

# Chapter 2

## Defining Concepts and Categorizing Interdependencies

Jørn Vatn, Per Hokstad and Ingrid Bouwer Utne

**Abstract** This chapter defines and discusses important concepts like risk, uncertainty, vulnerability and interdependency. In the literature, these concepts are used in various ways and there exists no common accepted terminology. Therefore, these terms are defined to provide a basis for consistent use throughout this book.

### 2.1 Observables and Uncertainty

Uncertainty is the fundamental concept when defining risk. Uncertainty is here used to describe the lack of certainty regarding events, conditions, magnitudes, etc. Especially, we are uncertain regarding so-called observables. Observables are quantities or events which in principle are observable at some point in time. At the analysis point in time, the observables are not known, but they will become known at a later stage; hence, they are treated as random quantities in the analysis. For example, the number of electricity users affected by a major outage is uncertain at the time of analysis, but will be known in principle after an outage has occurred. In order to express uncertainty in quantitative terms, probability statements are used. For observables directly related to the decision(s) to be made with support from the

---

J. Vatn (✉)

Department of Production and Quality Engineering,  
Norwegian University of Science and Technology, Trondheim, Norway  
e-mail: jorn.vatn@ntnu.no

P. Hokstad  
SINTEF Safety Research, Trondheim, Norway

I. B. Utne  
Department of Marine Technology, NTNU, Trondheim, Norway

risk analysis, a main objective is to quantify the uncertainty and presents the corresponding risk picture.

## 2.2 Risk

A variety of definitions of risk exist in the literature ranging from “probability times consequence” to “uncertainty related to issues valued by humans”. When it comes to expressing risk in a risk analysis, there are two important ways of thoughts: The traditional interpretation is that risk is a property of the system being analysed where risk comprises two dimensions; probability addressing whether undesired events will occur or not, and the consequences indicating the severity of the undesired events. A more recent interpretation (see e.g. [1]) takes uncertainty as a basis when risk is to be defined. In this interpretation, there are no inherent probabilities describing the system. The performance of the system in terms of whether events occur or not, and their severity is uncertain. This uncertainty is then expressed by probabilities reflecting the state of knowledge the risk analysis group has regarding the system being analysed. This interpretation is therefore often referred to as an epistemic risk definition and to quantify risk, three elements are introduced:  $\langle e, p, S \rangle$ .  $p$  is used as a probability measure of the occurrence of an event, say  $e$ .  $S$  represents the severity of the event. Note that  $S$  is a multidimensional random quantity, covering several dimensions like personnel safety, environmental impacts, material damages, loss of service, etc. Since there is more than one event to treat,  $i$  is used as an index to run through all relevant events. An operational definition of risk is now the set of all relevant triplets:

$$R = \{ \langle e_i, p_i, S_i \rangle \} \quad (2.1)$$

In Eq. (2.1),  $p_i$  is used to quantify uncertainty regarding the occurrence of an event  $e_i$  for a given time period. Rather than focusing on a given time period, it is often more convenient to consider a time unit, and the probability term is then replaced by a frequency. A frequency ( $f_i$ ) is then to be interpreted as the expected number of occurrences per unit time.

When risk is expressed in terms of Eq. (2.1), this is always done conditionally on a set of aspects which here is denoted as  $\mathcal{D}$ ,  $\mathcal{U}$  and  $\mathcal{V}$ .  $\mathcal{D}$  represents the result of dialogue processes and risk communication among stakeholders that elaborate on the values and preferences domain, such as who are exposed to threats, and whose needs in the society should be focused on. Further,  $\mathcal{U}$  represents the relevant information, the theories, the understanding and the assumptions which are the basis for the risk assessor, and finally,  $\mathcal{V}$  represents the result of any verification processes, for example, third party verification. See [2] for further discussion of this operationalization of the risk concept.

In the traditional or classical definition of risk, the probabilities in Eq. (2.1) are interpreted as true properties of the system being analysed. Since we have limited data and information regarding the system, it is impossible to reveal the exact values of these probabilities. It is then common to present uncertainty intervals for the risk measure.

In the epistemic interpretation, it is the other way around. Then, the basis is that there is uncertainty regarding whether the undesired events will occur, and the corresponding severity. Probabilities are used to express this uncertainty, and there is no additional uncertainty in the probability statements. However, as part of the documentation of the risk analysis, uncertainty is qualitatively stated in terms of discussion of assumptions and simplifications. In relation to Eq. (2.1), such arguments are stated as part of  $\mathcal{U}$ .

