Chapter 6

Machinery Safety Requirements as an Effective Tools for Operational Safety Management

Hana Pacaiova

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.71152

Abstract

Free circulation of goods is the major pillar of the single united market of European Union's (EU) member states and main motivated power of competitiveness and economical acceleration in EU. By using the legislative were defined base requirements on goods and also high level of authorized interest protection of goods users. The main changes in H&S (Health and Safety) management and also in Machinery safety started after implementation the Framework Directive 89/391/EEC and Directive 89/392/EEC in 1989 year. Directive 89/391/EEC implements systematical tools in H&S management as: H&S politics, Risk Management, education requirements, review activities, employee's involvement in H&S procedures. Directive 89/392/EEC, on the present time 2006/42/EC directive, implements for machinery producer or its contractor duties to access risk for each stage of machinery life cycle and implement adequate measures. These legislative requirements had changed all procedures and rules, which were used in H&S area.

Keywords: safety management, risk assessment, equipment criticality, maintenance, safety integrity

1. Introduction

Legislation defines a framework of organization operations and their fulfillment is a part of organization's business policy. Accepting customer's requirements also means fulfillment of legal requirements (e.g. laws, standards, regulations) [1, 2].

Risks management is a basic tool for demonstration of meeting the requirements in different areas of organization management (e.g. occupational health and safety, accidents prevention, critical infrastructure, dangerous substances transportation, environmental or financial requirements). Management of the organization often times is kind of "lost" while determining effective

economical actions to be able to follow the required legal frameworks of a business environment or achieve its own and more difficult goals. Benefits of the decision-making process, their reliability and efficiency are determined by a risk assessment analysis, which is increased by improper applied processes, risk assessment methods and a measurements selection for their management [1, 3, 4].

ISO 31000:2009 standard allows us to globally understand the risks assessment versus "unwanted losses" on an integrated level of all the management activities. However, this integrated management requires specific processes and methods of the risks management, which is derived from the system/object properties, risks assessment goals and processes management level in the organization [3].

2. Safety legislative requirements

Risks assessment is a basic requirement of technical systems safety and occupational health and safety (OHS) management.

2.1. Occupational health and safety management

Human legal requirement is a basic for assessing the safety level at work by meeting the minimal requirements which is defined by Council directive 89/391/EEC ("Framework Directive"); on the introduction of measures to encourage improvements in the safety and health of workers at work.

The scope of this Directive is defined for employers and employees in all sectors of the productive and non-productive sphere [1].

The Directive defines general requirements for prevention for an employer, who is obliged to apply the general principles of the prevention when implementing the measures necessary to ensure the safety and health protection at work, including the information, education and organization of work and tools. These principles include [1]:

- Exclusion of the hazard and the possible resulting risk.
- Risk assessment that cannot be excluded, especially while selecting or using working tools, materials, substances and methods.
- Implementation of the measures to eliminate hazards at the site of their occurrence.
- Prioritization of collective protective measures against individual protective measures.
- Planning and implementing a policy of the prevention through the safety working tools, technologies. methods, improvement of the working conditions with regard to working environment factors and through social measures.

The Directive application can be defined as follows:

- It is applied to all public and private areas, such as industry, agriculture, commerce, services, education, culture, leisure, and so on.

http://dx.doi.org/10.5772/intechopen.71152

- It does not concern areas, where specific public services and activities are involved, e.g. military and police activities or civil protection activities that may conflict with its requirements.

A number of specific directives (see **Figure 1**) have been adopted to implement the requirements of this Directive as individual directives within the meaning of Article 16 (1) of Directive 89/391/EEC in the following order (1. e.g. first individual Council Directive, etc.):

1. 89/654/EEC of 30th of November 1989 concerning the minimum safety and health requirements for the workplace.
2. 2009/104/EC (original 89/655/EEC) of 16th of September 2009 on the minimum health and safety requirements regarding the use of work equipment by workers at work.
3. 89/656/EEC of 30th of November 1989 concerning the minimum health and safety requirements for the use of personal protective equipment by workers at work.
4. 90/269/EEC of 29th of May 1990 on the minimum health and safety requirements for the manual handling of loads, especially where is a risk of injury to the lumbar spine of workers.
5. 90/270/EEC on minimum safety and health requirements for work with displaying units.

