AXELENT SAFETY™

Risk Assessment in Mechanical Engineering

- efficient
- target-oriented
- conforming to standards

Matthias Schulz

Matthias Schulz

Risk Assessment in Mechanical Engineering
- efficient
- target-oriented
- conforming to standards

(V 1.6, 06-2024)

Matthias Schulz
Manningaweg 3
D-26553 Lütetsburg (GERMANY)
Telephone: +49 73 66/9 17 09 02 (IP)
www.hiq-text.de
E-Mail: www.hiq-text.de

Sponsored by:

pgx software solutions gmbh
Ferdinand-Porsche-Str. 32
D-75382 Althengstett (GERMANY)
Telephone: +49 70 51 9 66 82-0
Fax: +49 70 51 9 66 82-29
www.pgx.de
E-Mail: info@pgx.de

Axelent GmbH
Business Devision Axelent ProfiServices
Tränkestrasse 11
D-70597 Stuttgart (GERMANY)
Telephone: +49 7 11 25 25 09-0
Fax: +49 7 11 25 25 09-49
www.axelent.de
E-Mail: profiservices@axelent.de

HiQ text GmbH
Manningaweg 3
D-26524 Lütetsburg (GERMANY)
Telephone: +49 73 66/9 17 09 00
www.hiq-text.eu
E-Mail: info@hiq-text.de

Table of Contents

1 Introduction

"Risk assessment" – mention of the word is enough to cause an allergic shock or a bad conscience in developers and machinery designers. Even more than 25 years after the introduction of CE marking for machinery numerous manufacturers still have not satisfactorily solved the "problem" risk assessment. Why is that?

The main reason is a lack of easy-to-learn, economical methods that would help remove risk assessment from the realm of "secret arts". This little brochure is meant to present such a method in brief and demonstrate its application.

2 Risk Assessment – Why?

When designing machinery, engineers primarily focus on function, efficiency and economic concerns. Safety rarely is of much concern, especially not at the early stages of a project. However, it may be very difficult to integrate safe operation into the overall functional and operating concept later on. In fact, safety measures added during the final stages of the project often impair accessibility and efficiency of the machinery.

What's in risk assessment?

- Specify functions of the machinery
- Identify hazards caused by the function
- Estimate risk involved (injury and probability occurrence)
- Seek to eliminate or reduce risk

Therefore it is best to think about the hazards generated by a function from the start and to conceive of counteracting measures as early as possible. Three, in some cases four, steps are needed:

1. Eliminate the hazard if at all possible, that is, tackle the problem at its very origin.
2. If you cannot get rid of the hazard or it would be too costly, lock the hazard in (or people out).
3. If you cannot keep people's hands and feet out, monitor the presence of people near the hazard, to stop it in time.
4. Warn the users of residual risks that could not be removed or reduced satisfactorily. This is done by warning signals, signs, and notes in the operating instructions.

This process of identifying hazards, determining their risk potential and then reducing or eliminating such risks is referred to as "risk assessment". (previously also referred to as "hazard analysis"). Until the late 1980s, engineers did not normally follow a methodical approach to safety issues. Only with the introduction of the Machinery Directive in 1995, "risk assessment" has become the most important step toward conformity with EU regulations.

3 Risk Assessment in Five Steps

How should you best go about risk assessment? The Machinery Directive (in Annex I, introduction) specifies five steps to be taken in risk assessment:

1. Determine the limits of the machinery, which include the intended use and any "reasonably foreseeable misuse";
2. Identify the hazards that can be generated by the machinery and the associated hazardous situations
3. Estimate the risks, taking into account the severity of the potential injury or damage to health and the probability of its occurrence
4. Evaluate the risks, with a view to determining whether risk reduction is needed
5. Eliminate the hazards or reduce the risks associated with these hazards by application of protective measures, in the order of priority set out in section 1.1.2(b) of Annex I of the Machinery Directive.