Methods and models used in risk analysis are often not affected by the interpretation of risk in Eq. (2.1). However, the way uncertainty is interpreted and presented will vary between the classical and the epistemic interpretations of risk.

## 2.3 Risk Register and Risk Matrices

A risk register is a formal document used to document the result of risk assessment exercises. The risk register is a table where each undesired event is listed in a separate row. The column headings may vary from analysis to analysis, but typical headings are (1) hazard/threat, (2) possible corresponding event, (3) probability of the event to occur and (4) consequence given that the event occurs. Since a risk register also serves as a follow-up tool as part of the risk management process, more headings are introduced that cover risk-reducing measures, responsibilities and due dates. The use of risk matrices in risk management is outside the scope of this book, but some challenges in documenting hazards and threats in a risk register are discussed in the following.

When documenting events in a risk register, it is common to specify probability and consequence in semi-quantitative terms, that is, by use of intervals. For example, P1 is used to represent a probability less than one per 1000 years, P2 is used to represent a probability between one per 100 years to one per 1000 years, and so on. Similar categories are used for the consequence dimension.

Each event in the risk register may then be plotted in a risk matrix illustrated in Fig. 2.1. The red-yellow-green colour regime indicates the magnitude of the risk and is a result of a calibration process. Typically, the red area represents a situation where we normally cannot proceed without implementing risk-reducing measures. The yellow area represents a situation where risk-reducing measures should be evaluated and implemented unless they are unreasonable costly or impractical. This is often referred to as the ALARP principle (as low as reasonably

**Fig. 2.1** Example of risk matrix

practicable). In the green area, one usually proceeds without any risk-reducing measures unless there are some obvious efficient measures available.

Regarding the severity of an undesired event, a challenge is encountered when the probability distribution over  $S$  is to be mapped into one single consequence number, since one often is dealing with several dimensions like safety, costs and outage of service. One way of tackling this is to specify one consequence number for each of these dimensions and then plot the events in separate risk matrices. What becomes trickier then is to map the probability distribution over each consequence dimension. If five consequence classes ranging from low to high were used, one could present five symbols in the risk matrix for each event and for each consequence dimension. The probability of each *symbol* is then found by multiplying the probability of the undesired event with the corresponding probability of the consequence. A more simplified approach is to insert only one symbol for each event using the worst-case consequence. A reasonable worst case means a situation where the probability of the consequence class is in the order of 5–10 %. Note that the probability statement must then also reflect the worst-case situation.

## 2.4 Reliability

Whereas risk is a term used to pinpoint what can go wrong the term reliability points to a system or a components ability to perform the predefined required functions. Reliability is measured in terms of the probability that a system or a component is able to perform its required function at a given point of time, or over a given period of time for a given set of conditions. For example, the reliability of a backup generator is the probability that it will start upon a demand and that it will function for eight hours.

## 2.5 Vulnerability

While the term risk primarily is used to express uncertainty regarding adverse events, the concept of vulnerability is more directly related to the characteristics of a system. In daily speech, a child is vulnerable since its ability to resist threats and dangers is low. Therefore, the focus in a vulnerability analysis moves away from the *possibility* that adverse events occur, to system properties determining how easy it is to eliminate major system functions. For example, a vulnerability analysis of power supply intends to examine how the system is able to withstand adverse events and threats, such as line breaks, sabotage and ageing. Often, a vulnerability analysis extends the regular system limits, that is, it does not only focus on the number of affected end users, but also the impacts, such as who is affected (e.g. a hospital or a key company in the region), and measures implemented to mitigate the consequences (e.g. mobile gasworks).

It is often valuable to use a checklist with vulnerability factors to assist the consequence assessments when using a risk register. Examples of such factors are as follows:

- Area
- Chain effects
- Culture
- Degree of coupling
- Dependency with other societal critical functions
- Duration
- Geographical scope
- Level of maintenance and renewal
- Mental preparedness
- Outdoor temperature
- Population density per 1 km<sup>2</sup>
- Quality of operational procedure and knowledge
- Substitution opportunities for infrastructure
- Time of day.

Scores may be defined reflecting a possible qualitative state of each factor. For example, the vulnerability factor “time of day” may include the states *Night*, *Evening*, *Working hours*, *Early morning* and *Rush hours*.

