Approaching an understanding of risk: a subject for the EFNDT Working Group 5 "NDT Technology for Public Security and Safety"

Kurt OSTERLOH 1, Norma WROBEL 1
1 BAM Federal Institute for Materials Research and Testing; Berlin, Germany;
Phone +49 30 8104 3654, Fax +49 30 8104 4657; kurt.osterloh@bam.de,
norma.wrobel@bam.de

Abstract
Safety and security both entail freedom from danger, i.e. unacceptable risk, whatever the cause might be. This entails an understanding of the term "risk" that is broadly used in areas such as economics, health, insurance etc. According a rather popular definition used in the economical sciences for a long time (KNIGHT), risk has a lot in common with uncertainty while the former is regarded quantifiable and the latter one is not. However, it has to be taken into account that there are other understandings of "uncertainty". Particularly encountering rare events never experienced before and recent contemporary definitions are weakening Knight's differentiation. This is reflected in some recent standard definitions. Attempts have been made to define a risk as common as possible covering not only societal, ecological and financial areas but also natural and technical, ones. This is of particular concern in non-destructive testing. This raises the question how far this can be achieved in a common understanding, i.e. the discussion on this term seems not at all finished yet.
It is a common ambition to lower the risk by several actions including detection technologies. This entails that a risk could be estimated somehow. The existence of numerous approaches indicates the complexity of this question. The EFNDT (European Federation for Non-Destructive Testing) Working Group 5 took a commitment also to tackle this central aspect of safety and security in its understanding as a bridging forum between these two areas.

Keywords: Risk definition, risk assessment, vocabulary standards, EFNDT Working Group 5 (WG5)

1. Introduction

The Working Group 5 of the European Federation for Non-Destructive Testing (EFNDT WG 5 http://www.efndt.org/Organisation/WorkingGroups/WorkingGroup5.aspx) is deeply engaged in elaborating common aspects of security and safety, both subjects of public concern. Though organised in different public entities, both subjects share the view of freedom of danger. This is even reflected in definitions found in international standards. A definition of security is rather rarely found in international standards. A useful one has been detected in the ISO 2800 [1] dealing with the security management for supply chains. This term is defined as "resistance to intentional, unauthorized act(s) designed to cause harm or damage …".

Many standards refer lastly to the ISO/IEC Guide 2 [2] when defining safety: "freedom from unacceptable risk of harm", continued in the ISO/IEC Guide 51 [3] in an abbreviated way, i.e. skipping "of harm". However, this entails an understanding of risk acceptance that is defined as "informed decision to take a particular risk" in the ISO Guide 73 [4]. A more sophisticated definition of safety has been found in the context with quality management as follows: "state in which the risk of harm … or damage is limited to an acceptable level"[5]. It should be mentioned that several languages only have a single word for both, safety and security. Hence, a very concise remark should be allowed about a common ground and difference may exist

between them both. Since an unexpected acting by someone with a malicious intend designed to cause harm can be regarded as a risk, the difference between safety and security seems to consist of the resistance to something or the freedom from it, i.e. emphasising on an active process in favour of a status that is achievable by such an act. These matches the definitions given by the Webster's Dictionary [6]: safety "freedom from exposure to danger …"
and security again, "freedom from danger", but also: "measures taken …", i.e. an active component. It should be emphasized that counteracting against malevolent intentions is con-sidered in this contexts as opposed to failings of a benevolent operator or unconscious neglect. As a consequence, an understanding of risk is really complex and may vary with time and circumstances. Therefore, a mutual consensus on the meaning of risk appears to be an indispensable effort for the success of a working group engaged in achieving cooperation between the different entities involved in this matter.

2. Defining risk

An understanding of risk might be aided by including the counterpart which is a "chance" in a broad consensus. However, both sides are not completely separable, "no risk no chance". No wonder that this subject has been broadly tackled by the economists in the world of business. At least and particularly in these areas, a rather popular definition of risk was provided by KNIGHT [7] in the past. Though he admits that the term is "loosely used in everyday speech and in economic discussions", he associated a quantitative property with it when differentiating it from "uncertainty", the non-quantitative pendant. This distinction has been perpetuated for quite a long time while some discrepancies became apparent in the understanding of risk even in the context of financial markets [8]. Moreover, it is obviously in conflict with the understanding in natural and engineering sciences when it comes e.g. to measuring uncertainties. This makes it essential to find a common base again when communicating between such different areas as encountered in technical safety and public security.