All five steps can be documented using a standard form or a software tool for risk assessment, e.g., the SafetyToolBox by pgx software solutions (download from www.axelent.de or www.pgx.de).

The entire procedure is illustrated on the next pages step by step, using a standard form. You may download the full sample from www.axelent.com. This example has been created using the SafetyToolBox software by pgx.

3.1 Step 1 – Determine Limits

In the first step, the limits of the machinery are defined. Six categories of limits with some guiding questions are provided for:

1. What is the intended use (application and its limits)?
2. In which field is the machinery to be used (private sector/industry)?
3. By whom will the machinery likely be used (professional qualifications of operators, service staff)?
4. Limits regarding space (space required, interfaces to other machinery, human-machine interface)
5. Limits regarding time (durability, pertinent service intervals for safety related parts)
6. Materials used in conjunction with the machinery (lubricants, hazardous fluids and gases)

Risk Assessment	Designation Wastes Shredder	Ty Re
		No 47

1	Limits of the machinery, intended use			
1.1	Intended use	Shredding of wastes, especially of completely empty containers mad		
1.2	Limitations of admissible use, foreseeable misuse	Do not shred: Glass, pressurised vessels (e. g. spraying cans), conta aggressive, or toxic liquids, stones, rubble, massive metal parts, expl completely coiled or bundled into the shredders funnel, shavings of fl		
1.3	Abuse (forbidden use/applications)	Shredding of foodstuffs or animal fodder for further processing (conta Shredding of explosives and ammunition		
2	**Field of application**			
	private, consumer			
	commercial	X		
3	**User groups, endangered persons**			
3.1	Users	Index	Description	Tasks
		3.1.1	Installation personnel	Assembly, installation
		3.1.2	Maintenance staff	Maintenance, small repair
		3.1.3	Operator	Operation (use)
3.2	Other endangered persons	Description		
4	**Space limits**			
4.1	Workplaces	Operator console on the operating and feed side. The console must l access to the emergency stop. Minimum distance to parts of a buildir		

Excerpt from a sample risk assessment. limits of machinery

3.2 Step 2 – Identify Risks

In the second step, many are still mainly using a list of hazards with mechanical, electrical, thermal and other types of hazards. For each hazard on the list some lines of description are added to the risk assessment. While this approach is not entirely wrong, it overlooks many hazard situations as the focus is on searching for situations matching a certain problem type ("Where, when and how can peoplebe injured due to the mechanical hazard crushing?").

It is better to define all relevant situations along a timeline from transport to disposal (the so called "phases of the life"). Then ask: "What are the hazards incurred in that situation?". This approach was first described by Matthias Schulz in his book "Gefahrenanalyse – Warum und wie?" (Hazard Analysis – Why and How?", published in Germany in 1999 (no longer available).

The method is now referred to as "task-based risk assessment" and described in chapter 5.4 of ISO 12100; it is also recommended in the

ISO TR 14121-2. ISO 12100 requires that risk analysis be organised by "phases of life" subdivided by so called "tasks". A "task" is one of the following:

Risk assessment should be organised by phases of life and tasks because
- this is the only way to identify close to all hazardous situations and hazards
- it makes risk assessment a logic, easy-to-learn process
- the method saves a lot of redundant work
- the mothod conforms to current standards

a) an activity of people (operators, service staff, machine fitters …)

b) an automatic process running in the machine (a movement, or a function like pressure build-up…)

c) a combination of a and b

This approach results in straight-forward identification of hazards, because the person(s) performing the risk assessment can focus on a specific situation occurring at a specific place and time. Concerning the defined situation they will simply ask: "What could go wrong, hurting people or causing substantial damage?" An example is shown below.