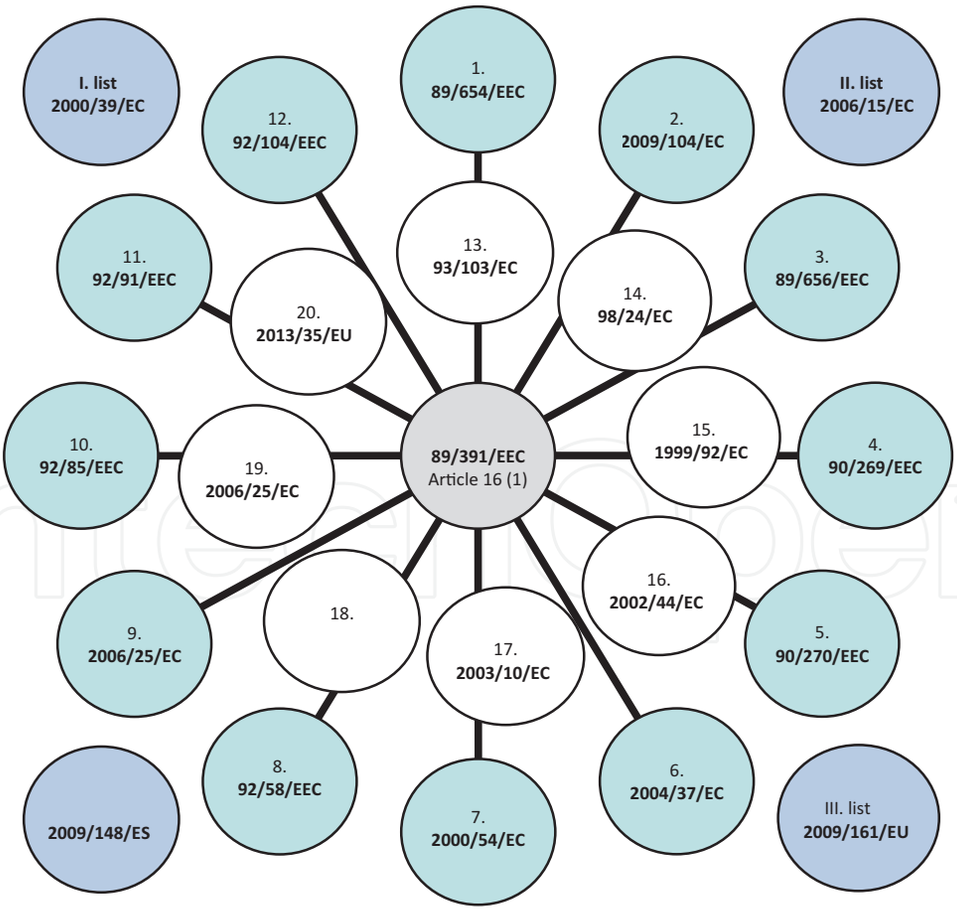

Figure 1. Relation between commission directive 89/391/EEC and individual council directives in accordance with Article 16 (1) [1].

6. 2004/37/EC of the European Parliament and of the Council of 29th of April 2004 on the protection of workers from the risks related to exposure to carcinogens and mutagens at work.

7. 2000/54/EC of the European Parliament and of the Council of 18th of September 2000 on the protection of workers from risks related to exposure to biological hazards at work, which is a consolidated directive of the previous Directives.

8. 92/57/EEC of 24th of June 1992 on the introduction of minimum safety and health requirements for temporary or site-changing buildings.

9. 92/58/EEC of 24th of June 1992 on the minimum requirements for the provision of safety and health signs at work.

10. 92/85/EEC of 19th of October 1992 on the introduction of measures to encourage improvements in the safety and health at work of pregnant workers and workers who have recently given birth or are breastfeeding.

11. 92/91/EEC of 3rd of November 1992 on the minimum requirements for improving the safety and health protection of workers in the extractive industry.

12. 92/104/EEC of 3rd December 1992 on the minimum requirements for improving the safety and health protection of workers on the ground and underground mining.

13. 93/103/EC of 23rd of November 1993 concerning the minimum safety and health requirements for work on board fishing vessels.

14. 98/24/EC of 7th of April 1998 on the protection of the health and safety of workers from the risks related to chemical factors at work.

15. 1999/92/EC of the European Parliament and of the Council of 16th of December 1999 on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive environment.

16. 2002/44/EC of the European Parliament and of the Council of 25th of June 2002 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical factors (vibration).

17. 2003/10/EC of the European Parliament and of the Council of 6th of February on minimum health and safety requirements regarding the exposure of workers to the risks arising from physical nuisance (noise).

18. Canceled Directive 2004/40/EC of the European Parliament and of the Council of 29th of April 2004 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical factors (electromagnetic fields), note: replaced by 20th Council Directive.

19. 2006/25/EC of the European Parliament and of the Council of 5th of April 2006 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical factors (artificial optical radiation).

20. 2004/35/EC of the European Parliament and of the Council of 18th of June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical factors (electromagnetic fields).

Other significant directives on OHS, but not issued as individual directives under Article 16 (1) The Health and Safety Directives can be classified as:

- Commission Directive 2000/39/EC of 8th of June 2000, which establishes the first list of indicative occupational exposure limit values for the implementation of Council Directive 98/24/EC on the protection of the health and safety of workers from the risks related to chemical factors at work.
- Commission Directive 2006/15/EC of 7th of February 2006, which establishes the second list of indicative occupational exposure limit values for the implementation of Council Directive 98/24/EC and amending Directives 91/322/EEC and 2000/39/EC.
- Commission Directive 2009/161/EU of 17th of December 2009, which establishes the third list of indicative occupational exposure limit values for the implementation of Council Directive 98/24/EC and amending Commission Directive 2000/39/EC.
- Directive 2009/148/EC of the European Parliament and of the Council of 30th of November 2009 on the protection of workers from the risks related to exposure to asbestos at work.

2.2. Machinery safety

The Machinery Directive 2006/42/EC on the approximation of the laws for the Member States relating to machinery is intended especially for machinery suppliers. For the machinery operators, the rules required in accordance with Directive 2009/104/EC, which replaced Directive 89/655/EEC, the so-called "The second individual Directive within the meaning of Article 16 (1) of Directive 89/391/EEC on the minimum safety and health requirements for the use of working equipment by workers at work (**Figure 2**).

The Machinery Directive covers the use of all technical equipment, including mobile and lifting equipment. These devices must be regularly inspected and maintained to ensure their readiness and security.

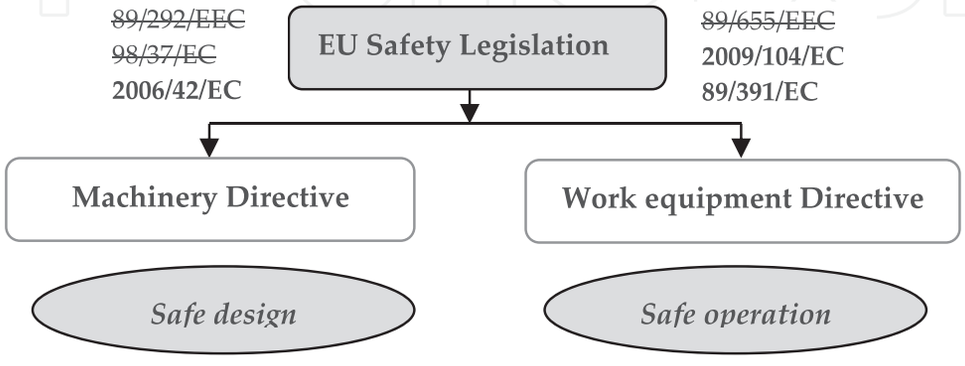

Figure 2. History of legislation on machinery safety and OHS.

The objective of this directive is to increase the level of equipment safety, with an emphasis on the analysis of possible risks in their intended operation and maintenance at the design and construction stage of the equipment. Emphasis is also placed on the creation of metering points for monitoring the status of equipment by the methods of the technical diagnostics already at the stage of the project. This creates conditions to prevent the occurrence of breakdowns and possible accidents by defining a real technical state, the impact of which would have an obvious effect on the safety and health of the operator or public. An important aspect is a detailed description of the operational regulations requirements in the native language of the country, where the technical equipment is in operation. Then, there are created standardized procedures for informing the operator of the existing hazards and residual risks arising from the operation of these devices [1, 5].

