Safety Science 49 (2011) 292–297

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

A risk perspective suitable for resilience engineering

Riana Steen, Terje Aven *

University of Stavanger, Centre of Risk Management and Societal Safety, Stavanger, Norway

ARTICLE INFO

Article history:
Received 14 January 2010
Received in revised form 29 July 2010
Accepted 3 September 2010

Keywords:
Resilience
Risk perspectives
Uncertainties
Vulnerability
Extended risk assessment

ABSTRACT

In recent years, resilience engineering has been given considerable attention among safety researchers and analysts. The area represents a new way of thinking about safety. Whereas conventional risk management approaches are based on hindsight knowledge, failure reporting and risk assessments calculating historical data-based probabilities, resilience engineering looks for ways to enhance the ability of organisations to be resilient in the sense that they recognise, adapt to and absorb variations, changes, disturbances, disruptions and surprises. The implications of this shift in thinking are many. We focus in this paper on the understanding of the risk concept and how risk can be assessed and treated. The traditional ways of looking at risk are not suitable for use in resilience engineering, but other risk perspectives exist. A main purpose of this paper is to draw attention to such perspectives, in particular one category of perspectives where probability is replaced by uncertainty in the definition of risk. We argue that the basic ideas of resilience engineering can be supported by such risk perspectives.

1. Introduction

Resilience engineering has become an important field for the understanding and management of safety in socio-technical systems. Considerable effort has been made in the last years to clarify basic features of resilient systems and develop suitable concepts, principles and methods that can provide the basic building blocks of the field; see for example Nemeth et al. (2009), Dijkstra (2007), Saurin et al. (2008), Hollnagel et al. (2008,2006) and Woods (2000). In many respects, resilience engineering represents an alternative to conventional risk management approaches which are based on hindsight knowledge, failure reporting and risk assessments calculating historical data-based probabilities. The proponents of resilience engineering consider conventional safety management and risk assessment methods to be inadequate for present-day systems (Hollnagel, 2007): "It is a simple fact that whereas technological and socio-technical systems have developed rapidly, and continue to do so, the repertoire of methods to address safety issues has not. There is therefore a clear need for new approaches to risk assessment and safety management, and resilience engineering has been proposed as a solution to satisfy that need." Hollnagel (2007) provides an excellent summary of the resilience engineering approach, and the basic premises and features of the field. For the purpose of the present paper, it is sufficient to draw attention to a few key points (Hollnagel, 2007):

- Many adverse events cannot be attributed to a breakdown or malfunctioning of components and normal system functions ("intractable events"). They are best understood as the result of unexpected combinations of normal performance variability.
- Effective safety management cannot be based on hindsight, nor rely on error tabulation and the calculation of failure probabilities. Safety management must not only be reactive, but also proactive.
- The conventional view on safety (risk) management considers performance variability, of any kind, as a threat and something that should be avoided. The result is often the use of constraining means (in particular for human performance variability) such as barriers, interlocks, rules, procedures and the use of automation.
- In resilience engineering, performance variability is considered both normal and necessary. It is the source of both positive and negative outcomes. Safety cannot be obtained by constraining performance variability, since that would also affect the ability to achieve desired outcomes. The solution is instead to dampen the variability that may lead to negative outcomes and at the same time to reinforce the variability that may lead to positive outcomes.

There are many formal definitions of resilience in a resilience engineering context; see the above-cited references. They capture more or less the same ideas.

Resilience is the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the

* Corresponding author.
E-mail address: terje.aven@uis.no (T. Aven).

0925-7535/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2010.09.003

presence of continuous stress. In order to be resilient, a system or an organisation must have the following four qualities: the ability to

(I) respond to regular and irregular threats in a robust, yet flexible manner,
(II) to monitor what is going on, including its own performance,
(III) to anticipate risks (risk events) and opportunities and
(IV) to learn from experience (Hollnagel, 2007).

As is clear from the above analysis that anticipating what may happen must go beyond the conventional risk assessments. The conventional risk assessments are not considered adequate for analysing socio-technical systems. The conventional approach to risk and safety assumes that systems are tractable (which means that the principles of functioning are known, that descriptions are simple and with few details, and that a system does not change while it is being described), but this not a reasonable assumption today (Hollnagel, 2007).