Risk Assessment

Designation
Wastes Shredder

T
R

N
4

Phase of life		Hazardous event	Measure
Task	Hazard		
4 Operation, operating modes			
4.1 Fill with wastes	Moving parts: crushing, cutting or severing Rotating elements: drawing in or trapping, entanglement	If the operator fills the machine while it is running, he could come in contact with the rotating knife blades and be drawn-in and injured.	Type of measure: guard, mechanical (IIa): Fixed panels on three sides (bolted to the Pendulum-type flap on the filling side with locking, but w/out guard locking, because ued run is not relevant. See Figure 3
			Type of measure: Combination of guards a tective devices (IIc): Monitoring of the position of the pendulum means of a door safety switch. If the flap n from its centre position, this causes immec stop of the shredder and the feeding press

Excerpt from a sample risk assessment. Organised by phase of life and tasks

In this example, the operation of an industrial waste shredder has been assessed. The task is "Fill with wastes", which is done manually. The next three columns show the hazards and their causes, followed by a more detailed description of the hazard situation resulting from the task. As is seen in the example, a task may entail a number of different hazards and associated hazard situations.

3.3 Step 3 – Estimate Risk

Once the hazards have been identified, one can follow through by estimating the risk. Generally risk is the product of two factors:

- the severest direct injury from the situation (e. g. loss of fingers, hand, arm etc.)
- the probability of its occurrence (subdivided into two or three aspects, depending on the method employed)

In most cases it is fully sufficient to estimate only the severity of injury. When the injury incurred can be severe (level S2 to ISO 13849-1 or Se3/Se4 to IEC 62061) designers will inevitably have to seek a solution to eliminate or reduce the risk.

	Type Render to pieces 7	Erstellt mit SAFETYTOOLBOX (www.pgx.de)
	No. 4712-5	

	Measure	Directives/standards	Risk estimation IEC 62061							
			Se	Fr	Pr	Av	C	R	SILcl	SIL
			Arguments							
	Type of measure: guard, mechanical (IIa): Fixed panels on three sides (bolted to the frame). Pendulum-type flap on the filling side with interlocking, but w/out guard locking, because continued run is not relevant. See Figure 3	1.4.2.1 - Fixed guard 1.4.2.2 - Interlocking movable guard EN ISO 12100: 2010: 6.3.2.2 EN ISO 13857: 2019: 4.2.2 and table 2 EN ISO 14120: 2015	Se4	Fr5	Pr2	Av1	8	32	SIL 2	
			Se: Severe irreversible injury, loss of body parts Fr: Frequent loading (several times per hour) Pr: It is unlikely that somebody will deliberately reach into the rotating knifes Av: The hazard is known; the operator starts machine movements by consciously pressing a start button							
	Type of measure: Combination of guards and protective devices (IIc):									

Excerpt from a sample risk assessment. Risk estimation to IEC 62061

In the example shown the risk estimation includes four elements (IEC 62061):

- severity of injury
- frequency and duration of presence in the hazard situation (exposure to the hazard)
- probability of occurrence
- ability to detect the hazard and escape timely from the hazard situation

For a detailed description of risk estimation and the methods used see Section 4 “Risk Estimation – Why and How?”, page 11.

3.4 Step 4 – Evaluate Risk

The fourth step logically follows risk estimation. It answers two questions: Can this risk be tolerated? Or is it necessary to eliminate the hazard or reduce the risk?

Risk evaluation does not mean:
- comparing the risk without safety measures to the risk after implementation of safety measures ("risk comparison")

but includes:
- determining what is state of the art
- deciding on safetymeasures for risk reduction so the state of the art is reached