In accordance with Annex I, 1 Machinery Directive is a manufacturer of a machine or a complex technical device obliged to define the hazards, that arise during the operation of the machine, to estimate the consequences of possible injury or damage to health as well as the probability of their occurrence, and then determine and asses risks in order to take measures to minimize them. This is also connected with an obligation to provide machine user relevant information on residual risks.

These requirements make activities of machinery designers, engineers, manufacturers and users of machinery (including maintenance requirements—item 1.6) conditional upon them. Relevant activities must be conducted in accordance with risk management rules.

2.2.1. Integrated safety principle

The Integrated Safety Principle is defined in Annex I to the Machinery Directive in five steps, as follows:

I. Devices must be designed and constructed in such a way that they are adapted to their function and can be operated, set and maintained, so people who use them are not exposed to the risks under the foreseeable conditions, also taking into account their reasonably foreseeable wrong use (e.g. operator error).

II. When selecting the most appropriate solutions, the manufacturer or his authorized representative, must apply the following principles in the following order:

- Eliminate or reduce risks as much as possible,
- Take the necessary measures to protect against risks,
- Inform users of the residual risks caused by the various shortcomings in the protective measures taken, notifying whether special training is required and determining any need to provide personal protective equipment.

III. When designing and constructing a machine device and when drawing up the instructions for use, the manufacturer or his authorized representative must assume not only the intended use of the machinery but also his reasonably foreseeable misuse.

http://dx.doi.org/10.5772/intechopen.71152

IV. Machine devices must be designed and constructed in such a way that include taking into account the limitations to which the operator is exposed as a result of the necessary or foreseeable use of personal protective equipment (PPE).

V. Machine devices must be supplied with all the necessary special equipment and accessories to enable them to be safely adjusted, maintained and used.

The objective of the taken measures must be exclusion of any risk for the machine life cycle, including the phases of transport, assembly, disassembly, decommissioning and disposal [5–7]!

The instruction manual must inform about residual risks, meaning that informs a user of the ways, in which the machine devices should not be used.

A **risk** (under the Machinery Directive) is defined as a combination of probability and severity of injury or injury to health that may result from a dangerous situation!

3. Basic principles of a risk assessment

In the risk assessment in the field of OHS, there are usually used simple methods based on the causal model of the accident (hazard → hazard situation → initiation → harm → loss). These methods are usually combined according to their use in the individual steps of the risk assessment algorithm (Brainstorming, Check-list, Risk matrix [1–3]).

The basic risk assessment algorithm is a structured logical sequence of steps (**Figure 3**) [1]. It does not matter whether it is a project, process, technology, device or a provided service. The analyzed system/object must be broken down into individual elements as is required to fulfill a defined task (activity, function). Each element is evaluated separately in terms of the possibility of endangering the target role (function). The probability or frequency, with which this hazard situation may occur at the time considered (duration of action), is the basis for the risk assessment together with the assessment of the severity (consequence) for the target function. In the financial sector, the risk is also declared positively (as ISO 31000 also accepts the concepts of opportunities), while the analysis of technologies and work activities is assessed only in relation to negative consequences [3].

Measures derived from the assessed risks are defined either by legislation (relevant directives for specific areas—hazards, such as work with display units, noise protection, vibration, etc.), or/and requirements resulting from the overall culture and the advancement of the organization's management to reduce the risk value to the lowest level possible (risk acceptability level) [1, 8].

Normally, risk assessment for OHS in organizations uses a "Risk matrix" (see **Table 1**), which is based on an assessment of the probability and consequence of the analyzed hazard that is determined from work activities [1, 9]. Emphasis is placed on a simple form of an evaluation and risk assessment and its understanding by all involved parties (employees, third parties, etc.).