## 2.6 Resilience

In recent years, the term resilience has been introduced in relation to risk and safety. In general, resilience is the ability of a system to react and recover from unanticipated disturbances and events (see e.g. [3]) in contrast to reliability which is the ability of a system to have an acceptable low failure probability with respect

to a defined function and a given operational conditions [4]. Since reliability at least implicitly restricts focus to a *given* set of stress, the term resilience is therefore preferred in situations where any kind of stresses and disturbances are to be considered. McDaniels et al. [5] point out two key properties of resilience, namely robustness and rapidity. *Robustness* refers to a system’s ability to withstand a certain amount of stress with respect to the loss of function of the system, or as Hansson and Helgesson [6] define it: “the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations”. *Rapidity* on the other hand refers to a system’s ability to recover from an undesired event with respect to the speed of recovery. Vulnerability as defined above may thus be seen as the antonym to resilience, capturing both the robustness and the rapidity aspects of a system.

2.7 Bow Tie Diagram

Figure 2.2 shows a so-called bow tie diagram often used as a conceptual model to assist the risk modelling. The starting point for the analysis is the undesired event shown in the middle of the diagram. To the left, possible causes behind the undesired event are illustrated, and the consequences that might follow are included to the right. Several barriers and safety functions are implemented to prevent the undesired event from occurring and to mitigate the consequences given that the event has occurred. Vulnerabilities are conditions related to the system being analysed which may have a negative impact on either the possibility of the undesired event to occur or consequences given that the event has occurred. For example, given a bad state of the vulnerability factor *maintenance and renewal*, an electrical grid is more prone to blackout events, that is, on the causal side. On the other hand, a bad state of the vulnerability factor *quality of operational procedure*

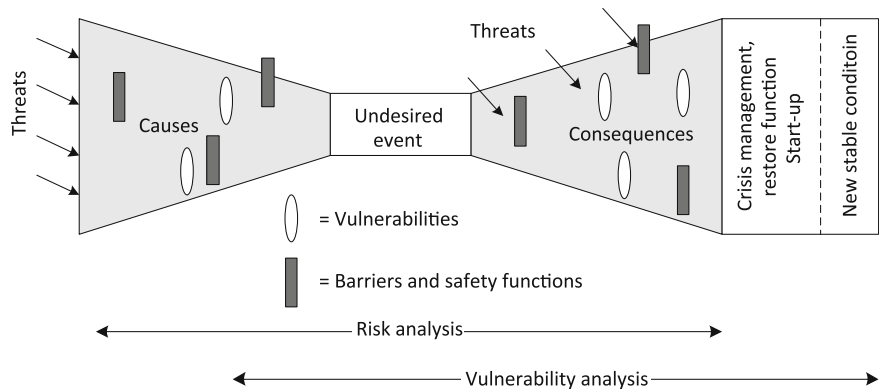


Fig. 2.2 Bow tie diagram with related terms

*and knowledge* will lead to longer restoration time, and hence, more severe consequences.

Figure 2.2 also indicates that a traditional risk analysis starts early in the course of events that may lead to the undesired event, and that typically stops at the immediate consequence(s) of that event. The vulnerability analysis has less focus on the causes behind disturbances in the system, but focuses more on the vulnerabilities that may cause such disturbances to result in the undesired event. The vulnerability analysis also has a more comprehensive view on the recovering process that follows after the immediate consequences of the event.

## 2.8 Basic Needs, Societal Critical Functions and Infrastructure

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and the economy. Since the word *infrastructure* points to physical assets, other terms are often introduced focusing on what to achieve, such as *life lines* and *societal critical functions*. Societal critical functions can be defined as functions that are essential to ensure the basic needs of a society. DSB [7] has made a systematization of needs, functions, infrastructures, and inputs, described below.

### 2.8.1 Basic Needs

The basic needs point to what is considered essential in a society, and in this context, this means as follows:

- Food
- Water
- Heating and cooling
- Safety and security.

### 2.8.2 Societal Critical Functions

A variety of societal critical functions are required to ensure that the basic needs of a society are fulfilled. It is not always obvious which societal functions are to be considered as critical. DSB [7] proposes to limit critical functions to those functions where (1) a loss of the function in seven days or more will threaten basic

needs and (2) such a loss occurs under disadvantageous conditions and/or in combination with coincidence of other events. Based on such an argument, the societal critical functions are as follows:

- Water supply
- Food supply
- Heat supply
- Financial security
- National security
- Life and health
- Crisis management
- Law and order.

