1)=1, Fr=min(2,4)=2, Av=min(3,1)=1. Then, Cl=4 and the risk becomes acceptable (see Table 2). This result cannot be compared to [15], as this latter does not report the analysis of the effects of PMs on risk reduction.

Table 2: case study results

Se	Pr	Fr	Av	Cl
4	min(2,1)=**1**	min(2,4)=**2**	min(3,1)=**1**	**4**

9.2 Pressure Energy in the bladder when the tyre curing machine is above the semi-closed position

While the upper moving part is locked open, a mixture of gases is inflated into the bladder, whose internal pressure rises up to almost 0.4 bars. This allows correctly positioning the green tyre in its plate. Later, when the moving upper part starts closing, the pressure reaches almost 6 bars and, finally, it reaches almost 30 bars when the MUP is locked closed.

The hazard scenario $S_1^{1,2}$ we are considering refers to the first part of the pressure cycle, at 0.4 bars, which lasts almost 60 seconds. The hazardous event $E_1^{1,2}$ is the blow up of the bladder, which could result into a release of very hot steam together with small, sharped particles of the green tyre with high kinetic energy. This can cause serious injuries to the operators performing operation Op^1.

$E_1^{1,2}$ can be due to either a flaw of the bladder, which undermines its capability of withstanding the pressure load, or a failure in the pressure control system, which leads to a bladder overpressure and the consequent overload on the green tyre that can blow up, or to an erroneous setting of the pressure value due to a human error (see Figure 11). From the evidence gathered in production plants, the probability of $E_1^{1,2}$ is cautiously estimated as $Pr_1^{1,2}$ =3.

HZ is defined as the zone where the steam temperature or the kinetic energy of the released small green tyre particles is sufficient to cause injuries. A refined simulation model should be built to map the different energy levels of steam and sharped particles onto the radius of HZ and, thus, onto the possible severities of the injuries. For example, we can rely on a map similar to that of Figure 4. However, this simulation model is still lacking; then, we rely on judgments from experts, who conservatively assume that the zone indicated by Area 1 in Figure 9, which is accessed by the operator to perform Op^1 is certainly included in the HZ where the harm severity is $Se_1^{1,2} = 4$, whereas the severity is negligible in the other zones. For this, the same considerations drawn for the previous scenario apply for the estimation of factor $Fr_1^{1,2}$. The difference in this case is that the duration of the hazardous condition is 60 seconds, instead of 30. Accordingly, the probability of entering the hazardous zone while the bladder is not inflated at 0.4 bars can be roughly estimated as 1-60s/1200s=0.95. This probability value must be squared to consider that the accesses are two in every cycle. Then the probability of not having an overlap is 0.90. Thus, the probability of having overlap of Op^1 and bladder inflated within a 1 hour machine operation interval is 1-0.90^3=0.27. That is, the frequency of $HS^{1,2}$ is almost three events every ten hours. According to the risk matrix in Appendix, $Fr_1^{1,2}$=5, which is de-rated by one to take into account that the exposure duration is shorter than 10 minutes. Thus, the final score is $Fr_1^{1,2}$=4.

Finally, the very high speed of both the green tyre particles and the steam entails that the time the operator takes to recognize the blow up may be larger than that of the particles to reach him/her. Accordingly, $Av_1^{1,2} = 5$.

To sum up, $Cl_1^{1,2} = Fr_1^{1,2} + Pr_1^{1,2} + Av_1^{1,2}$=4+3+5=12, whereas $Se_1^{1,2} = 4$. From the risk matrix in Appendix I we conclude that the risk is not acceptable. To reduce it, we perform a mapping between $(E_1^{1,2}, S_1^{1,2})$ and the 18 classes of PMs, to select those applicable to this scenario and quantify the reduction in the risk scores.

Notice that the final value of Cl is different from that found in [15] for the same risk scenario. This difference cannot be further investigated, due to the lack of details on the estimation of the single subfactors of the likelihood factor. However, the structured reasoning used for the analysis makes the risk analysts more aware and confident on its final results.