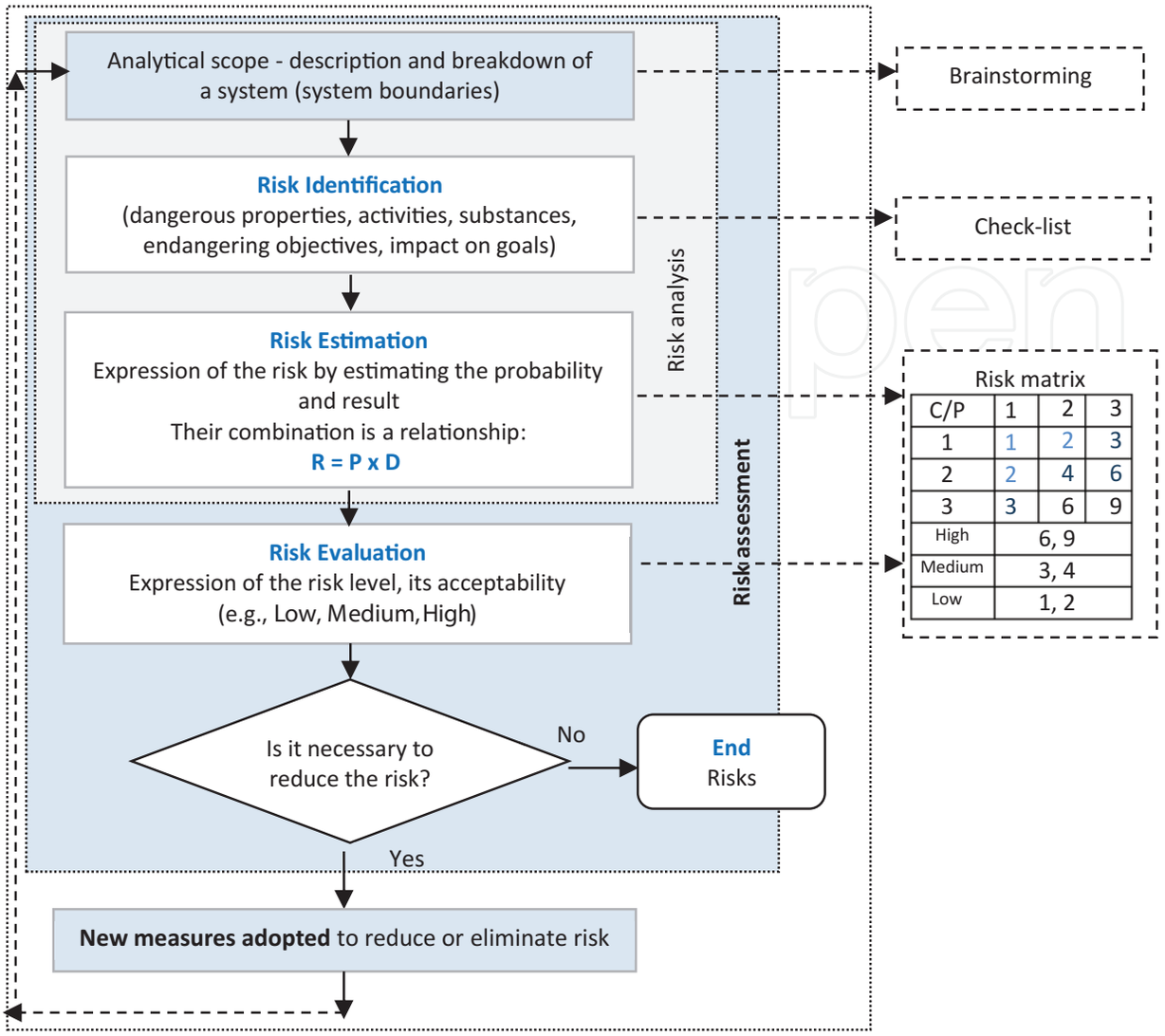

Figure 3. Basic algorithm for risk assessment and management.

Consequence	Probability		
	Low	Medium	Almost certain
Insignificant	L	L	M
Significant	L	M	H
Catastrophic	M	H	H
Risk level	L – low	M – medium	H – high

Table 1. "Risk matrix" example.

It is essential to apply appropriate tools and procedures to meet legislative requirements. These are evolving and changing in terms of requirements for risk assessment, risk management and health and safety management at work. They can be broken down as follows:

http://dx.doi.org/10.5772/intechopen.71152

3.1. Risk assessment

- Canceled standard EN 1050 Machines Safety: Principles of risk assessment (1998- replaced by EN ISO 14121-1: 2007, nowadays canceled too).
- IEC 60300-3-9 Reliability Management: Part 3, Section 9: Risk Analysis of Technical Systems (1995).
- EN ISO 12100 Machines Safety: General principles of machine design; Risk Assessment and Reduction (2010), Consolidation of ISO 12100-1 and ISO 12000-2 requirements.
- Canceled standard ISO 14121-1: Machines Safety: Risk Assessment. Part 1: Principles; TNI/ISO/TR 14121-2: Practical Guides and Examples (2007).

3.2. Risk management

- ISO 31000 Risk management—principles and implementation guides (2009).
- ISO 31010 Risk management—risk assessment techniques (2009).

3.3. Health and safety management systems

- OHSAS 18001:2007: Occupational Health and Safety Management System—Requirements.
- OHSAS 18002:2000: Occupational Health and Safety Management System—Implementation guide OHSAS 18001.
- New standard ISO 45001:2017, which is used to transform and complement the requirements of OHSAS 18001 internationally.

4. Machinery risk assessment standards and tools

The safety issues of machines and machine devices are devoted to a number of harmonized standards which have their hierarchy [1] (see **Figure 4**).

Type A standards: safety standards, providing basic concepts and principles for design, construction and general considerations that can be applied to all machine devices. Basic safety standards of Type A include for example EN ISO 12100.

Type B standards: safety standards that mostly take care of only one safety aspect or one type of safety device that can be used for a larger amount of machines. They are divided into: Type B1 standards, which are related to individual safety aspects (e.g. safety distances, surface temperatures, noise, etc.) and Type B2 standards for the relevant safety devices (e.g. different shields, pressure sensitive devices, two-hand control device, locking device, etc.).

Type C standards: safety standards for machines that define detailed safety requirements for a particular machine type or group of machines. They refer to related Type A and B

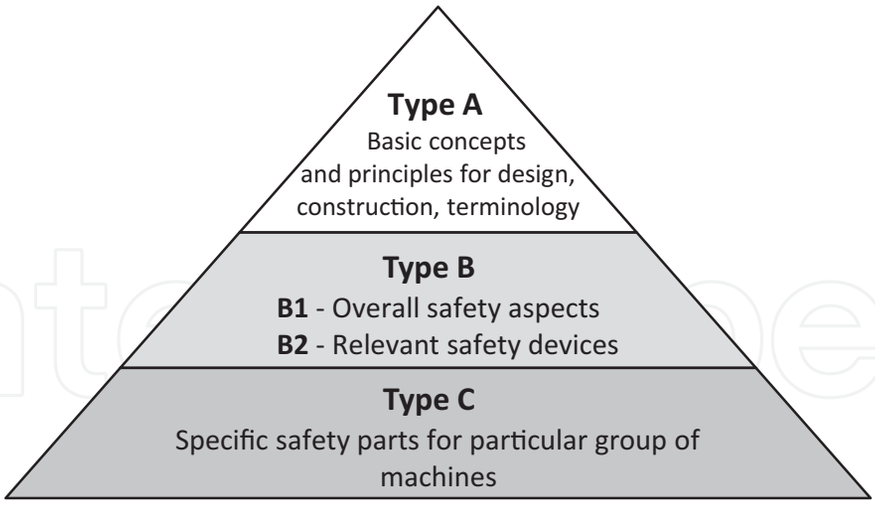

Figure 4. Hierarchy of standards for the machines and equipment safety.

standards or, if possible, also to other Type C standards and define safety requirements and identify the risks and priorities that are required. The principle is that the Type B and C standards cannot be repeated or verbally describe the text of the other standards to which they refer.

From a legal point of view, any product is safe, which is meeting the requirements of the relevant regulation or where no prescription for this product is meeting the standards requirements or corresponding to the state of scientific and technical knowledge known at the time of its placing on the market.

In general, the safety assessment rules for health and safety at work are based on the basic principle of meeting the requirements of the technical regulations and standards.

4.1. Requirements of EN ISO 12100

The requirements of directive 2006/42/EC support EN ISO 12100—defines the terminology and methodology used to achieve machine device safety. The purpose of this standard is to provide to the constructors a basic framework for designing safe machines. This standard has a historical development from the basic standard EN 292-1, 2, through EN 1050. Now it is replaced also EN ISO 14121-1 standard [1, 10].

