Technical article

Technology report: Methods for risk assessment

The European Machinery Directive requires that a risk analysis be performed for every machine before being brought to market. The convergence of IT and OT as well as the rapid technological development has made it necessary to revise the Machinery Directive. The result is the new Machinery Regulation: It will replace the Machinery Directive as the legal foundation. It contains additional requirements on the risk analysis. In addition to the general procedure for the risk analysis, various processes for the risk assessment are introduced and their properties explained in the following.

Legal fundamentals

In accordance with EU Machinery Directive 2006/42/EC, a manufacturer of machinery may not bring a machine to market if it poses a danger. For the purpose of written confirmation, he performs a CE conformity assessment that includes the creation of a risk analysis. Machines may only bear a CE mark if the evaluation process was fully completed and the risk analysis shows that the machine is safe.

The Machinery Directive describes the process of the risk analysis in very general terms, even if it lists in an appendix possible dangers that must be taken into account during the analysis. You can find a more exact description of the risk analysis process in standard ISO 12100 - Risk assessment and risk reduction (figure 1). It defines an iterative process in which one first identifies, assesses and evaluates the hazards. If the evaluation shows that unacceptable hazards are present, these must be minimized. The procedure for reducing the hazards is divided into three levels; it is mandatory that the sequence of these levels be followed.

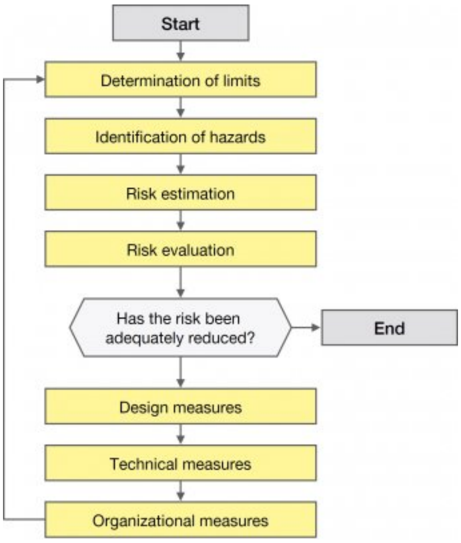


Figure 1: Iterative process for the risk assessment in accordance with standard ISO 12100.

The first level pertains to constructive measures. This means that the machine must be designed so that it is safe. In the event that this is not possible, the manufacturer can employ technical measures. These include, for example, guards, such as fences or electro-sensitive protective devices like safety light curtains. Both ensure that the operator can no longer reach the hazards. If neither technical nor constructive measures are possible, organizing measures may be used. An example of these would be the instruction of the employees.

If the defined measures for risk reduction are implemented, the iterative process starts again. Other hazards that were not fully eliminated by the measures or that were caused by the measures may thereby be identified. The iterative process ends once all hazards have been sufficiently minimized.

The new EU Machinery Regulation EU 2023/1230 replaces the Machinery Directive on January 20, 2027. No provision is made for a transitional regulation. Revision of the Machinery Directive was necessary due to technical advancements. The Machinery Regulation now details requirements on the safety of machines that arise in the areas of:

- Networking of machinery
- Digitization and more complex control technology
- New technologies, such as AI or collaborating robots

In appendix III – Safety requirements for the design and construction of machinery – the Machinery Regulation covers hazards that are not explicitly listed in the Machinery Directive. The following sections describe the main changes to the risk analysis.

With respect to the networking of machines, this is the protection against corruption. The connection of hardware and/or software must not lead to damage. In addition, unauthorized access to the machine and the possibility of tampering with data must be prevented. The failure or restoration of a communication connection must likewise not result in a dangerous situation.

The controls of machines must be protected against external influence so that no intentional or unintentional changes can be made to the software or the configuration. An access log of changes to the hardware and/or software is to be stored for five years. Both the software as well as the configuration must have an identifier (ID).

Furthermore, the Machinery Regulation regulates the topic of artificial intelligence of self-learning systems. Machines must not execute any actions that go beyond their defined task and movement range. Data that lead to decisions that are relevant to safety must be archived for one year. Furthermore, it must be possible at any time to correct the machine to ensure safety. The Machinery Regulation defines additional requirements for autonomous, mobile machines as well. They must, thus, detect obstacles or persons, and, in the event of collisions, batteries must not cause any hazards.