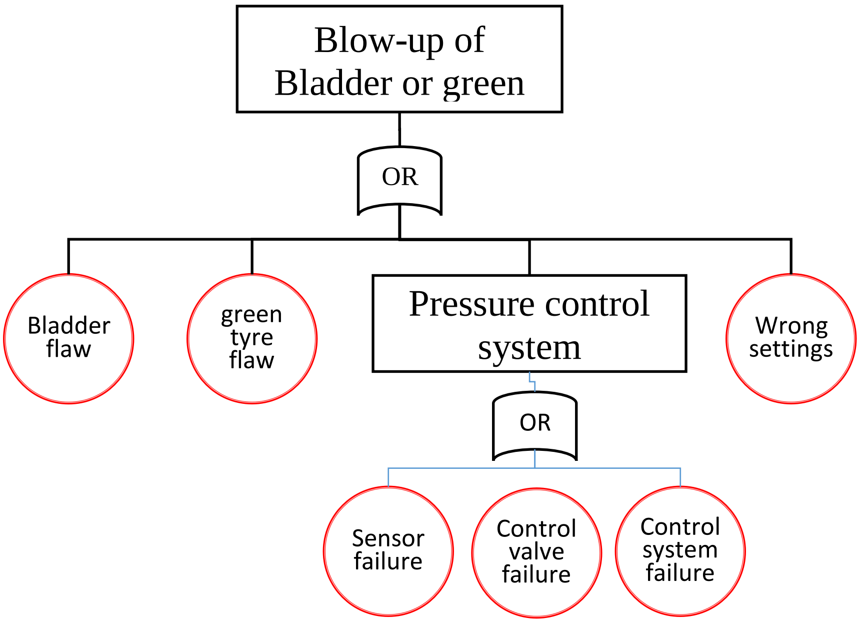


Figure 11: Fault Tree of the initiating event

9.2.1 Risk reduction by design

Pressure energy is necessary for the tyre curing process; then, hazard energy reduction PMs are not applicable to $S_1^{1,2}$.

The impact of the working procedures on Fr is discussed in Section 9.2.4. Working procedures can also impact on the probability of the initiating event $E_1^{2,2}$, as this also depends on the human error of the set-up operator in setting the pressure. However, before quantifying the reduction in the Pr score, it should be borne in mind that the final effect of the PMs on the probability of $E_1^{2,2}$ depends on the reduction of all its causing events, as modelled by the OR gate in the Fault Tree of Figure 11. In this respect, the reliability improvement PMs can certainly reduce the probability of failure of both the pressure control system and the bladder. However, when the cause of $E_1^{2,2}$ is a defect of the green tyre, a reduction of the failure probability can only be achieved through a change of the entire process to produce the green tyre. This is not doable, as it would require a major change in the working procedures, which could consider an X-ray control on the green tyre before its loading.

To sum up, we cannot reduce $Pr_1^{1,2}$ because we have no viable PM to avoid the green tyre flaw event leading to $E_1^{1,2}$.

The considerations about the probability of $E_1^{1,2}$ allow us highlighting two main issues, which will be addressed in future research work:

1) The approach we are using to safety PM selection and positioning is based on what-if analyses, through which we consider the effect of the PMs and check whether the risk decreases beyond the acceptable threshold. This way, the set (i.e., portfolio) of PMs finally installed may be not cost-efficient.
2) The rule of considering the final reduction score of an OR gate as the minimum of the reduction values of its input events may be very limiting.

9.2.2 Safeguarding

Fixed guards cannot be installed on Area 1, as justified in the analysis of $H_1^{1,1}$.

Fixed LDs allow the bladder pressure to not exceed a pre-fixed threshold value. Although in principle they can be applied for risk reduction in the analysed scenario, their practical application is undermined by the fact that the curing cycle relies on different pressure values in the different phases (0.4, 6 and 30 bars). Then, it is not possible to assure that the pressure does not exceed 0.4 bars if we know that it must reach 30 bars.

With respect to activated LDs, as mentioned for scenario $S_1^{1,1}$, interlocking guards and the devices controlled by operators are not eligible as alarm triggers for activated LDs, due to the high frequency of the operations. Then, we assume that SPE is used to trigger the activated LD.