The standard is principally structured to:

- Risk assessment, i.e. basic principle and hazards identification.
- Risk reduction, i.e. three-step method and measures.

This standard has a list of the potential hazards to be taken into account when designing a machine device (examples of hazards are part of Annex B, which is taken from the canceled standard ISO 14121-1. Hazards analysis must take into account the entire life-cycle of the machine—from its design, construction, manufacture, installation, operation and maintenance to its disposal.

http://dx.doi.org/10.5772/intechopen.71152

4.2. Risk assessment and reduction strategy

This safety strategy—the risk assessment and risk management steps are defined as follows [1, 11, 12]:

> **Step 1**: determination of machine boundaries, including intended use of the machine and consideration of its foreseeable misuse (e.g. operator errors),
>
> **Step 2**: identification of hazard sources and hazardous situations,
>
> **Step 3**: The risk estimation for each hazard and the resulting hazard situation,
>
> **Step 4**: the risk evaluation and consideration of the necessary reduction by introducing measures,
>
> **Step 5**: elimination of a hazard or risk reduction associated with hazards by applying appropriate measures (application of the so-called three-step risk reduction method).

The first three steps represent a process of **risk analysis**—a combination of specifications for determining the machine boundaries, hazard and hazard situations identification and risk estimation.

The overall procedure includes risk analysis and **risk evaluation** (fourth step). It is the process of **risk assessment**.

The **risk management** process is based on a risk assessment and proposes to take appropriate measures to implement and monitor their effectiveness.

Note: Risk assessment does not include a step of taking measures, only the steps of consideration—the classification of the estimated size of the risk according to the pre-selected scheme (e.g. the risk matrix) and the decision-making process "what to do with that now" based on the risk acceptance rate.

This risk management process is a basic and unchangeable process, and represents an iterative approach (ALARP—As Low As Reasonably Practicable), which the designer or constructor must observe in designing the machine, but also the user in managing workplace safety [1, 12].

The designer must consider designing the machine, all anticipated activities (even not expected ones during normal use of the machine), production must take into account possible risks in a machine manufacturing, the user (or the employer) must ensure the safety of the machine in the working environment.

4.2.1. Step 1: determination of machine boundaries

The purpose of this step is to understand the principles of machine operation, the conditions and the way it is used. Determining machine boundaries serves to identify sources of hazards, a description of possible hazard scenarios while performing the required activities (e.g. machine operator and maintenance, visit, or third-party activities performed at the working site), or predictable behavior when using the machine by unskilled workers. Also an appropriate

procedure is to define the so-called functional machine structures for identifying dangerous elements on the machine. It can be, for example a control function, safety function, stability function, etc.

Procedures to determine the machine boundaries according to EN ISO 12100 standard [1]:

Usage limits (intended use and foreseeable misuse)

- Operating modes and preventive procedures, including manipulation with the machine when misused,
- The way and the place for the machine use (household, industry) by persons, their skills and the ability to use the machine,
- Expected level of qualification, experiences, education and capabilities of the concerned persons (a maintenance worker, an attendant, an apprentice or public),
- Other persons who may be at risk from the machine (other machines operation, administrative staff, visits).

A. Layout: range of motion, operating and maintenance area, relationship between the machine and power source.

B. Time limit: machine lifespan (parts), maintenance intervals.

C. Other boundaries: properties of the processed material, purity, environment (temperature, external conditions, etc.).

4.2.2. Step 2: identification of hazards

After determining machine boundaries, the basic step of the risk assessment is to identify the types of hazard situation depending on the hazard properties of the machine, taking into account each stage of the machine's life-cycle [1, 4, 8, 9, 11].

Account is also taken of the behavior of the operator [1, 11, 13], e.g.:

- Loss of control by the operator (e.g. manual or mobile machines),
- Improper behavior of the person in the event of failure of the machine, in the event of a breakdown or accident,
- Behavior resulting from lack of a concentration or inattention,
- Behavior resulting from the search for options beyond the prescribed procedure (instruction manual), the "least resistance way,"
- Behavior resulting from the effort to keep the machine running at all costs,
- Behavior of another group of people (children, people with disabilities).

EN ISO 12100 provides a description of 10 types of potential hazards (e.g. mechanical, electrical, thermal, noise, vibration, radiation, ergonomics, etc.), their potential sources and possible consequences. It is based on the requirements of the Machinery Directive.

http://dx.doi.org/10.5772/intechopen.71152

Similarly, it is possible to proceed with identifying hazards in relation to the work being done at the workplace in order to assign appropriate personal protective equipment.

4.2.3. Step 3: risk estimation

This is one of the most important risk assessment steps [1, 3, 9, 11]. The level of the risk reflects the severity of a hazardous situation and is dependent on the following parameters:

a. Consequence *C* or the severity of the hazard situation: the impact on health, property or environment,

b. Probability *P* of the damage occurrence that depends on:

- Exposure of the person to the hazard situation, Exposure time: *E*,
- Probability (or frequency) of occurrence of a hazard situation: P_H,
- Technical and human possibilities to prevent or limit the range of possible damage: *M* (measure).

The level of risk can be calculated as function of these parameters, using this formula:

$$R = f\left(E, P_H, M, C\right) \tag{1}$$

The risk assessment uses simple methods based on the expression of probabilities and consequences and on the risk evaluation, so-called "Risk matrix" (risk rating tool) […].

Usually the level of risk is defined as combination of these parameters:

$$R = P \times C \tag{2}$$

Creating a Risk matrix as a tool for analysis and risk assessment requires establishing criteria for estimating probabilities and consequences (**Tables 2** and **3**).

For the risk assessor, the "common sense" principle must be applied to determine the range of the level of the assessed parameter (e.g. from 1 to 3).

4.2.4. Step 4: risk evaluation

The risk matrix (see **Table 4**) can be created by the "ordinary" multiplication of the individual levels assigned to the probability and consequence. The number of levels of the estimated

Probability	Level description of a probability	Level
Low	Low probability of event occurrence	1
Medium	An event can be expected with a higher probability	2
High	The probability of occurrence is almost certain	3

Table 2. Description of the probability of occurrence of a hazardous event: *P*.