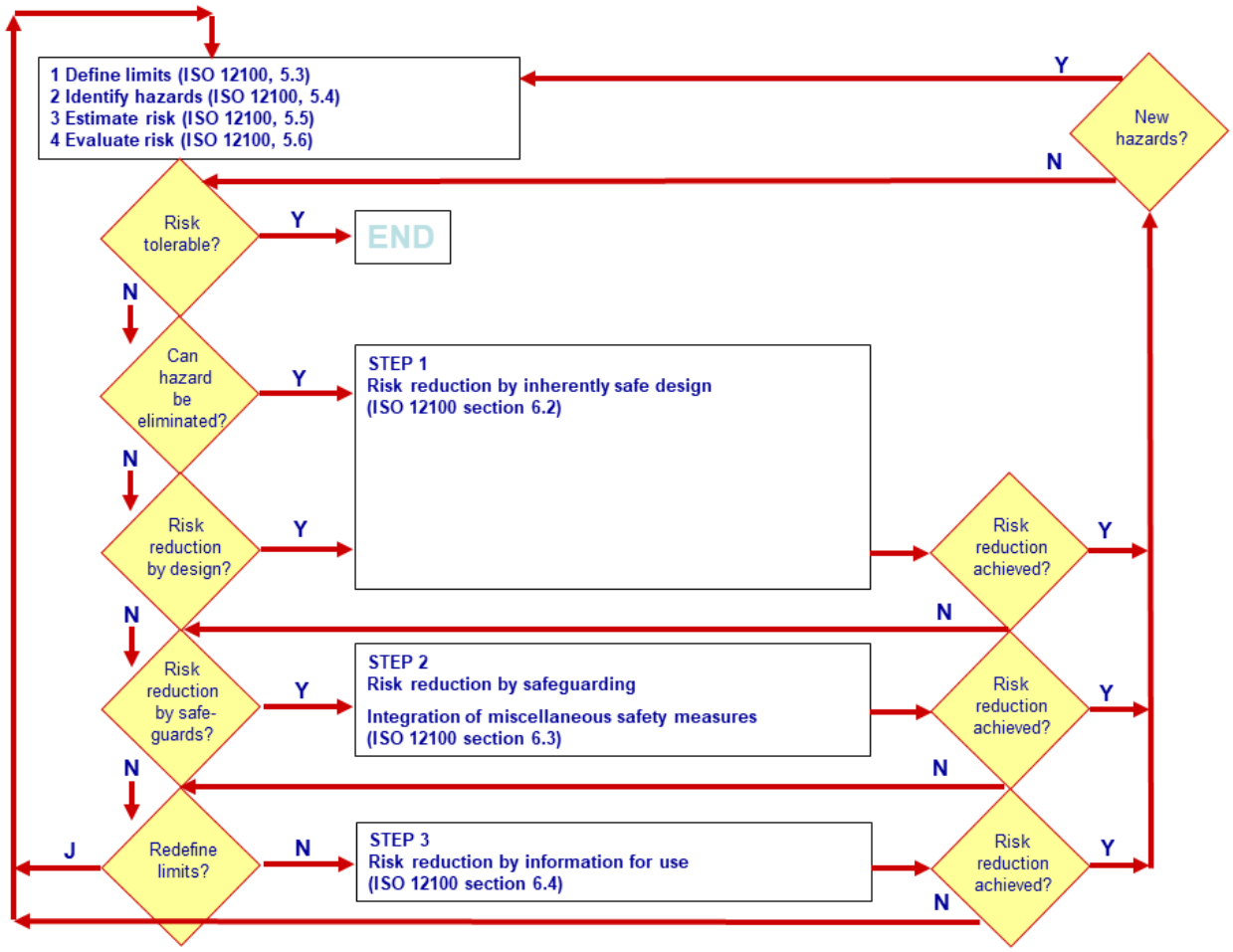
Generally speaking, severe injury always is a reason to attempt risk reduction. However, designers must seek to reduce *every* risk to the level that is allowed by the EU directives and standards. Thus, step 4 involves standards research, which in turn requires use of external tools like databases etc.

Admissible risk levels may vary from product to product. In chain saws, for instance, it is still quite normal that an operator could seriously hurt himself or others, because the revolving chain is largely uncovered. But this would not be accepted in a stationary circular saw, because covering a large part of the saw blade is possible in such machinery. The acceptability of specific risks today is largely determined by EN, EN ISO and EN IEC standards (ISO and IEC standards outside the EU).