Activated LDs completely de-energize the pressure hazard, with consequent 100% reduction of the hazard energy and, thus, of HZ. Accordingly, $Se_1^{1,2}$=1 and $\overline{Fr}_1^{1,2}$ =1, assuming that the HZ is included in the zone limited by SPE. With respect to the avoidance factor, the effect of activated LDs is on factor q, which increases to infinite the time to safely recover from the HS. Then, $\overline{Av}_1^{1,2}$ is set to 1.

With respect to the probability of occurrence of the hazardous event, its reduction depends on both the intrinsic failure probability of the activated LDs and the failure probability of the alarm triggers. The same considerations for the activated LD of $S_1^{1,1}$ apply and, thus, $\overline{Pr}_1^{1,1}$=1.

The effect of the interlocking guards on Fr is that of reducing HZ. As mentioned above, the installation of these PMs is not recommended when the frequency of the operations requiring the interlocking opening is high, as in the present case.

9.2.3 Complementary

Isolation and/or energy dissipation PMs are not applicable to the MUP under analysis, as these are typically applicable for operations related to maintenance, only.

Emergency stop. This PM is not applicable, as the scenario analysed is so fast that it is not credible that an additional operator is always so prompt to immediately recognize the emergency situation.

Escape and rescue of trapped persons: this PM is not applicable, as the scenario analysed does not concern operator trapping.

Personal protective equipment is not applicable, as the protections commonly available in industrial practice to reduce the effect of steam on a human body are not comfortable for operating the tyre curing machine.

No effect on Av, as there is no equipment that can improve the operator capability of leaving the moving space of the machine.

Provisions for better handling of machines cannot reduce the Pr value, due to the fact that the hazardous event is due to a device failure/green tyre flaw or human error.

9.2.4 Information for use

Pictograms, Visual-Audible alarm and Training on Working and Emergency Procedures also in this case are judged to have no effect on Pr.

With respect to the working procedures, theoretically these can heavily impact on Fr: by enabling the operator access to the front zone (Figure 9) only when the MUP is closed, we render impossible the occurrence of $HS_1^{1,2}$ and, thus, we can set $\overline{Fr}_1^{1,2}$ =1. As mentioned before, the final reduction in the Fr score is mitigated by the effectiveness of the training procedures (PM 17 in Table 1), which yield a final score $Fr_1^{1,2}$=2.

The effect on Av of Training on Working and Emergency Procedures is also negligible, as there is no particular procedure to improve the operator escaping from the machine moving space.

9.2.5 Results

To conclude, in this scenario the application of activated LDs is sufficient to make the risk acceptable, as Se=1, Av=1, Fr=1, Pr=1 and, then, Cl=3. Also in this case, we cannot compare the result to [15], as this latter does not report the analysis of the effects of PMs on risk reduction.

Table 3: results of the case study

Se	Pr	Fr	Av	Cl
1	1	1	1	3

10 Analysis and discussion of the results

By applying the proposed methodological framework to the tyre curing machine case study, the risk analysts have particularly appreciated the reasoning scheme proposed in Section 4, as it forces to unambiguously identify the initiating event, the hazardous situation and, then, sketch the hazardous scenario. This is deemed fundamental to improve the repeatability of the estimation of the scores of the risk factors. For comparison, the analysis in [15] of the second scenarios discussed in Section 9 starts from the identification of the hazardous situation (i.e., pressure to the bladder when the tyre curing machine is above the semi closed position for the scenario in Section 9.2) and, then, finds the corresponding hazard (e.g., bursting and ejection of materials or steam). In our view, the hazard is the pressure energy, whereas the release of materials is a first event in the event sequence originated by the hazardous event of bladder failure (i.e., $E_1^{1,2}$, not mentioned in [15]), which ends with the harmful consequences to the operator, should she/he be in the hazardous area. To the risk analysts, the reasoning approach proposed in this work makes clearer the roles of hazard, initiating event, hazardous situation, etc., and how they are linked to the three factors of likelihood, which could become equivocal otherwise.