Consequence	Level description of a severity/consequence	Level
Negligible	Small event impact range, minimal or no consequence, near-miss	1
Serious	Medium range of an event consequence - serious consequence, injury—occupational accident (e.g. from 3 days off work)	2
Very serious	Large range of an event consequence—very serious consequence, death or mass injury	3

Table 3. Description of the consequence *C* or the severity of the hazard situation: *C*.

Probability	Consequence		
	Negligible	**Serious**	**Very serious**
Low	1	2	3
Medium	2	4	6
High	3	6	9

Table 4. Risk matrix 3 × 3.

parameters determines the type of matrix, for example, 3 × 3, 4 × 5, 6 × 4, etc. Determining the number of levels depends on the depth, to which the risk assessor intends to specify the probability and consequence of a negative effect.

As can be seen from **Table 4**, the estimated risk sizes range from 1 to 9. In the next step, the risk (risk evaluation) needs to be evaluated, so for the assessor which level is high, medium, and low in severity level (e.g. acceptability) of the risk.

Values: 1–2 can be assigned to a low level, meaning small or low risk: L; from 3 to 4: medium level: M; from 6 to 9: high level: H.

For a better illustration, the Risk matrix can be adjusted more clearly, where the principle of so-called "traffic light" effect is applied, **Table 5** [1, 9, 11].

There is no binding rule to determine the level of a risk (e.g. H: high risk, M: medium risk, L: small or low risk), whether in qualitative, quantitative or semi-quantitative form. The applied methodology depends on the area of investigation (e.g. machine failure and its consequences) and data availability (e.g. monitoring machine failures) [6, 11].

Probability	Consequence		
	Negligible 1	**Serious 2**	**Very serious 3**
Low 1	L(1)	L(2)	M(3)
Medium 2	L(2)	M(4)	**H(6)**
High 3	M(3)	**H(6)**	**H(9)**

Table 5. Risk matrix 3 × 3 "traffic light".

http://dx.doi.org/10.5772/intechopen.71152

Important at this stage of the risk assessment is to ensure sufficient information, e.g. historical data about machine failures, near-misses, injuries, accidents, as well as opinions of the experts and practitioners in the investigated area or system.

Risk analysis can be done principally in two ways, applied in specific methods [1, 11]:

a. **Up-bottom approach** (deductive methods)—lead off from information based on statistics of accidents and other undesirable events, analysis of their causes and consequences. So it is based on the events that have already occurred.
b. **Bottom-up approach** (inductive methods)—proceeds from the examination of all hazards and consideration of ways in which damage can occur, meaning: from predicting the probabilities and consequences of a possible undesirable event.

The choice of these methods depends on the experience and knowledge of the team that deals with the assessment process. The inductive methods may have the advantage over deductive methods in a more advanced analysis of all possible hazards and hazard situations but on the other hand they may be more time consuming.

4.2.5. Step 5: risk reducing measures

Reducing the risk to the residual level is conditional on machines by following the **three-step method**—constructional measures excluding or limiting the risks; by installing the necessary protective systems and additional protective measure for those risks that could not be reduced or eliminated in the first step; by providing information on residual risks to the machine user (by providing the instructions for use) [1, 9, 11].

1. Step: **Custom Construction Safety**—this phase of the risk reduction is the most important. Even the most reliable protective systems and additional protective measures can fail during the life cycle of the machine.
2. Step: **Safety protection and additional protection measures**. Protective covers and protective devices must be used when their own construction safety has not adequately eliminated hazard and so does not sufficiently reduce the risk. In this case, another additional protective measure may be applied. Typical examples of protective measures include locking covers, light curtains, safety mats, two-hand control and activation switches. Additional protective measures are the devices which perform emergency stops, escape routes, equipment for manual start of certain parts during emergency stops, communication devices to make emergency calls, disconnection from the power source, handling devices (load lifting), and so on.
3. Step: **User manual**—information on safe use of the machine must be provided in the required quality, understandable language and to the extent that all information on the machine uses and its operating modes. They must inform and warn about the residual risk.

Residual risk—is a risk that remained after the adoption of the implemented measures (protective measures) so it can be manageable. It can describe protective or safety measures taken at the design stage or other additional measures taken by the user of the device, at the stage of its operation [1].

5. Process safety

Machine safety under the Machinery Directive requires an integrated approach to the safety. However, the machine is a complex construction that is not only mechanical or electrical, but often times it is a complex control unit whose reliable function affects not only machine safety but also the whole process [6, 12, 14]. For this reason, safety integration is understood as a requirement not only for the safety of the machine itself, but also for the safety of the whole process (IEC 61511). Standard IEC 61511 defines requirements for safety control systems of continuous technological processes and on the other hand IEC 61508 defines functional safety requirements for electrical/electronic/programmable electronic safety systems (**Figure 5**) [1, 5, 10].

The objective of ISO 13849-1 (Type B-1) is to provide guidance on the design and construction of control (safety) systems so the requirement of integrated security is ensured.

A designer—constructor while reducing a risk considers applying safety measures that contain one or more safety features. The parts of machine control systems that provide a safety function are called safety-related parts of the control system and labeled as SRP/CP SRP—Safety related parts; CP—control system). They may consist of hardware and software, but may not be part of the machine's control system.

5.1. Safety control systems

Safety control systems are designed to perform a safety function. It's the part of the control system (or the control system itself) that prevents the hazards. It could be said that it creates a barrier between hazards and hazards situation (e.g. shields). For these reasons, the safety system must work reliably, under all foreseeable circumstances.

The safety function is implemented by the machine components of the machine control system in such a way so it maintains the device (or bring it into a state) in a safe state with respect to the specific risk circumstances.

According to ISO 13849-1 standard, this is the function of a machine, whose failure can lead to an immediate increase of a risk.

The main task of the designer of the safety system is to avoid hazardous conditions and to prevent the possibility of an unintentional machine start.