2.1 The term "risk"

The recent accident with the damaged passenger vessel near the north-eastern coast of Italy painfully reminds the assumed origin of the term "risk" from the Italian language of the 16th century meaning something like "sailing round a cliff". The closer you navigate the ship to the cliff, the shorter or more spectacular the way might be, but you may hit it. The other way round, if you keep distance, you may take the longer way. Again, the antagonism of risk and chance, as mentioned above, becomes evident here, or in other words, the possibility of a gain and that one of a loss. Today, the negative aspect of "risk" seems to prevail in the view of threatening losses leaving it close to the term "danger". In spite of several initiatives by ISO/IEC and others, it appears rather cumbersome to achieve a commonly accepted definition of risk though the term itself is commonplace in our conversations. According to an actual literature search, the ndt-community has not yet contributed significantly to this. At large, standards are regarded as an appropriate tool to achieve a common sense, particularly because they comprise the result of extensive discussions between several experts. Therefore, international standards explaining "risk" or related terms in their terminology section have been screened for appropriate definitions – with heterogeneous results as shown in the subsequent subsection (2.2). Interestingly, "probability" occurs as an intrinsic element of risk beside "uncertainty", however, not as defined by KNIGHT [7], i.e. as a completely non-quantitative opposed to "risk". With that, an interface is given to the field of statistics dealing with distributions and frequencies that could be derived from observations in the past. However, this makes it inevitably difficult when dealing with rare events or of that kind which have not been encountered before as described by TALEB [9].

It certainly does not make sense to deal with frequencies in such a case. This leaves pondering about probability what it could mean and what not. However, taking a risk lastly means deciding how close sailing round a cliff to gain an advantage, to stay with the initial view. At the end, there might be two oppositional outcomes, either the benefit having taken a chance or being confronted with an irreversible harm or damage. But the point of decision comes before an event. This is the problem of risk and makes it desirable to know whether it remains within certain acceptable limits or may become intolerable. In essence, at least an estimate is requested. This is a matter being discussed in the next subsection (2.3). Unfortunately, it would go beyond the scope of this contribution also to include combinations and related terms.

2.2 Standard definitions of risk

As mentioned before (2.1), standards are assumed as a source of a base of understanding. In this context, this means an appropriate and an acceptable definition of risk. However, some heterogeneity remains even within the international ones as demonstrated in Table 1. Moreover, the definitions have been shifted with time resulting in the introduction of new terms such as "objectives" instead of "consequences" or "severity of … harm". It has to be transferred to further discussion if this kind of development has been of benefit towards a common understanding of the term "risk". In that course, it should be considered whether the recent changes may contribute achieving a better common understanding or not. Particularly since the term "risk" is being used in so many profoundly different areas such as engineering, financing or social sciences, it is still a requirement to find a common ground to communicate understandably. As a consequence, it might be suggested that organisations such as the ISO/IEC could take a lead in this discussion. Other obstacles in an international understanding are linguistic peculiarities when it comes to transfer international standards into national regulations.

Table 1. Risk definitions as reflected in international standards

year	standard	subject	definition of risk
1999	ISO/IEC Guide 51 [3]	safety aspects	combination of the probability of occurrence of harm and the severity of that harm
2001	EN 13701 [10]	aerospace	a quantitative measure of the magnitude of a potential loss and the probability of incurring that loss
2002	ISO/IEC Guide 73 [11]	risk management (*old*)	combination of the probability of an event and its consequences
2005	ISO/IEC 27002 [12]	information technology	*quoted from ISO/IEC Guide 73:2002*
2007	ISO 22399 [13]	societal security	"
2009	ISO Guide 73 [4]	*new*	effect of uncertainty on objectives
2009	ISO 11014 [14]	chemical products	*quoted from ISO Guide 51:1999*
2009	ISO 31000 [15]	risk management	*quoted from ISO/IEC Guide 73:2009*
2011	ISO/IEC 27005 [16]	information technology	"
2011	DIN EN ISO 12100 [17]	Safety of machinery	*identical with ISO/IEC Guide 51*

Interestingly the ISO/IEC 27005:2011 norm has a definition of the combined term "level of risk" as a magnitude of a risk expressed in terms of the combination of consequences and their likelihood [16]. Apparently, this seems to be indirect return to the earlier definition of risk given in the ISO/IEC guide 51 [3] by introducing the add-on "level", however, giving rise to further discussions. A justification of the term "likelihood" is given in the notes of the new standard (note 2); it is preferred in favour

of “probability” since the latter is “often narrowly interpreted as a mathematical term”. In this context, it is further noted in this norm that the term “probability” has a broader interpretation in other languages than in English. This linguistic problem should be discussed more thoroughly with the experts in several different languages beside the English one.