3.5 Step 5 – Eliminate Hazard or Reduce Risk

Where risk is considered unacceptable/intolerable, the designer will choose measures to either eliminate the hazard or reduce the risk. That may include reducing the severity of the potential injuries or the probability of their occurrence. The Machinery Directive and international standards dictate taking three steps in finding adequate solutions:

- eliminate the hazard, that is, change the design so the hazard is removed (example deburr sharp edges)
- add guards and safety-related control devices (fencing, covers, safety switches, light curtain …)
- instruct the operators and other target groups regarding residual risks and precautions to be taken (warning on the product and/or in the instructions, e.g., requirement to wear personal protective equipment like a helmet and gloves etc.)



Risk assessment – Overview of the process (adapted from ISO 12100)

4 Risk Estimation – Why and How?

The third step, risk estimation, often takes up a lot of the time spent for risk assessments. The reasons for this are:

- often excessive importance is attributed to risk estimation
- the risk elements are not defined clearly, which leads to time-consuming discussions

Risk estimation may serve three purposes:

1. Facilitating decisions on safety measures. To make such decisions, it is often sufficient to be aware of the severity of potential harm. Injury may be irreversible, such as the loss of a finger or a broken limb or hand; in such cases, risk reduction is always required. The question then only is whether it is feasible.
2. Determining the required reliability of safety-related control system functions (expressed in the form of the required PL or SIL). This is only needed if a control function is used to achieve risk reduction in a given hazard situation. The example discussed in this brochure therefore contains detailed risk estimations only for those risks that will be reduced by a function of the machine's control system.
3. Comparing risks. Generally, the risk without safety measures is compared with the risk after safety measures have been implemented. Many designers are convinced that this is mandatory and

that risk assessment is only complete if they can show that the risk has been reduced in every case. However, there are no indications to this effect in either the Machinery Directive or the applicable standards (ISO 12100, ISO 13849-1 or IEC 62061). However, it is essential to add safety measures that meet the requirements of the Machinery Directive and/or the applicable safety standards. In view of this goal, risk comparisons before/after implementation of measures are completely worthless in most cases. The time spent on such comparisons could often be used more effectively for standards research and exploration of enhanced safety measures and operating concepts. However, if you wish to do before/after risk estimations, be sure to employ a method that uses sufficiently graduated criteria, such as the method presented in Annex A of IEC 62061 or in Annex F of the US standard ANSI B11.0 (2023).

The decision for a specific method should depend on the objective of risk estimation.

Different risk estimation methods may be used. The three most well-known are:

- ISO 13849-1 Annex A – three risk elements (probability of occurrence is part of the element "Possibility of avoiding or limiting harm")
- IEC 62061 Annex A - four risk elements
- ISO TR 14121-2 section 6.3.2 – four risk elements