However, other perspectives on risk exist and in this paper we focus on one category of perspectives which we believe would better support the basic ideas of resilience engineering. It is referred to as the (A, C, U) risk perspective (Aven, 2009; Aven and Renn, 2009a). Here, A represent threats (events), C the consequences of A, and U the associated uncertainties (will an event A occur? what value will C take?). Following this perspective, uncertainty replaces probability in the definition of risk. Uncertainty – and not probability – is the key concept of risk. Probability is a tool used to express uncertainties based on the knowledge available, but it is just a tool, with limitations. The risk assessments need to see beyond the computed probabilities by describing uncertainties more or less "hidden" in the background knowledge that the probabilities are based on. The result is a broad risk description that sees qualitative aspects as equally important as assigned probability figures.

In this paper, we present a new framework based on this risk perspective that provides

1. a structure for linking the concepts of risk and resilience
2. a conceptual basis for resilience engineering

The work aims at strengthening the scientific platform of the risk and safety discipline by providing new insights into the relationship between risk and resilience. For this discipline, as for all other scientific disciplines, it is essential that the conceptual basis is solid. However, the present work is not only of theoretical and foundational interest. The main contribution of the paper is not the definition of the concepts per se, but the structure developed to understand and analyse the related features of risk and resilience in a risk management and resilience engineering context. The analysis of the paper is closely linked to the discussion on the role of risk assessment in the case of safety management for intractable systems.

Before presenting and discussing this framework, we briefly summarise the basic features of the conventional risk perspective and the alternative (A, C, U) type of perspectives.

2. Basic introduction to risk perspectives

Many perspectives on risk exist; see e.g. Aven and Renn (2009a). In this paper, we distinguish between the following two main categories:

1. The main component of risk is probability, and this probability is interpreted as an objective property of the activity being studied. This perspective is referred to as the traditional risk perspective.
2. The main component of risk is uncertainty, and probability is considered a knowledge-based (subjective) tool for expressing these uncertainties. It is acknowledged that risk extends beyond probabilities. This perspective is referred to as the alternative risk perspective.

In the traditional risk perspective, risk is defined by a probability or probability distribution, expressing stochastic (aleatory) uncertainties. A population of similar situations to the one studied are constructed and the probability P of an event A equals the fraction of situations where A occurs. The probability P is unknown and is estimated based on "hard data", i.e. measurements related to the occurrence of A for similar situations. Analogously, we define a probability distribution P_X associated with a random variable X. Modelling of the phenomena may also be used, linking the probability P to a set of parameters q on a more detailed system level. More generally, we may consider the perspective based on a probability model F which is assumed dependent on some unknown parameters μ. The estimation of μ is based on traditional statistical methods, e.g. regression analysis.

Hence, risk is defined by P and P_X, and the associated risk description covers the estimates of these quantities. Uncertainties of these estimates should be addressed, but are often neglected or restricted to simple confidence intervals reflecting only statistical variation.

In the alternative risk perspectives, uncertainty and not probability is the main component of risk. Different definitions of risk can support such a perspective, as discussed in Aven and Renn (2009a) and Aven (2010). In this paper, we focus on the following categories of perspectives (Aven, 2010):

> By risk we understand the two-dimensional combination of
> (i) events A and the consequences of these events C, and
> (ii) the associated uncertainties U (will A occur and what value will C take?) (I)

We refer to this as the (A, C, U) perspective, as already mentioned. We may rephrase this definition by saying that risk associated with an activity is to be understood as (Aven and Renn, 2009a):

> *Uncertainty about and severity of the consequences of an activity* (I′).

Here, severity refers to intensity, size, extension, scope and other potential measures of magnitude and is with respect to something that humans value (lives, the environment, money, etc.). Losses and gains, for example expressed by money or the number of fatalities, are ways of defining the severity of the consequences. The uncertainties relate to the events and consequences; the severity is just a way of characterising the consequences (Aven and Renn, 2009a).