2.3 Assessing risk

Since the definition of safety entails “unacceptable risk” in the understanding of exceeding an acceptable level, it becomes quite obvious that there is a desire to quantify risk as stated by KNIGHT [7]. Several suggestions how to put it straight and simple have been made as illustrated in Figure 1. As long as probability has to be considered as an intrinsic feature of risk, it is certainly not measurable like a physical property such as a length with a ruler, in analogy to Taleb [18]. Alternatively, the mere product of probability and consequences as shown in the next line within Figure 1 appears too simplified since the relationship between these two building blocks of risk appears much more complex in most cases, by far more than a linear function. There is no change to this when involving threat, asset and vulnerability. The question remains if it could be an insurance sum only the insurer knows how it might be calculated.

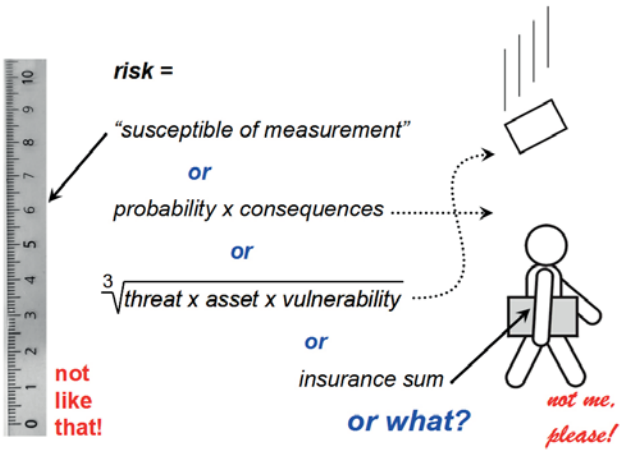

Figure 1. Ideas and suggestions for numerical quantification of risk: measurements and calculations. It should be suggested that risk only could be estimated at last.

It should be acknowledged that a distinction should be made between a calculation and an estimate, i.e. an exact result and a vague number associated with certain assumptions. Any numerical approach requires an estimate how often an event may occur, i.e. a “probability”. Combining this with the possible outcome if anything happens in a highly simplified manner by a multiplication of the probability of an event and the harm it might cause resulted in an approach used in the insurance mathematics or in the context of fire protection [19]. A more complex variation includes a vulnerability variable [20]. As said before, probability is an intrinsic feature of risk, no doubt. The question remains how to understand probability. A plethora of literature exists on this topic, however, it is rather commonly reduced on a Gaussian distribution curve whereas sufficient evidence exists that Mother Nature is anything else than Gaussian distributed. Sudden events may even not fit into any linear algebraic model. This in particular makes forecasting based on distributions of probabilities so difficult and unreliable. It should be kept in mind that probability should not be confused with predictability. Any event with a probability of occurrence could happen any time, right now, soon or whenever. As it could be understood from the standards (2.2), risk does not consist only of the probabil-ity of an event, but also entails the occurrence of harm itself and its severity. From the technical point of view, this part could be easier estimated than the first one in a given environment. There are countable values around that could be damaged or destroyed by an event that could be evaluated. Nevertheless, some uncertainty remains also here. A big blast e.g. makes walls tumbling down, so far so sure. However, it cannot be predicted how far the bricks might flow possibly causing further damages. In principle, the definition of risk given in the ISO Guide 51 [3] gives at least a technically feasible approach, i.e. a combination of the prob-ability of occurrence of harm and the severity of that harm. How these two aspects are linked together depends on the nature of the occurring event and how this could be converted into calculable terms.

There have been many discussions of this kind which are manifested in some rules and regulations. It would be beyond the scope of this contribution even to refer to some examples. However, it seems to be sure that these discussions will continue in the future.

3. Practical approaches

Whenever it has to be decided whether an activity should be launched or not, or which way to choose, risks are or should be considered into the decision process. This means that they have to be identified and to be assessed. The fact that this has been and is in progress in various areas entails that many approaches exist in parallel to some individual understandings of risk. Again, standards may have the potential to pave the way of a common understanding since they have been preceded by numerous discussions among the experts, as said before. A starting point might be the risk identification and assessment which risk analysis and risk evaluation as stated in the international guides ISO Guide 51 [3] and ISO/IEC Guide 73 of 2009 [4]. This includes the decision whether a risk and/or its magnitude is acceptable or tolerable. From the technical point of view, an interesting aspect always is if there are measures available to make a given risk acceptable or tolerable.