The proposed classification into 18 groups of the PMs considered by ISO/TR 14121-2: 2012, has been judged as a good compromise solution between the need of working with a limited number of alternatives for building the mapping of PMs onto the risk factors and that of providing the machine designers with specific solutions for risk reduction. Moreover, the changes introduced by our classification with respect to ISO/TR 14121-2: 2012 are considered not compromising the compliance of the proposed framework to the standards.

The systemic approach to map the 18 PM classes onto the risk factors they affect has been considered the most critical point of the methodology, as it does not fully agree with ISO/TR 14121-2: 2012. Although the mapping is deemed clear and preventing possible misunderstanding, nonetheless the risk analysts wonder what would be the impact of producing analyses not fully compliant with the technical report ISO/TR 14121-2: 2012. This remains an open issue to be addressed together with the reference committees.

The insights given about the estimation of the score reduction yielded by the PMs in different contexts and scenarios have been considered useful for the risk analysis of a machinery with PMs. In this respect, notice that quantitative metrics of the benefits obtained cannot be disclosed.

Finally, generalization of the proposed approach is an open issue, which requires harmonizing and synthesizing the many standards cited in Section 7. This issue, together with those concerning the improvement of the methodology described and its validation on other case studies, will be tackled in future research works

11 Conclusions

In this work, a methodological framework is developed to carry out risk analyses compliant with ISO 12100: 2010. This is specific for the tyre production industry, although the considerations outlined are general and applicable to other industries. The methodology builds on ISO/TR 14121-2: 2012 to propose a scheme for identifying the contribution of PMs to the reduction of risk in a machinery under design. A classification is provided of the PMs commonly used in industrial practice, enhancing the classification given in ISO/TR 14121-2: 2012 and a systemic approach is developed to map the 18 PM classes onto the risk factors they affect.

Insights are given on how to estimate the score reduction yielded by the PMs in different contexts and scenarios, with examples to structure the risk analysis of a machinery with PMs. Generalization is an open issue, which requires harmonizing and synthesizing the many standards cited in Section 7. This is something to be considered by the reference committees.

The methodology has been applied in practice by expert risk analysts from Pirelli Tyre to a real case study concerning a tyre curing machine. The risk analysts involved have appreciated the systemic approach for considering all PM classes and analysing their impacts on the risk factors, which gives a structured guide to estimate risk reductions.

12 References

[1] AIEA: Defence in depth in nuclear safety: INSAG-10/ a report by the International. Nuclear Safety Advisory group. - Vienna: International Atomic Energy Agency, 1996.

[2] Andersen, H., Casal, J., Dandrieux, A., Debray, B., De Dianous, V., Duijm, N. J., et al. ARAMIS—user guide. EC Contract number EVG1-CT-2001-00036 (2004).

[3] ANSI/ASHRAE (American National Standards Institute/American Society of Heating, Refrigeration and Air-conditioning Engineers), ANSI/ASHRAE Standard 55–2004 Thermal Environmental Conditions for Human Occupancy. Atlanta, GA, ASHREA, 2010.

[4] Aven, T., Renn, O., On risk defined as an event where the outcome is uncertain, Journal of Risk Research, Vol. 12, pp. 1-11, 2009.

[5] Aven, T., The risk concept—Historical and recent development trends, Reliability Engineering and System Safety, Vol. 99, pp. 33-44, 2012.

[6] Bethea, D., Parsons, K.C., The Development of a Practical Heat Stress Assessment Methodology for Use in UK Industry (Research Report 008). HSE. Retrieved from http://www.hse.gov.uk/research/rrpdf/rr008.pdf, 2002.

[7] Burlet-Vienny, D., Chinniah, Y., Bahloul, A., Roberge, B., Design and application of a 5 step risk assessment tool for confined space entries, Safety Science, Vol. 80, pp. 144-155, 2015.

[8] Caputo, A.C., Pelagagge, P.M., Salini, P. AHP-based methodology for selecting safety devices of industrial machinery, Safety Science, Vol. 53, pp. 202-218, 2013.