To describe the uncertainties, we use knowledge-based (subjective) probabilities P. If the probability equals 0.1 (say), this means that the assessor compares his/her uncertainty (degree of belief) about the occurrence of the event A with the standard of drawing at random a specific ball from an urn that contains 10 balls (Lindley, 2006). A risk description based on this perspective includes the following elements: (A, C, P, U, K), where A and C refer to identified events and consequences, respectively, and K is the background knowledge (assumptions, etc.) that the description is founded on. The U represents an uncertainty assessment that extends beyond the probabilities, for example a qualitative assessment of uncertainty factors (these factors are mainly a result of assumptions made to determine P) (Aven, 2010).

In this perspective, an objective risk description does not exist. The P part of the risk description covers probability distributions of A and C, as well as predictions of A and C, for example a predictor C^* given by the expected value of C, unconditionally or conditional on the occurrence of A, i.e. $C^* = EC$ or $C^* = E[C|A]$.

The alternative perspective acknowledges that probability is just a tool used to express the uncertainties but is not a "perfect" tool. By restricting risk to the probability assignments alone, we see that aspects of uncertainty and risk are "hidden". There could be a lack of understanding about the underlying phenomena, and strong assumptions may have been made to determine P, but the probability assignments alone are not able to fully describe this status.

3. A conceptual framework for resilience engineering

This section presents the framework announced in Section 1. The basis is the (A, C, U) risk perspective introduced in the previous section. The framework provides a structure for linking the concepts of risk and resilience, as well as a conceptual basis for resilience engineering.

To define resilience, we first introduce the concept of vulnerability (antonym: robustness) (Aven, 2008):

Vulnerability (robustness) = (C, U|A).

In other words, the vulnerability is the two-dimensional combination of consequences C and associated uncertainties U, given the occurrence of an initiating event A. For example, the vulnerability of a person with respect to a certain virus is the potential consequences of this virus and associated uncertainties (what will the consequences be?). The definition of vulnerability follows the same logic as that of risk. The uncertainty of various consequences can be described by means of probabilities, for example for the probability that the person will die from the virus attack. A description of vulnerability thus covers the following elements:

(C, P, U, K|A),

i.e. the possible consequences C, probability P, uncertainty U, and the background knowledge K, given that the initiating event A takes place. In line with Aven and Renn (2009a), we may interpret vulnerability in relation to the event A as uncertainty about and severity of the consequences of an activity given the occurrence of A.

When we say that a system is vulnerable, we mean that the vulnerability is considered high. The point is that we assess the combination of consequences and uncertainty to be high should the initiating event A occur. If we know that the person is already in a weakened state of health prior to the virus attack, we can say that the vulnerability is high. There is a high probability that the patient will die.

Vulnerability is an aspect of risk. Because of this, the vulnerability analysis is a part of the risk analysis. If vulnerability is highlighted in the analysis, we often talk about risk and vulnerability analyses.

Resilience is closely related to the concept of robustness. The key difference is the initiating event A. Robustness and vulnerability relate to the consequences and uncertainties given a fixed A, whereas resilience is open for any type of A, also surprising events. We may get ill due to different types of virus attacks; also new types of viruses may be created. From this idea, we define resilience as

Resilience: (C, U|any A, including new types of A)

and the resilience description:

(C, P, U, K|any A, including new types of A).

Hence, the resilience is considered high if the person has a low probability of dying due to any type of virus attack, also including new types of viruses. Resilience is about the consequences in the case of any "attack" (virus attack) and associated uncertainties. We say that the system is resilient if the resilience is considered high. Of course, in practice we always have to define some boundaries for which A events to allow for.

For all these definitions, the consequences C depend on the performance of barriers (denoted B) (Flage and Aven, 2009), and to explicitly show this we write C = (B, C), resulting in a resilience description (B, C, P, U, K|any A, including new types of A).

The performance of the barrier can be expressed through the capacity of the barrier (and associated uncertainty, probability), for example the strength of a wall. The barriers and the system performance in general are influenced by a number of performance influencing factors (PIFs), for example resources, level of competence, management attitude.

