Risk Matrices and Pitfalls



Risk is a concept we implicitly understand as human beings, and we discuss and evaluate it in many situations on a day-by-day basis. But what is the actual definition of risk? And what is considered an acceptable/tolerable risk? Does this concept change depending on the context, or has it an absolute meaning? How do we represent the risk? Lucia Capogna and Stephen Bull explore these questions and provide advice on some of the pitfalls that may be encountered when categorising and treating risk.

Risk definition – a reminder



In this article we will try to answer the questions around risk and present one of the possible representations and method for risk ranking: the risk matrix. Examples, types of matrices, their calibration and the main pitfalls are also discussed.

The International Electrotechnical Vocabulary (IEV) defines risk as "combination of the probability of occurrence of harm and the severity of that harm".

This definition has been adopted by many standards, including EN 61508-4:2010 and ISO 26262-1:2018.

A slightly deviation from this definition of risk is documented in the EN50126-1:2017, where "risk, <for railway RAMS>," is defined as "combination of expected frequency of loss and the expected degree of severity of that loss".

Thus, "risk" can be seen as a two-dimensional concept, where the two dimensions are the probability or frequency of occurrence of an event and the severity of the consequence of that event.

What is a risk matrix?

A Risk Matrix is a common method used for risk ranking or categorisation.



A Risk matrix is defined by Cox (2008) [1] as "a table that has several categories of "probability," "likelihood," or "frequency" for its rows (or columns) and several categories of "severity," "impact," or "consequences" for its columns (or rows, respectively)".

There are three types of risk matrices:

- qualitative risk matrix: the items on the axes of the matrix are defined with qualitative or descriptive terms (not numerical)
- quantitative risk matrix: the items on the axes of the matrix are defined in quantitative or measurable terms (numerical)
- semi-quantitative matrix: it is a combination of the qualitative and quantitative matrices. One of the axes can be defined qualitatively and the other one is expressed quantitatively (or one or both axes could be defined both qualitatively and quantitatively).

This is an example of a qualitative risk matrix (although it could be made quantitative by defining ranges for the descriptive frequency and severity labels).

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

For reference, CENELEC, EN 50126-1:2017 Annex C [5] gives an explanation of risk matrices (although no guidance on their calibration).

Where are risk matrices used?

Risk matrices, independently from the type, are commonly used to rank/categorise risks in a hazard log to prioritise effort and/or to single out high risks for further attention.

Later in the lifecycle they are used to accept risks in a hazard log.

Risk matrices are also used in many other fields than safety to determine the acceptability of other types of risks, e.g. they are also used for determining the acceptability of the operational, security, reputation and environment risks.

Example risk matrices

Examples of risk matrices can be found in many standards or codes of practice applicable to different industries or sectors, but also in guidance created for specific projects (usually where the project is complex or high profile).

With regards to the railway industry, an example risk matrix can be found in the EN 50126-1:2017 standard. This has been also reproduced in the Network Rail (NR) guidance on CSM-RA. Project-specific examples include the recently opened Crossrail in London; many other examples or guidelines can be found.

Other examples can be found in the Defence Industry:

- the Regulatory Article 1210 (RA 1210) issued by the Military Aviation Authority and specific for the ownership and management of operating risks, and
- the MIL-STD-882E issued by the US Department of Defence. This standard identifies the Department of Defence (DoD) approach for identifying hazards and assessing and mitigating associated risks encountered in the development, test, production, use, and disposal of defence systems.

Pitfalls in the definition and the use of risk matrices



When looking into the definition of risk matrices, we should consider that there are multiple exposed populations in different roles (e.g. workers and passengers) and the (perceived) risk appetite may be different for each. Thus, the risk matrices specific for each population are likely to be different. (For example, the UK HSE document Reducing Risks, Protecting People (R2P2) [3] assigns different targets for workers and members of the public.)

The judgement around the frequency, the severity or the risk appetite is often subjective and dependent on the experience of the people involved in their definition/calibration, in hazard workshops and in hazard review meetings.

In addition, the risk matrices definition should not be a standalone exercise but should consider the big picture (including applicable law or regulations and possible contradictions), otherwise across the same project/programme or domain the adopted risk matrices may be inconsistent. This does not mean that risk matrices for different operational aspects should be identical, but that it is very important they are compatible.

This should be also considered when different organisations are involved in the same programme. A supplier/subcontractor may have their own risk matrix which is not (necessarily) aligned to the programme / operator's matrix. The specific project scope (or portion of the project scope) should be considered in the risk matrix definition, as the overall risk matrix may be not adequate for the scope of the analysis or the sub-system. This adds additional burden to the entity in charge of the integration and responsible to "import" the contribution from a different matrix with possible transformation consequence.

This practice attracted criticism from the Haddon-Cave report into the Nimrod XV230 crash [2], which said "There are a myriad of different Hazard Risk Matrices used to determine risk categorisations. This is confusing, potentially dangerous, and makes it more difficult to compare risks across platforms", and we share that view that multiple risk matrices can cause confusion. However, for the reasons presented in this paper it is essential to calibrate matrices to the individual application. It is also essential that the reasons for different matrices are clearly justified and that care is taken to ensure that matrices used within the same project or programme reach consistent conclusions on the level of risk.