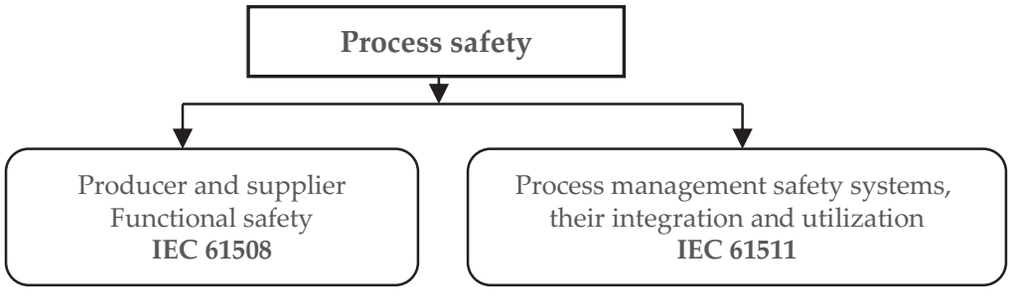

Figure 5. Relation between IEC 61508 and IEC 61511.

http://dx.doi.org/10.5772/intechopen.71152

The safety feature may have several parts, e.g. for a protective cover it is possible to define it in three steps:

- When the cover is closed, the risks (for which the cover has been constructed) can not endanger the person,
- By opening the cover, the exposure to an operational risk must be excluded,
- Closing the cover does not restore the risk.

For safety systems, the use of "safety requirement or after safety requirement" are used as a result of their mode. An example of the requirement for the safety function is the interruption of the light curtain, the opening of the cover, where the operator may require to stop the machine parts or leave them without power if they had already been stopped after the safety function triggered [1, 5, 10].

The safety function is performed by the machine control system safety parts (elements). The safety function begins by sending a command and ends with a response (by doing an activity).

The safety system must be designed with a level of integrity that corresponds to the machine's risk level. Higher risks require a higher level of integrity so the safety performance is ensured. The machine safety system can be partitioned to the performance level of the capability to ensure the performance of the safety function or otherwise, the functional level of safety integrity.

5.2. Functional safety of control systems

Functional safety—it is a part of the overall safety that depends on the correct functioning of the systems or devices in responding to their inputs (stimulus) [1, 10, 15].

Functional safety is the identification of potential hazards based on the activation of protective or corrective devices or mechanisms to prevent a dangerous event or to reduce the level of its consequence.

According to IEC 61508 standard, an example of functional safety is, for example, an overheat protection device that uses a thermal sensor in the motor winding to disconnect the voltage before it is overheated and subsequently could occur a destruction. But, e.g. a special insulation, resistant to high temperatures, is not an example of functional safety, even though it provides protection against the same hazards as a thermal sensor. Similarly, the fixed door as an intrusion barrier does not have a characteristics of the functional safety feature, like on the other hand, door locked housing.

In order to achieve the functional safety, it is necessary to meet the requirements for:

- Safety function,
- Safety integrity.

Risk assessment is the basis for creating the functional safety requirements: risk analysis provides the basis for the safety function requirements and risk evaluation forms the basis for specifying the safety integrity, i.e. the levels of system properties!

5.3. Standards for the functional safety of control systems

The basic standards for the functional safety of the machine control systems are [1, 5, 10, 15]:

a. IEC/EN 61508: Functional Safety of Electrical, Electronic/Programmable Electronic Safety Systems (Part 1, 2 and 3). This standard is general, not limited to the field of a machinery and contains requirements that apply to the design of complex electronic and programmable control systems.

b. IEC/EN 62061: Machine Safety—Functional Safety of Safety-Related Electrical/Electronic/Programmable electronic control systems that are connected with the safety. This is, in fact, a specific implementation of the IEC/EN 61508 standard for the machinery. The requirements of this standard can be applied to system level design for all types of electrical control systems as well as to not very complex subsystems and devices.

c. EN ISO 13849-1: Machine Safety—Safety Parts of Control Systems. This standard provides requirements and guidance for designing, constructing and integrating safety parts of the safety control systems (safety-related parts), including the software design. For these components, there are specific characteristics that include the power level required to ensure the safety function.

d. IEC 61511: Functional Safety. Safety Control Systems of Continuous Technological Processes. This standard was developed in accordance with the introduction of IEC/EN 61508 for industrial processes.

The application of standards has its own possibilities and limitations, e.g. IEC/EN 62061 and EN ISO 13849-1 standards, which deal with an electrical safety management systems (later on they should be unified), they use different methods to achieve their results, and the user can choose them as they are both harmonized under the EU Machinery Directive. The difference between them is in a use in different technologies. IEC/EN 62061 standard is restricted to electrical systems only, while the second ISO 13849-1 standard deals with pneumatic, hydraulic, mechanical and electrical systems.

5.4. SIL and IEC/EN 62061

This standard describes an extent of the risk, which needs to be reduced but also the capability of the control system to reduce this risk with the Safety Integrity Level (SIL) [5, 15]. In the field of machinery, there are three levels from SIL1 to SIL3 (highest level of integrity) are used.

Since the risks may also occur in a different industry, such as the petrochemical, energetic or a rail sector, e.g. in the manufacturing industry (applies specific standard IEC 61511), this standard also offers another category of the safety integrity level, SIL4.

The SIL category refers to the safety function. The subsystems or elements of the system, into which the safety function is implemented, must have the appropriate capability to be assigned to a particular SIL category. This capability is called SIL Claim Limit.

PL	PFD_{avg} (average probability of a dangerous failure per hour)	SIL (safety integrity level)
a	$\geq 10^{-5}$ to $<10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
c	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	2
d	$\geq 10^{-7}$ to $<10^{-6}$	3
e	$\geq 10^{-8}$ to $<10^{-7}$	4

Table 6. Relation between SIL and PL.

5.5. PL and EN ISO 13849-1

This standard does not use SIL, instead of that; it uses Performance Level (PL), properties level or performance. It defines five levels, where PLa is the lowest and PLe is the highest (**Table 6**) [1, 5, 15].

Application of adequate methods of determining SIL requirements depend on organization's risk criteria.

Some standards offer similar methods, e.g. EN 61508 offers three methods: quantitative, risk graph, risk matrix and IEC 61511 offers more as semi-quantitative methods, Safety layer matrix and Layer protection analysis (LOPA) [5, 10].

6. Risk management

The risk is an occurrence of a random event that can happen with a certain probability, when it occurs, it may have a negative impact on the organization's business objectives.

In the process of a risk management, it is necessary to accept three principles [1, 3]:

1. The outcome of the assessment is uncertain. If it is certain, it is not possible to talk about the risk.
2. It is possible to assign at least one of the types of estimated negative consequences (high loss of property, death, environmental damage, financial loss, etc.).
3. Assessment depends on time and changing circumstances, that's why it must be systematic and repeated.