### ***2.8.3 Infrastructure***

The societal critical functions depend on infrastructure components. To some extent, infrastructure components may be replaced by other substitutes; hence, their criticality depends on the organization of infrastructure components in the society. The following basic infrastructure components are often considered:

- Telecommunication network
- ICT-network
- Network of roads
- Railway network
- Water and sewage network
- Fuel supply and logistics
- Power grid
- Harbours.

### ***2.8.4 Input Factors***

Finally, several input factors are required to provide the infrastructure elements and/or the societal critical functions. These are as follows:

- Labour
- Other services
- Transportations
- ICT-services
- Telecommunication
- Goods and products
- Energy.



## 2.9 Dependency and Interdependency

In classical risk analysis, the concept of *stochastic dependency* is crucial since various types of dependencies may compromise the effect of the “defence in depth” principle emphasizing the importance of multiple barriers to control hazards. Two events A and B are said to be stochastic independent if information regarding the occurrence of one of the event will not alter the probability of the other one. Mathematically, this is expressed by:

$$\Pr(A|B) = \Pr(A) \quad (2.2)$$

Stochastic dependency then means that information regarding the occurrence of one of the events will change the probability of the other. Our main concern is *positive dependency* where the occurrence of an event typically represents a barrier failure, and positive dependency then means that the probability of failure of one of the barrier increases if it is known that the other barrier has failed. Although stochastic dependency is accounted for in risk analysis, it does not indicate the type of dependency or causes behind.

In risk modelling of critical infrastructures, there are several types of dependencies to take into account: Various regimes exist in order to classify types of dependencies, and it is common to use the term *interdependency* between infrastructures, rather than the term dependency. Rinaldi et al. [8] propose a categorization regime with 6 dimensions to understand various aspects of interdependency. Three types of interdependencies and failures are applied in this book, motivated by Rinaldi et al. [8]:

- a. *Cascading failures*, where a failure in one infrastructure causes disturbances in another infrastructure. In this situation, there is a functional relationship between two or more infrastructures. For example, water supply is dependent on electricity for water treatment.
- b. *Escalating failures* where failure in one infrastructure worsens an independent disturbance in another infrastructure. For example, a breakdown in the metro is significantly worse if a main road is unavailable due to a fire in a tunnel.
- c. *Common cause failures* where two or more infrastructures are disrupted at the same time due to a common cause. For example, a fire in a culvert may cause interruption of electricity, water and telecommunication at the same time. Often, the term geographical dependency is used to explain such failures because one or several elements of the infrastructures are in *close proximity* so that external threats may knock out several infrastructures at the same time.

When categorizing dependency and interdependency, the term *functional interdependency* is used in situations where there are cascading failures, the term *impact interdependency* is used in situations where there are escalating failures and the term *geographical dependency* is used in situations where there are common cause failures.

The term escalating failures is used to describe that the impact of a failure in one system is worsened by a failure of another system reflecting the overall system demand, for example, transportation needs. Such escalating effects may be evident even if the performances of the two systems are *independent*. The structure of the overall system demand will often cause higher load on one system in case of a failure of another system which may increase the probability of failure or reduced performance. The two systems are therefore stochastically dependent, but it cannot be categorized as a common cause failure since there is no common cause that causes the failure of the two systems, and the term escalating failures is also used to express such load dependency between systems.

## References

1. Aven, T. (2003). *Foundations of risk analysis. A knowledge and decision-oriented perspective*. New York: Wiley.
2. Vatn, J. (2012). Can we understand complex systems in terms of risk analysis? *Journal of Risk and Reliability*, 226(3), 346–358.
3. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot: Ashgate Publishing Limited.
4. Zio, E. (2009). Reliability engineering: Old problems and new challenges. *Reliability Engineering and System Safety*, 94, 125–141.
5. McDaniels, T., Chang, S., Cole, D., Mikawoz, J., & Longstaff, H. (2008). Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change*, 18(2), 310–318.
6. Hansson, S. O., & Helgesson, G. (2003). What is stability? *Synthese*, 136, 219–235.
7. DSB (2011). Nasjonal sårbarhets og beredskapsrapport (NSBR) (2011). ISBN: 978-82-7768-246-4. <http://dsb.no/Global/Publikasjoner/2011/Rapport/NSBR2011.pdf> Last visited 2011-10-18.
8. Rinaldi, SM., Peerenboom, JP., Kelly, TK. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25.

Risk and Interdependencies in Critical Infrastructures

A Guideline for Analysis

Hokstad, P.; Utne, I.B.; Vatn, J. (Eds.)

2012, VIII, 252 p., Hardcover

ISBN: 978-1-4471-4660-5