Parameters for the risk assessment
There is not generally any unit of measurement for a risk. The risk is typically described as low/high by means of a risk indicator or a failure probability. A textual description of the risk is often easier to understand than the definition with risk indicators. If the actual risk is to be estimated using a risk indicator, its value range must be known.

The Machinery Directive defines that to determine the risk of an observed danger, two parameters must be taken into account: the extent of damage and the probability of an injury (figure 2).

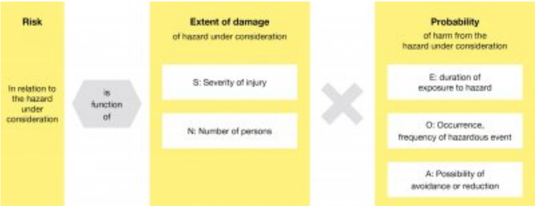

Risk
In relation to the hazard under consideration
is function of
Extent of damage
of hazard under consideration
S: Severity of injury
N: Number of persons
Probability
of harm from the hazard under consideration
E: duration of exposure to hazard
O: Occurence, frequency of hazardous event
A: Possibility of avoidance or reduction

Figure 2: Parameters for the risk assessment.

These two parameters can – depending on the process used for the risk assessment – be divided into further parameters. Some processes divide the extent of damage into:

- Severity of the injury (S, Severity)
- Number of injured persons (N, Number).

In automation technology, only one person is usually affected by an event; thus, parameter N has no meaning there. In process technology, where many persons could be injured by an event, parameter N is important for assessing the risk.

To more precisely define the probability of an injury, this is often divided into subparameters:

- Duration of the exposure to a danger (E, Exposure)
- Frequency of the dangerous event (O, Occurrence)Possibility for avoiding the dangerous event (A, Avoidance)

Not every dangerous event automatically results in harm. Harm only occurs if a person is present in the endangered area at the same time as the dangerous event and is unable to avoid the danger. In practice, one minimizes either the duration, E, of the hazard with a hard guard or the frequency, O, of the hazard, by means of a machine stop with safe sensors in order to obtain a safe system.

In summary, the risk can be represented as follows: **S=f(S,N)* f(E,O,A)**

Process for risk assessment
The objectives of the risk assessment are the quantification of the risk using the parameters specified above and the representation of the risk by means of a risk indicator as numerical value. There are no normative specifications for assessing the risk. Some standards do, however, specify a process in the informative appendix. Furthermore, processes may originate from technical reports from standards organizations or other publications. The choice of process is left to the machine manufacturer. In general, the risk assessment should be performed by a team of people to ensure that the evaluation is as objective as possible.

The processes for the risk analysis can be divided into three classes:

- Graphical processes
- Tabular processes
- Numerical processes

Graphical processes determine the risk through a graph. Each node usually only has two branches, which represent different parameter values. The options are described in text form here. Due to the limited number of options, the risk is usually only classified roughly, but simply and easy-to-understand.

Presented as an example of a graphical process is the risk graph acc. to standard ISO/TR 14121-2 - Practical guidance and examples of methods (figure 3). It is often used to depict the effectiveness of risk-reducing measures and has the four parameters S, E, O, A. The resulting risk index has a numerical value between 1 and 6. The values 1 and 2 represent a state of low danger. The example also shows that graphs with more than two branches per node become confusing.

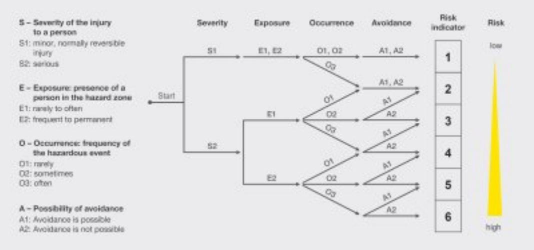
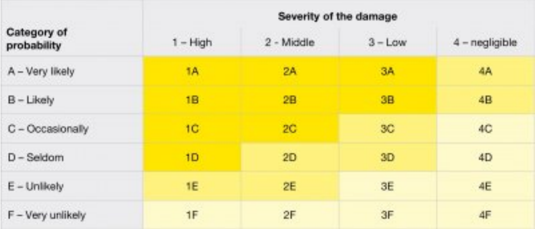