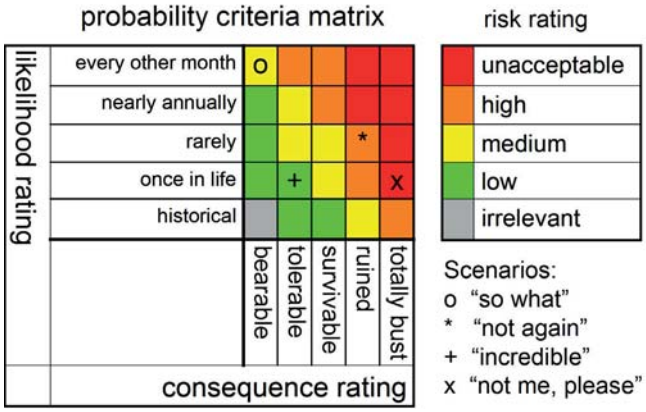

Figure 2. An example of risk assessment techniques as principally in IEC/ISO 31010. The parallel wording of "probability" and "likelihood" has been left unchanged to indicate the linguistic discussion mentioned above which is still open. The matrix has to be adopted for each individual application anyway.

In any case, an assessment is requested, and it has to be decided how to approach this problem. It remains beyond the scope of this treatise to tackle even a selection of the existing ones. Therefore, just a single one is picked from suggestions in one of the international standards.

The annex of the IEC/ISO 31010:2009 [21] provides an appreciable collection of recipes. From the selection of more than 30 approaches how to assess a risk, an example is given in Figure 2 showing a "consequence/probability" matrix in a modified form. This kind of approach is in use at the German Federal Office of Civil Protection and Disaster Assistance (BBK). Each row represents a level of likelihood ranging from an event occurring very often, i.e. every other month, or so rarely that there might be a chance to miss it in one's life. The consequences of an event are found in the columns of the matrix running from a bearable touch to a devastating clash in an arbitrary scaling in this example. Each cell of the matrix is assigned to a verbal risk rating from irrelevant, i.e. there is no risk, up to completely unacceptable. This kind of qualitative scaling allows a vast dynamic range and some nonlinearity. There is no decisive threshold in the matrix for accepting a risk or taking measures. Instead, there is a medium zone, marked in yellow, where a decision may depend largely on the individual circumstances. This matrix is suitable to place certain scenarios into appropriate cells. They may be related to individual situations in certain circumstances depending on time, place or individuals involved. This matrix setup should serve only as an example, the most colourful, how to approach the problem of risk assessment. There are several more approaches how risks can be evaluated. Some of them use mathematical/statistical methods to investigate interrelationships such as the Markov chains or the Bayesian statistics. It appears quite obvious the annex of the IEC/ISO 31010 provides a lot of stimulating suggestions how to approach the risk assessment problem. However, a recipe alone does not fill one's stomach.

4. Conclusion and outlook

Apparently, the discussion how to understand risk has not come yet to a commonly accepted conclusion satisfying all areas. From the historic approaches to the shifted definitions found in the current international standards, one has been found that might suit also technical requirements and expectations. It is the ISO/IEC guide 51 of 1999 [3] where the two elements probability and the severity of a harm that may occur. It remains an open issue among the areas where the term "risk" is being used how to tackle the "uncertainty" or probability aspect. It certainly should never be confused with predictability since any event with any probability of occurrence could happen within the next moment or ages ahead. Presumably the definition of the "level of risk" might assist to find a common understanding as found in the "new" ISO Guide 73: "magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood" [4]. Very obviously, another term has been introduced: "likelihood". As a consequence, the discussion on the understanding of risk goes on. Seeking a common base, the technical experts, the providers of safety and security related technologies and all the organisations responsible for a safe and secure public environment should participate in this discussion. Even and particularly if finding a commonly accepted definition of risk emerges as a difficult task, a common understanding of it remains the base of fruitful discussions and of projecting collaboration between all the different areas involved. Without it, confusion may be raised that might be contraproductive. The EFNDT Working Group 5 has adopted a commitment in this direction.