[9] Chinniah, Y., Gauthier, F. Industrial machinery risk assessment tools: A review of risk estimation parameters, Proceedings of International Conference on Computers and Industrial Engineering, CIE, 1, pp. 229-241, 2013.

[10] Chinniah, Y., Gauthier, F , Lambert, S., Moulet, and F. Experimental Analysis of Tools Used for Estimating Risk Associated with Industrial Machines, 77 pages. Report R-684. Montreal: IRSST (Research Institute Robert-Sauvé Health and Safety), 2011.

[11] de Galvez, N., Marsot, J., Martin, P., Siadat, A., Etienne, A., EZID: A new approach to hazard identification during the design process by analysing energy transfers, Safety Science, Vol. 95, pp. 1-14, 2017.

[12] Delvosalle, C., Fiévez, C., Pipart, A., Debray, B., ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. Journal of Hazardous Material, Vol. 130(3), pp. 200–219, 2006.

[13] EN 982:1996 + A1:2008, Safety of machinery - Safety requirements for fluid power systems and their components – Hydraulics, 2008.

[14] EN 983:1996 + A1:2008, Safety of machinery - Safety requirements for fluid power systems and their components – Pneumatics, 2008.

[15] EN 16474:2015 E, Plastics and rubber machines - Tyre curing machines –Safety requirements, European Committee for Standardization, 2015.

[16] Gauthier, F., Lambert, S., Chinniah, Y. Experimental analysis of 31 risk estimation tools applied to safety of machinery, International Journal of Occupational Safety and Ergonomics, Vol. 18 (2), pp. 245-265, 2012.

[17] Gnoni, M.G., Bragatto, P.A., Integrating major accidents hazard into occupational risk assessment: An index approach, Journal of Loss Prevention in the Process Industries, Vol. 26(4), pp. 751-758, 2013.

[18] Guldenmund, F.W., Hale, A.R., Goossens, L.H.J., Betten, J., Duijm, N.J., The development of an audit technique to assess the quality of safety barrier management, Journal of Hazardous Material, Vol. 130(3), pp. 234–241, 2006.

[19] IEC/EN 62061: 2005, ”Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems.

[20] IEC TS 60479-1: 2005, Effects of current on human beings and livestock - Part 1: General aspects.

[21] ISO 12100:2010 Safety of machinery -- General principles for design -- Risk assessment and risk reduction, International Organization for Standardization, Geneva, 2010.

[22] ISO 13732–1:2005 Ergonomics of the Thermal Environment –Methods for the Assessment of Human Responses to Contact with Surfaces –Part 3: Cold Surfaces, International Organization for Standardization, Geneva, 2005.

[23] ISO 13849, Safety of machinery -- Safety-related parts of control systems. International Organization for Standardization, Geneva, 2006.

[24] ISO 31010:2009 Risk Management – Risk Assessment techniques, International Organization for Standardization, Geneva, 2010.

[25] ISO 7933:2004, Ergonomics of the thermal environment— Analytical determination and interpretation of heat stress using calculation of the predicted heat strain, International Organization for Standardization, Geneva, 2004.

[26] ISO 9886:2004 Ergonomics –Evaluation of Thermal Strain by Physiological Measurements, International Organization for Standardization, Geneva, 2004.

[27] ISO/TR 14121-2: 2012 Safety of machines – Risk assessment: Practical guidance and examples of methods, Second edition, International Organization for Standardization, Geneva, 2012.

[28] Johansen, I.L., Rausand, M., Ambiguity in risk assessment, Safety Science, Vol. 80, pp. 243–251, 2015.

[29] Kaplan, S., Garrick B.J., On the quantitative definition of risk, Risk Analysis, Vol. 1, pp. 11-27, 1981.

[30] Keeney, R., H. Raiffa. Decisions with Multiple Objectives: Preferences and Value Trade-Offs. John Wiley & Sons, New York, 1976.

[31] Kirkwood, C.W., Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets. Duxbury Press, Belmont, CA, 1997.