S – Severity of the injury to a person
S1: minor, normally reversible injury
S2: serious
E – Exposure: presence of a person in the hazard zone
E1: rarely to often
E2: frequent to permanent
O – Occurrence: frequency of the hazardous event
O1: rarely
O2: sometimes
O3: often
A – Possibility of avoidance
A1: Avoidance is possible
A2: Avoidance is not possible
Start
Severity
Exposure
Occurrence
Avoidance
Risk indicator
Risk
S1
S2
E1, E2
E1
E2
O1, O2
O1
O2
O3
A1, A2
A1
A2
1
2
3
4
5
6
low
high

Figure 3: Risk graph in accordance with ISO/TR 14121-2.

Tabular processes usually have more than two values per parameter; the values are described in text form. There are more options than with graphical processes. The classification is still relatively rough, as the number of parameters is limited in order to preserve clarity.

A simple example for a tabular process is described in standard ISO 14798 - Lifts (elevators), escalators and moving walks (figure 4). It has only the two parameter 'severity of the harm' and 'probability of a hazard'. This makes the process easy to follow; like the graphical process, the classification is, however, only rough. The resulting risk index is described by a number and a letter that indicate a low, medium or high hazard.



Category of probability	Severity of the damage			
	1 – High	2 - Middle	3 – Low	4 – negligible
A – Very likely	1A	2A	3A	4A
B – Likely	1B	2B	3B	4B
C – Occasionally	1C	2C	3C	4C
D – Seldom	1D	2D	3D	4D
E – Unlikely	1E	2E	3E	4E
F – Very unlikely	1F	2F	3F	4F

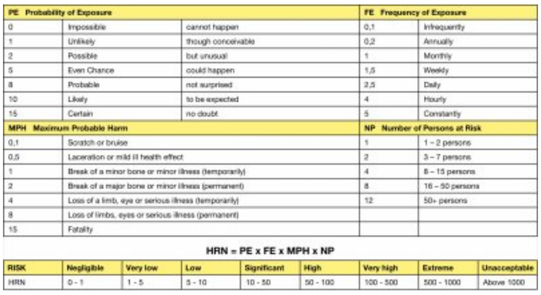
Figure 4: Risk table from ISO 14798.

Numerical processes determine a risk indicator through addition or multiplication of the parameter values. As a result, many parameters with many different values are possible and the risk is determined in greater detail. This can give a false impression of accuracy, as the parameter values are always determined subjectively and depend on the capabilities of the user. Nevertheless, the greater level of detail helps in comparing the hazard of different risks with one another. Due to the many parameters and options, numerical processes are not as simple and easy to understand as graphical or tabular processes.

Due to the high level of detail, it is possible to compare the risk of various hazards with one another and to identify the hazard with the greatest risk. This can be important for prioritizing the steps for overhauling a machine.

An example of a numerical process is HRN, Hazard Rating Numbers (figure 5). It was published in 1990 by Chris Steel and exists in several variants. The text description of the numerous parameter values does, however, make it more difficult to select the correct value. The original form has the four parameters S, N, E, O. Parameter A for the possibility of avoidance was omitted. The resulting risk is determined through multiplication:

R=S*N*E*O



PE	Probability of Exposure		FE	Frequency of Exposure
0	Impossible	cannot happen	0,1	Infrequently
1	Unlikely	though conceivable	0,2	Annually
2	Possible	but unusual	1	Monthly
5	Even Chance	could happen	1,5	Weekly
8	Probable	not surprised	2,5	Daily
10	Likely	to be expected	4	Hourly
15	Certain	no doubt	5	Constantly
MPH	**Maximum Probable Harm**		**NP**	**Number of Persons at Risk**
0,1	Scratch or bruise		1	1 – 2 persons
0,5	Laceration or mild ill health effect		2	3 – 7 persons
1	Break of a minor bone or minor illness (temporarily)		4	8 – 15 persons
2	Break of a major bone or minor illness (permanent)		8	16 – 50 persons
4	Loss of a limb, eye or serious illness (temporarily)		12	50+ persons
8	Loss of limbs, eyes or serious illness (permanent)			
15	Fatality			

HRN = PE x FE x MPH x NP

RISK	Negligible	Very low	Low	Significant	High	Very high	Extreme	Unacceptable
HRN	0 - 1	1 - 5	5 - 10	10 - 50	50 - 100	100 - 500	500 - 1000	Above 1000

Figure 5: Numerical process in accordance with HRN.