4.1 Risk Estimation to ISO 13849-1

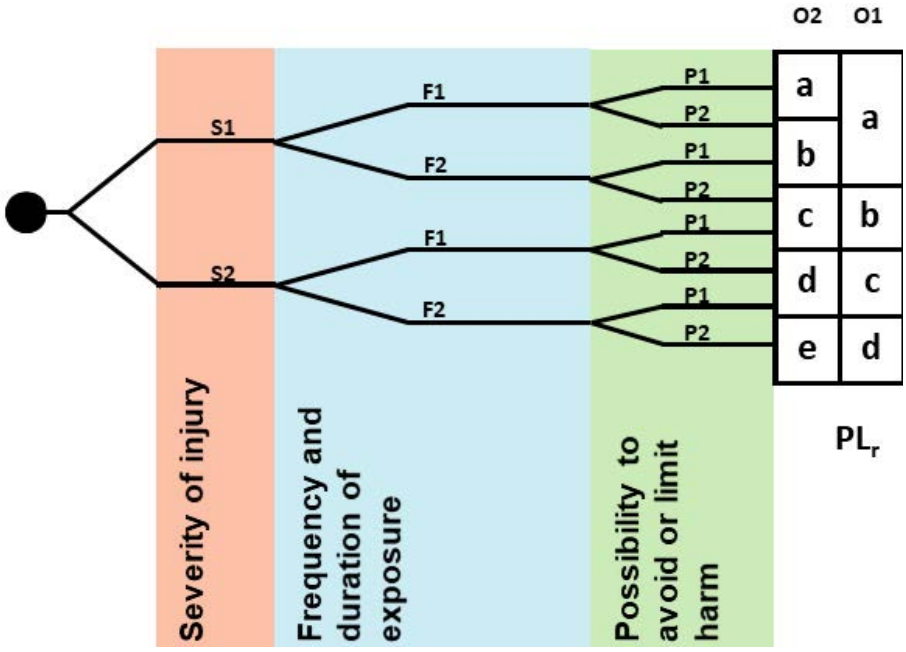
This is the most well-known but also the most problematic method. Since it has three risk elements only and a very coarse demarcation of the criteria, its results are unidimensional at best. According to the 2023 version, the probability of occurrence can also be estimated. However, there is no separate parameter for this in the standard. In this guide, the risk element "O" for "occurrence" = probability of occurrence is used for clarification. The PL_r may be reduced by one level, if the probability of occurrence can be estimated as low. The method is just good enough for its purpose: to determine the required performance level (PL_r) for safety functions. It is not suitable for risk comparisons.

However, ISO 13849-1 carries the so called "assumption of conformity" under the EC Machinery Directive and many think it must be preferred, therefore. However, that is no pertinent reason to decide for this method; IEC 62061 also has the assumption of conformity and its risk estimation method is thus at least equivalent.

The graph on the following page shows how the risk elements are used. Unfortunately, the definition of the criteria is very general, making it difficult to determine the limits. The table "PL/SIL" lists the interpretations of the respective results. The risk may be low to very high, and the required performance level (PL_r) ranges between a and e. It defines the required degree of reliability of a control function used to reduce a risk.

Additionally, the table shows which signal word to ISO 3864-2 should be selected for warning signs on the machine and for warning messages in the operating instructions. The three signal words Danger, Warning, and Caution represent three different risk levels.

Risk Graph



Risk graphic according to ISO 13849-1, supplemented by the parameter O = probability of occurrence

Risk Elements and Criteria

Severity of harm S:

- S1 = slight injury (can be healed or is reversible)
- S2 = serious/fatal injury (cannot be healed or is irreversible; generally this begins with broken limbs, since this often results in permanent limitations for the person injured)

Frequency and/or duration of exposure F:

- F1 = seldom to quite often and/or short exposure time
- F2 = frequent to continuous
  (Limit > 4/hour to EN ISO 13849-1 and total exposure time > 1/20 of operating time)

Possibility of avoiding or limiting the harm P:

- P1 = possible under specific conditions
- P2 = nearly impossible

The following criteria are important for the estimation:

- speed with which the hazardous situation arises (e.g. quickly or slowly);
- possibilities to withdraw from the hazardous situation (e.g. avoidance by escaping);
- practical safety experiences relating to the process;
- whether operated by trained and suitable operators;
- operated with or without supervision.

When a hazardous event occurs, P1 should only be selected if there is a realistic possibility of avoidingor significantly reducing harm. Otherwise, P2 should be selected. To support designers in the estimation, the 2023 version of the standard contains an additional table. However, experiences with the application of this table are not yet available; therefore, we recommend not to use it.

Probability of occurrence O

- O1 = probability of occurrence low (well substantiated, e.g. by statistical evidence or accident history)
- O2 = probability of occurrence is high or cannot be estimated

4.2 Risk Estimation to IEC 62061

This is the best-documented method. Since it includes all four risk elements and uses finely graduated criteria, it is the most precise and also suitable for risk comparisons.

IEC 62061, like ISO 13849-1 carries the assumption of conformity under the EC Machinery Directive, already since 2005 even. The method therefore is completely equivalent to ISO 13849-1. The 2021 version contains a direct allocation of SIL and PL.