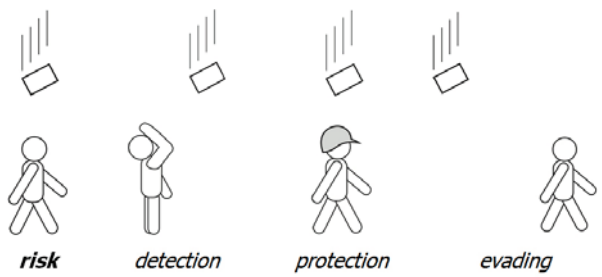

Figure 3. Tackling a risk

Finally, approaching a common understanding of risk does not provide a solution how to get around with it. This is the next subject to be tackled, unfortunately leaving the scope of this contribution. However, some ideas are given in Figure 3 as an outlook. The ndt-community has its place in the forefront of preventing disasters, i.e. the detection. Therefore, it has a legitimate position to participate in the discussion on the understanding of risk.

Acknowledgements

The Authors are deeply indebted to Director and Professor Dr. N. Pfeil of BAM for numerous fruitful discussions and many valuable and highly appreciable hints and advices. They also wish to thank the German Federal Ministry of Education and Research (BMBF) for supporting this work in part (project "FluSs", FKZ: 13N10054 and project "SefLog", FKZ: 13N11225). Information about the EFNDT Working Group 5 can be found at: http://www.efndt.org/Organisation/WorkingGroups/WorkingGroup5.aspx

References

1. ISO 28000:2007(E): Specification for security management systems for the supply chain | 2. ISO/IEC Guide 2:2004(E/F/R): Standardization and related activities — General vocabu¬lary; Normalisation et activités connexes — Vocabulaire général; Стандартизация и смежные виды деятельности. Общий словарь | 3. ISO/IEC Guide 51:1999(E): Safety aspects – Guidelines for their inclusion in standards | 4. ISO Guide 73:2009(E/F): Risk management – Vocabulary, Management du risque – Vocabulaire | 5. DIN EN ISO 8402, 2. Erg.-Lieferung/Dezember 1995: Qualitätsmanagement, Begriffe, Quality management and quality assurance – Vocabulary, Management de la qualité et assurance de la qualité (ISO 8402 :1994) | 6. Webster's Third New International Dictionary of the English Language, unabridged, G. & C. Merriam Co., 1976, USA | 7. Frank H. Knight: Risk, Uncertainty, and Profit, 1st ed. 1921. Hart, Schaffner &Marx; Boston: Houghton Mifflin Company, The Riverside Press, Cambridge | 8. Glyn A. Holton: Defining Risk, Financial Analysts Journal 2004, 60(6), 19-25 | 9. Nassim NicholasTaleb: The Black Swan, The Impact of the Highly Improbable, Penguin Books London, revised edition 2010, ISBN 978-0-141-03459-1 | 10. EN 13701:2001: Aerospace - Space systems - Glossary of terms; Trilingual version | 11.ISO/IEC GUIDE 73:2002(E/F): Risk management — Vocabulary — Guidelines for use in standards; Management du risque — Vocabulaire — Principes directeurs pour l'utilisation dans les normes | 12. ISO/IEC 27002:2005: Information technology – Security techniques – Code of practice for information security management | 13. ISO 22399:2007(E): Societal security — Guideline for incident preparedness and operational continuity management | 14. ISO 11014:2009(E): Safety data sheet for chemical products — Content and order of sections | 15. ISO 31000:2009(E): Risk management — Principles and guidelines | 16. ISO/IEC 27005:2011: Information technology — Security techniques — Information security risk management | 17. DIN EN ISO 12100:2011-03 : Safety of machinery – General principles for design, Risk assessment and risk reduction (ISO 12100:2010), English translation of DIN EN ISO 12100:2011-03 | 18. N. Taleb, Der Schwarze Schwan: Konsequenzen aus der Krise, C. Hanser Verlag München, ISBN 978-3-446-42410-4, The Black Swan. The Impact of the Highly Improbable, New York, Random House 2007 | 19. DIN EN ISO 13943:2000: Brandschutz - Vokabular, Fire safety – Vocabulary, Sécurité a feu – Vocabulaire | 20. M. Nöldgen, A. Nawabi, M. Juszkiewicz: Risk Evaluation for Critical Built Infrastructure, Asset Classification and Evaluation. 6th Future Security, Berlin 2011, Proceedings ed. J. Enders and J. Fiege (ISBN 978-3-8396-0295-9), Session B.6, 490-497 | 21. IEC/ISO 31010:2009: Risk management – Risk assessment techniques; Gestion des risques – Techniques d'évaluation des risques