Through multiplication, it can suffice if one parameter is very small or becomes very small through risk reduction.

Risk reduction through technical measures

If the risk evaluation yields too high a risk, it must be reduced through appropriate measures. The sequence of the measures is defined. Technical measures can be realized only if constructive measures are not possible.

Technical measures are often realized with safe controls that are part of a safety function. A safety function consists of safe components, i.e., safe sensors, a safe control and safe actuators. The components must satisfy a certain reliability, which defines the probability of a dangerous failure of the component. The greater the risk that it safeguards, the greater the reliability needs to be: In the event of a failure of the components, protection against the hazard is no longer present. The reliability of the component is also referred to as the safety level. In order to determine this value, a risk assessment must therefore be performed. In this case, the result is not a risk value that defines the risk but rather a minimum necessary safety level of the components of the safety function.

Standards for safety-related control systems define their own process for risk assessment with which the required safety level can be determined.

In automation technology, standard ISO 13849-1 - Safety-related parts of control systems - is usually used to define the safety system of a machine. It can be used for electronic, mechanical, hydraulic and pneumatic systems. Appendix A describes a risk graph for determining the necessary performance level PLr of the safety function (figure 6). The risk graph contains three parameters: the extent of damage (S), the duration of the presence of persons in the dangerous area (E) and the possibility of avoidance (A). As with other graphical processes, it is simple and easy to understand and works with a rough classification. If users select the higher value due to uncertainty, the resulting requirements are too high and the safety technology becomes unnecessarily expensive.

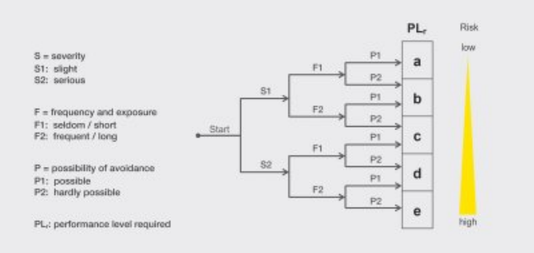
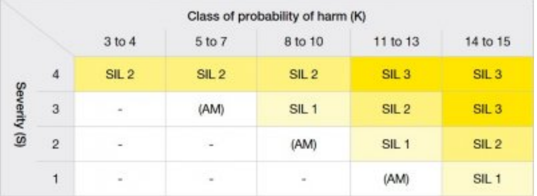


Figure 6: Risk graph in accordance with ISO 13849-1.

An alternative for electrical and electronic control systems is standard IEC 62061- Functional safety of safety-related control systems. Appendix A describes a combination of tabular and numerical processes for determining the necessary safety level SILCL of the safety function (figure 7). The process is more complex than the risk graph of 13849-1. A detailed classification is, however, possible, as more different values are available for selection for the four parameters.



		Class of probability of harm (K)				
		3 to 4	5 to 7	8 to 10	11 to 13	14 to 15
Severity (S)	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
	3	-	(AM)	SIL 1	SIL 2	SIL 3
	2	-	-	(AM)	SIL 1	SIL 2
	1	-	-	-	(AM)	SIL 1

Figure 7: Risk assessment in accordance with IEC 62061.