Risk Table

Severity of injury Se	Class C (Fr+Pr+Av)								
	3	4	5-7	8	9-10	11	12-13	14	15
4	SIL 1	SIL 1	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	SIL 3	SIL 3
	PL_r b	PL_r c	PL_r d	PL_r d	PL_r d	PL_r e	PL_r e	PL_r e	PL_r e
3	0		OM	SIL 1	SIL 1	SIL 2	SIL 2	SIL3	SIL 3
			PL_r a	PL_r b	PL_r c	PL_r d	PL_r d	PL_r d	PL_r e
2	0			OM	OM	SIL 1	SIL 1	SIL 2	SIL 2
				PL_r a	PL_r a	PL_r b	PL_r c	PL_r d	PL_r d
1				0		OM	OM	SIL 1	SIL 1
						PL_r a	PL_r a	PL_r b	PL_r c

OM = other measures recommended, i.e. no reliability requirements to IEC 62061 apply.
0 = no SIL or PL required
*PL b does not correspond to SIL 1 if only control category B to ISO 13849-1 is achieved

We recommend IEC 62061 because:
- it uses all four risk elements, which are finely graduated
- the results can be interpreted as a PL directly
- the method is universally applicable for risk comparisons

Risk Elements and Criteria

Severity of injury Se:

1	reversible: requiring first aid
2	reversible: requiring attention from a medical practitioner
3	irreversible: broken limb(s), losing a finger(s)
4	irreversible: death, losing an eye or arm

Frequency and duration of exposure to hazard Fr:

Duration of exposure ≥ 10 Min.	Duration of exposure < 10 Min.	Frequency
2	1	< 1 per year
3	2	< 1 per 2 week to ≥ 1 per year
4	3	< 1 per day to ≥ 1 per 2 weeks
5	4	< 1 per hour to ≥ 1 per day
5	5	≥ 1 per hour

Probability of occurrence Pr:

1	negligible
2	rarely
3	possible
4	probable
5	very high

The following questions should be asked:

- Is the personnel under stress while doing their work/in the situation (e. g., by a piece-rate, time constraints)?
- Is the person well trained and familiar with the risks?
- Is spontaneous failure of components (not of the safety-related control system) or triggering of malfunctions likely?

Take the mean value from the estimation of these questions.

Probability of avoiding or limiting harm Av:

1	probable
3	rarely
5	impossible

Three questions should be asked concerning the risk element Av:

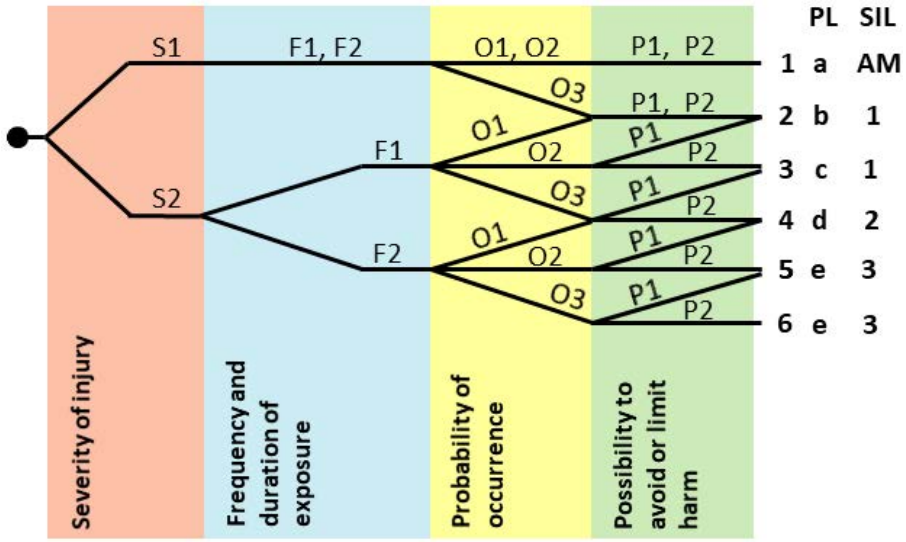
- Is the hazard detectable or known due to training?
- Can the person still escape/react, especially considering the speed of motion?
- Does the person him-/herself trigger the hazard (e. g., by consciously causing start by operating a control)?