When using a risk matrix, it is also fundamental to consider the level of detail at which individual events are assessed. If the risk matrix is calibrated (see below) to consider hazards at the boundary of a system then separate assessment of the individual causes of the hazard (each representing a smaller portion of the overall risk) may lead to the false conclusion that the risk is acceptable. This needs to be taken into account:

- when deriving a risk matrix for a particular programme/project and
- when applying the risk matrix to individual hazards.

When using the risk matrices to rank risks, there are a few other areas that can lead to misuse or misinterpretation of the risk matrices too. For example, the link between tolerable and ALARP. There is the misconception that a tolerable risk is automatically ALARP. However, they are two different concepts: it is still necessary (and legally required in the UK) to demonstrate that all practicable measures have been taken to reduce the risk (ALARP). Hence, a risk matrix cannot be used on its own to declare that a risk is ALARP!

"There are a myriad of different Hazard Risk Matrices used to determine risk categorisations. This is confusing, potentially dangerous, and makes it more difficult to compare risks across platforms." (Haddon-Cave)

Another important pitfall in the use of risk matrices is the understanding and interpretation of the risk matrix axes.

The frequency of occurrence can be understood as "frequency of the Event (often the hazard) that might lead to the consequence" or the "estimated frequency of the Consequence". Many people do not understand the difference and mix them up in the same analysis. Instead, the consequence may be understood as the "worst case consequence" or the "most likely reasonably foreseeable consequence". It is very important to not mix up these concepts in the same analysis and understand the difference in their interpretation.

Sometimes standards and codes of practice may help in solving this. For example, in the railway sector a clear definition of the axes is documented in the EN 50126-1:2017, that states that the axes should be interpreted as the frequency and consequence of the accident arising from the hazard.

Another aspect to consider is the "additionality": if the scope of the programme is increased during its execution, then an amount of extra risk is likely to be added: depending on the nature of this risk, the risk matrix may need recalibrating and existing risks may need re-evaluating.

For further information, RSSB, Taking Safe Decisions, 2019 [4] provides useful principles on how to evaluate safety of a system.

Calibration

It is possible to calibrate a risk matrix from "first principles", taking into account that there are lots of issues and shortcomings. Often this calibration is necessary to ensure that the matrix is appropriate for the project.

When the risk is derived from a generic (overall) target, the calibration of the risk matrix must consider the scope of the analysis and how much of the overall risk can reasonably be assigned to the system under consideration.

The calibration should also consider the level of the risk assessment, i.e. if the scope is the assessment of individual hazards, then only a proportion of the risk budget (i.e. the tolerable level of risk for the overall system) is available per hazard and the risk matrix needs to be scaled accordingly.

For further reading on calibration, GE/GN8642 Issue 2 (withdrawn, but available from RSSB) (Appendix C) provides some guidance on calibrating a risk matrix [6].

Conclusions

The use of the risk matrices is considered an "easy" approach and for this reason they are very often overused or abused.

In reality, they are not really so easy to use, as they require to be calibrated to their particular application and there are many possible pitfalls in their use or definition.

Risk matrices can be a useful tool to quickly assess risks if properly customised / calibrated, however there are contexts where the use of risk matrices is not appropriate and alternative techniques are available.

Any use of a risk matrix should be accompanied by expert judgement as to the suitability and relevance of the outputs; it must also consider the context and the possible misuses and misinterpretations. Perhaps any risk matrices should come with a comprehensive set of assumptions and warnings!

References

[1] Cox Jr., "What's Wrong with Risk Matrices? Risk Analysis 28", L.A. 2008

[2] Charles Haddon-Cave QC, "The Nimrod Review - An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006", Oct. 2009

[3] HSE, Reducing Risks, Protecting People (R2P2), 2001: HSE's general approach to risk management, including the "carrot diagram" and overall targets for acceptable risk

[4] RSSB, Taking Safe Decisions, 2019: gives principles about how to evaluate safety of a system

[5] CENELEC, EN 50126-1:2017 Annex C: gives an explanation of risk matrices (no guidance on their calibration)

[6] GE/GN8642 Issue 2 (withdrawn, but available from RSSB) (Appendix C) provides some guidance on calibrating a risk matrix

Image attribution
top image 99257674 © Alphaspirit | Dreamstime.com
risk 114395146 © Anyaberkut | Dreamstime.com
risk matrix 175934678 © Elnur | Dreamstime.com
pitfall 48702118 © Alexmillos | Dreamstime.com

Lucia Capogna, Principal Engineer, Ebeni Limited

Lucia has over 15 years' experience in software, safety and cyber security with background in multiple industries including Railway, Defence, Oil & Gas and Renewable Energy. Lucia also represents the UK in several CENELEC and IEC standardisation groups for software, cyber security and safety standards.

Stephen Bull, Principal Safety Engineer, Ebeni Limited

Stephen has over 25 years' experience in the development and assurance of safety critical systems in a variety of industries, including rail, defence and air traffic control. He is a Chartered Engineer and a Fellow of the Safety and Reliability Society.