Risk estimation in accordance with HARMONY

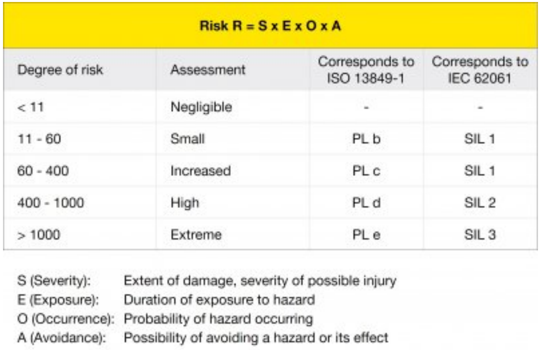
The described processes guide the user through the risk assessment two times with different processes and different objectives: first with process 1 for assessing the initial and final risk of a hazard and then with process 2 for determining the safety level of the safety function.

This procedure appears unnecessarily complex and burdensome. A considerable simplification is possible if the process for the risk assessment defines not only the risk indicator but also automatically defines a safety level for technical measures.

For this reason, Leuze satisfied this requirement in its HARMONY process. The term HARMONY is the abbreviated form of HAzard Rating for Machinery and prOcess iNdustrY. The process is used in automation technology and process technology.

HARMONY is an adaptation of the HRN numerical process and determines a risk indicator by multiplying the extent of damage (S), duration of the hazard (E), frequency the dangerous event (O) and the possibility of avoidance (A):
R=S*E*O*A

The value ranges of the risk indicator R are defined so that they can be assigned a performance level PLr in accordance with ISO 13849-1 or a Safety Integrity Level SILCL in accordance with IEC 62061. Figure 8 shows this assignment.



Risk R = S x E x O x A

Degree of risk	Assessment	Corresponds to ISO 13849-1	Corresponds to IEC 62061
< 11	Negligible	-	-
11 - 60	Small	PL b	SIL 1
60 - 400	Increased	PL c	SIL 1
400 - 1000	High	PL d	SIL 2
> 1000	Extreme	PL e	SIL 3

S (Severity):	Extent of damage, severity of possible injury
E (Exposure):	Duration of exposure to hazard
O (Occurrence):	Probability of hazard occurring
A (Avoidance):	Possibility of avoiding a hazard or its effect

Figure 8: Risk assessment in accordance with HARMONY.

Summary
In accordance with the Machinery Directive and the Machinery Regulation that is replacing it, a risk analysis must be carried out for every machine before being brought to market as it must not pose a danger at any point in time.

During the risk analysis, a systematic and careful procedure is important in order to identify all hazards. Only if the hazard has been identified can an appropriate measure for risk reduction be undertaken. This is complex and time-intensive. Various processes are available for risk assessment; there are, however, no normative requirements. Every organization must find the appropriate procedure itself. Criteria for the selection can include the complexity of the task or the specialist knowledge or preferences of the employees. The HARMONY process defined by Leuze helps to simplify the process for the risk assessment and to reduce the amount of work.

Author:

Rolf Brunner
Senior Safety Expert at Leuze

With curiosity and determination, the Sensor People from Leuze have been creating innovations and technological milestones in industrial automation for 60 years. They are driven by the success of their customers. Yesterday. Today. Tomorrow. The technology leader's high-tech product range includes a number of different sensors for the field of automation technology. Among these are switching and measuring sensors, identification systems, and data transmission and image processing solutions. As a Safety Expert, Leuze is also focused on components, services and solutions for safety at work. Leuze concentrates on its core industries, in which the Sensor People have extensive, specific application know-how and many years of experience. These include intralogistics and the packaging industry, machine tools, the automotive industry as well as laboratory automation. Leuze was founded in 1963, headquartered in Owen/Teck in Southern Germany. Today there are more than 1400 Sensor People around the world who are working with determination and passion for progress and transformation to make their customers successful in a constantly changing industry. Regardless of whether in the technological competence centers or in one of the 21 sales companies, supported by more than 40 international distributors.

Leuze electronic, Inc
2150 Northmont Parkway Suite N
Duluth, GA 30096
Jennifer Mass
Phone: +1 (248) 752-6712
Jennifer.Mass@leuze.com

Leuze France SARL
ZI Nord de Torcy - Rue des Tanneurs
BP62 – Bâtiment 3
77202 Marne la Vallée CEDEX1
France
Solveiga Suopyte
Phone: +33 (1) 60 05 12 20
Fax: +33 (1) 60 05 03 65
Solveiga.Suopyte@leuze.com