4.3 Risk Estimation to ISO TR 14121-2

ISO TR 14121-2 is not a standard in the true sense of the meaning but a technical report (TR) authored by an ISO workgroup. This report is a summary of different methods practised in the industry.

The method for risk estimation presented in section 6.3.2 is gaining popularity. The reason for this is that it includes the fourth risk element – the probability of occurrence. But otherwise the method has the same weaknesses as does ISO 13849-1 Annex A. Even worse: The criteria for the probability of occurrence can hardly be used, especially for new products, because they depend on data from application of the machine.

Risk Graph



Risk graph to ISO TR 14121-2, 6.3.2 (Allocation of PL/SIL by author)

Risk Elements and Criteria

Severity of injury S:

- S1 *slight injury*, usually reversible; examples: scratch, laceration, bruise, light wound requiring first aid; the person is not more than two days incapable of performing the same task
- S2 *serious injury*, usually irreversible, including fatality; examples: broken or torn-out or crushed limb, fracture, serious injury requiring stitches, major musculoskeletal trauma (MST) etc.; the person is more than two days incapable of performing the same task

Frequency and/or duration of exposure to hazard F:

- F1 *seldom to quite often and/or short duration of exposure*
  Exposition twice or less per work shift or less than 15 min cumulated exposure per work shift
- F2 *frequent to continuous and/or long duration of exposure*
  Exposition more than twice per work shift or more than 15 min cumulated exposure per work shift

Probability of occurrence of a hazardous event O:

- O1 *low*, so unlikely that it can be assumed that occurrence may not be experienced
- O2 *medium*, likely to occur sometime, technical failure observed in the two last years. Inappropriate human action by a well-trained

person aware of the risk and having more than six months experience on the work station.
- O3 *high*, likely to occur frequently, technical failure regularly observed (every six months or less). Inappropriate human action by an untrained person having less than six months experience on the work station.

Possibility of avoidance or reduction of harm A:

- A1 *possible under some conditions:*, if parts move at a speed less than 250 mm/s and the exposed worker is familiar with the risk and with the indication of a hazardous situation or impending event; the worker also has to be capable of noticing the hazardous situation and being capable of reacting. Avoidance is possible depending on particular conditions (temperature, noise, ergonomic, etc.). *The person at risk himself triggers the hazardous event (presses a start button or enabling button) – the latter has been added by the author, it is not contained in the standard.*
- A2 *impossible*

SIL/PL

Originally, the method was not meant to be used to determine the PL or SIL, however, it may also be used for this purpose. The graph above shows a possible allocation of the results to the PL/SIL (added by the author).

5 What We Can Do for You

Together with their partners Axelent offers the following products and services around risk assessment:

- Book “Risk Assessment for Machinery and Systems”, Matthias Schulz, 2023, www.gft-verlag.de (currently available in German only).
- Software for risk assessment SafetyToolBox by pgx software solutions gmbh, www.pgx.de.All examples shown in this brochure were created using the SafetyToolBox..
  You may freely download the software and an evaluation code from:
  www.axelent.de
  www.pgx.de
- Coaching of risk assessment on site with intensive know-how transfer from our consultant to your staff
- Open and inhouse seminars on the following topics:

  - Risk assessment

  - ISO 13849-1 and computing of reliability with SISTEMA

  - Safety engineering for machinery and plant systems

  - CE Marking

  - Technical documentation and operating instructions meeting EU regulations

  - Basics of explosion protection

  - Product liability

5.1 Sample Risk Assessment

A complete risk assessment sample can be downloaded from Axelent's website. This example has been created using the Safety-ToolBox software by pgx.