These three principles are often ignored in practice. The manager in the company expects the results of the risk assessment to produce a clear result: "what is wrong and how to fix it" or "I did everything I could and we have no risks at all."

Risk management, particularly in terms of social acceptability, is expressed through the ALARP principle (As Low As Reasonable Practicable). Its priority is to reduce the level of a risk "to such an extent as is reasonably practical," while working with the level of risk between an unacceptable and fully acceptable (tolerable) level.

Acceptable Risk: represents a risk that is reduced to a level that can be tolerated in an organization, but at least it must respect provided requirements of binding regulations and the organization's own policy [1, 3, 11].

ALARP was defined by health and safety executive (HSE) organization in Great Britain. The goal is to manage the residual risk to the extent that it is practical (bearable) for the organization. In Great Britain and New Zealand, this model is also described as SFAIRP (So Far As It Is Reasonably Practicable) in the USA by ALARA (As Low As Reasonably Achievable) [1, 12].

When implementing the ISO 31000 standard for considering the so-called "positive risk" — an assessment of opportunities, it would be possible to apply a new approach for assessing an effectiveness, that is AHARP (As High As Reasonably Practicable) [1, 12].

The OHS management system is part of the organization's overall management system that creates and implements the OHS concept and manages health and safety risks. So it represents a set of mutually beneficial elements to make a policy and achieve the set goals.

The OHSAS 18001 standard required the most time to obtain the "standard" status. Since the safety requirements were different in each country and are strongly supported by the country's legislation, the transition to standard was relatively slow.

After accepting the British BS 8800 standard, the ISO organization had issued for the first time the OHSAS 18001 standard in 1999, which was first revised in 2007. In 2017, transition to the HLS structure (High Level Structure) is expected, as well as the standard also gets a new definition by ISO 45001 standard [1, 3].

To understand connection between Machinery Safety and OHS management is important for organization maturity and its competitiveness. Management system requirements are coming from context description of organization operating (external and internal relationships). This context is a base for risk assessment process coming from organizational business activities and is defined as Risk-based Thinking principles (RBT) [1, 4]. Newly prepared standard ISO 45001:2017 requires proactively approach in Risk Management processes. RBT distinguishes term risk and term opportunities, and also is linked with principles of ISO 31000. This brings a natural pressure for assuming methods and tools for risk assessment in relation with organization objectives on all management level.

Acknowledgements

This work was developed within the projects APVV-15-0351 "Development and Application of a Risk Management Model in the Setting of Technological Systems in Compliance with Industry 4.0 Strategy" and 7FP entitled "iNTegRisk," no. CP-IP213345-2 and co-financed by APVV based contract No. DO7RP-0019-08.

Author details

Hana Pacaiova

Address all correspondence to: hana.pacaiova@tuke.sk

Safety and Quality Production Department, Faculty of Mechanical Engineering, Technical University of Kosice, Slovakia

References

[1] Pačaiová H, Markulik Š, Nagyová A. The Importance of Risk in Management Systems. Kosice: Beki Design; 2016. 276 p ISBN 978-80-553-2618-4

[2] Ferjencik M, Slovackova I. Trust managers and respect workmen: What does it mean to be competent in caring about safety? Journal of Loss Prevention in the Process Industries, Elsevier; pp. 95-104. DOI: 10.1016/j.jlp.2014.08.001

[3] ISO 31000: Enterprise Risk Management: CERM Academy Series on Enterprise Risk Management. USA. 235 p. Greg Hutchins PE CERM; ISBN 9780965466578

[4] Pacaiova H, Sinay J, Nagyova A. Development of GRAM – A risk measurement tool using risk based thinking principles. Elsevier: Measurement; pp. 288-292. DOI: 10.1016/j.measurement.2017.01.004

[5] Blecha P, Blecha R, Bradáč F. Integration of Risk Management into the Machinery Design Process. Mechatronics Recent Technological and Scientific Advances. Springer-Verlag Berlin Heidelberg. 9th International Conference Mechatronics 2011; Varšava; 2011; pp. 473-482

[6] Krajček K, Nikolić D, Domitrović A. Aircraft performance monitoring from flight data. Tehnicki Vjesnik; pp. 1337-1340. DOI: 10.17559/TV-20131220145918

[7] Starr A, Al-Najjar B, Holmberg K, Jantunen E, Bellew J, Albarbar, A. Maintenance today and future trends. In: E-Maintenance. London: Springer-Verlag London; 2010. pp. 5-10. DOI: 10.1007/978-1-84996-205-6_2

[8] Balazikova M, Tomaskova M, Dulebova M. Study of non-auditory effects of noise MM Science Journal; pp. 912-913. DOI: 10.17973/MMSJ.2016_06_201609

[9] Baybutt P. Calibration of risk matrices for process safety. Journal of Loss Prevention in the Process Industries. Elsevier; pp. 164-166. DOI: 10.1016/j.jlp.2015.09.010

[10] Gulland W.G. Methods of determining safety integrity level (SIL) requirements—pros and cons. In: Redmill F, Anderson T, editors. Practical Elements of Safety. Springer, London. p. 105-122. DOI: 10.1007/978-0-85729-408-1_6

[11] Haimes Y Y, Sage P A. Risk modelling, assessment and management, 4nd ed. Hobocen: Wiley; pp. 56-117. ISBN: 978-1-119-01798-1

[12] Tablot J. ALARP (As Low As Reasonably Practicable). Available from: http://www.jakeman.com.au/media/alarp-as-low-as-reasonably-practicable [Accessed: 24-09-2016]

[13] Pacaiova H. Human reliability in maintenance task. Frontiers of Mechanical Engineering in China; pp. 184-187. DOI: 10.1007/s11465-010-0002-4

[14] Maletic D, Maletic M, Al-Najjar B, Gomiscek B. The role of maintenance in improving company's competitiveness and profitability: a case study in a textile company. Journal of Manufacturing Technology Management; pp. 441-452. DOI: 10.1108/JMTM-04-2013-0033

[15] Kingsley J. Safety Integrity Level (SIL)—Explained Simply. 2017. Available from: https://www.linkedin.com/pulse/safety-integrity-level-sil-explained-simply-john-kingsley [Accessed: 20-07-2017]