[32] Kirwan, B., A Guide To Practical Human Reliability Assessment, CRC Press, 1994.

[33] Levitin, G., Lisnianski, A., Structure Optimization of Power System with Bridge Topology, Electric Power Systems Research, Vol. 45, pp. 201-208, 1998.

[34] Moedden, H., Probabilities in safety of machinery—elements of a risk model and comparison with field data, Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, pp. 515-521, 2015.

[35] NASA/SP-2010-580/Version 1.0, HQ-STI-12-032: NASA System Safety Handbook. Volume 1; System Safety Framework and Concepts for Implementation, 2011.

[36] Neogy, P., Hanson, A.L., Davis, P.R., Fenstermacher, T.E., Hazard and Barrier analysis guidance document, Rev. 0. US Department of Energy (DoE), 1996.

[37] Nix, D., Chinniah, Y., Dosio, F., Fessler, M., Shrever, M. Linking Risk and Reliability—Mapping the output of risk assessment tools to functional safety requirements for safety related control systems, Proceedings of EMC Society Symposium, Dresden, 2015.

[38] Paques, J.J., Gauthier, F., Perez, A. Analysis and Classification of the Tools for Assessing the Risks Associated With Industrial Machines, International Journal of Occupational Safety and Ergonomics, Vol. 13(2), 173-187, 2007.

[39] Petroleum Safety Authority Norway, Principles for barrier management in the petroleum industry, 29.01.2013.

[40] Podofillini, L., Park, J., Dang, V. Measuring the influence of task complexity on Human error probability: an empirical evaluation. Nuclear engineering and technology, Vol. 45(2), pp. 151-164, 2013.

[41] Sadeghi, L., Mathieu, L., Tricot, N., Al Bassit, L., Developing a safety indicator to measure the safety level during design for safety, Safety Science, Vol. 80, pp. 252-263, 2015.

[42] Salo, A., Hämäläinen, R.P., Preference ratios in multiattribute evaluation (PRIME) – elicitation and decision procedures under incomplete information, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 31(6), pp. 533-545, 2001.

[43] Salvi, O., Debray B., A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive, Journal of Hazardous Material, Vol. 130(3), pp. 187–99, 2006.

[44] Skelt, S., Safety barriers: Definition, classification, and performance, Journal of Loss Prevention in the Process Industries, Vol. 19(5), pp. 494–506, 2006.

[45] Svenson, O., The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries, Risk Analysis, Vol. 11(3), pp. 499–507, 1991.

[46] Von Winterfeldt, D., Edwards, W., Decision Analysis and Behavioral Research, UK: Cambridge University Press, Cambridge, 1986.

[47] Zio, E., An Introduction to the Basics of Reliability and Risk Analysis, World Scientific Publishing, 2007.

Appendix

Table 4: Risk matrix compliant with ISO/TR 14121-2 ([21])

Injury Severity **Se**		Likelihood **Cl** (Fr+Pr+Av)					Hazard Exposure Frequency **Fr**		Probability of Occurrence of Hazardous Event **Pr**		Harm Avoidance **Av**	
		3-4	5-7	8-10	11-13	14-15						
Very serious (Fatality, permanently debilitating injury or illness, that is involving the loss of an organ and therefore its function)	4	🟨	🟥 d	🟥 d	🟥 e	🟥 e	> 1/ h	5	Very High	5	Impossible	5
Serious (Seriously debilitating injury or illness, that is involving the weakening of an organ and therefore its function)	3		🟨	🟧 c	🟥 d	🟥 e	≤ 1 /h & > 1/24 h	5	Probable	4	Possible	3
Moderate (Injury or significant disease requiring specialized medical treatment)	2			🟨	🟧 c	🟥 d	≤ 1/24 h & > 1/ 2weeks	4	Possible	3	Probable	1
Minor (Injuries or minor injuries requiring first aid (no loss of working days))	1				🟨	🟧 c	≤ 1/ 2weeks & > 1/ year	3	Rare	2		
Red and Orange areas: safety barriers required Yellow area: additional barriers.							≤ 1/year	2	Negligible	1		