These concepts provide a basis for defining related terms, such as resilience engineering (management):

Resilience engineering (management) is all measures and activities carried out to manage resilience (normally increase resilience).

These measures and activities are based on the PIFs. For example, we may add resources or increase the competence to obtain a higher level of resilience. We may exercise and avoid smoking to increase the resilience in case of an illness.

The above definition of resilience is in line with the one given in Section 1 (Hollnagel, 2007): the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress.

A risk assessment following the (A, C, U) perspective describes risk by (A, C, U, P, K) as explained in Section 2. To ensure that the risk assessment includes the vulnerability and resilience dimensions, we may add that the risk assessment also highlights the descriptions

(C, P, U, K|A) and (C, P, U, K|any A, including new types of A).

We refer to such risk assessments as extended risk assessments. Fig. 1 summarises the main elements of an extended risk assessments. Note that the term "cause" should be interpreted as the

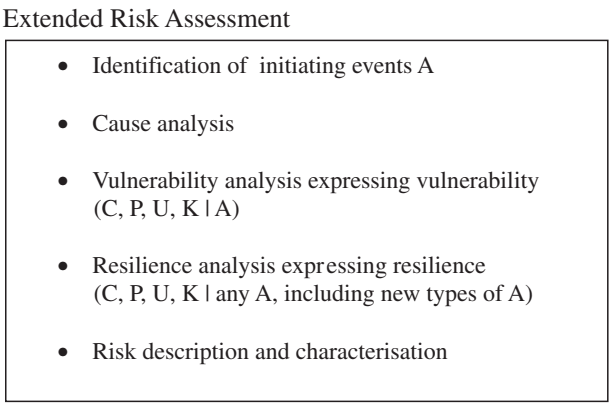

Fig. 1. Main elements of an extended risk assessment.

events and conditions that lead to a specific outcome, here the occurrence of A (Hollnagel, 2004).

Having established this conceptual framework, we need to relate it to practical resilience engineering. How does our framework fit the basic features of the resilience thinking as defined by Hollnagel and others?

4. Discussion: to what extent is an (A, C, U) risk type of risk perspective supporting resilience engineering?

According to Hollnagel (2007), for an organisation or a system to be defined as resilient, it should meet the four features I–IV mentioned in the introduction. The issue we raise in the present section is to what extent an (A, C, U) type of risk perspective and the use of extended risk assessments as described in the previous section can support the process of meeting these criteria, i.e. support the main pillars of resilience engineering.

To illustrate the discussion, we consider an example related to cyber attacks on a railway system. A possible scenario is that attackers use the internet to access a railway control system and cause two trains to collide. Table 1 presents the key concepts introduced in the previous section in the context of this example. A more detailed illustration is provided in Fig. 2. These will be used when we, in the following, review the various elements of an extended risk assessment (see Fig. 1) and discuss to what extent the criteria I–IV can be met. Comments are made on the differences between the (A, C, U) approach and a more traditional statistically based approach.

Table 1
Key definitions interpreted in the context of the example of potential cyber attacks on a railway system.

Concept	Description and definition
Risk	Two-dimensional combination of (i) attacks and their consequences and (ii) associated uncertainties
Vulnerability	Vulnerability related to a specific attack A: two-dimensional combination of (i) the consequences of A and (ii) associated uncertainties
Resilience	Resilience related to any type of attack A: two-dimensional combination of (i) the consequences of the As and (ii) associated uncertainties
Resilience engineering	All measures and activities carried out to manage resilience (normally increase resilience), for example identify and use resources so that the railway system can maintain its functions when an attack occurs
Uncertainty	Epistemic uncertainty, i.e. lack of knowledge about the occurrence of cyber attacks and their consequences
Probability	A knowledge-based (subjective) probability expressing the analyst's uncertainty (likelihood, degree of belief) about unknown quantities (A, C). If a probability is assigned equal to 0.1 (say), it means that the assessor compares his/her uncertainty (likelihood, degree of belief) with randomly drawing one particular ball out of an urn comprising 10 balls

4.1. The various elements of an extended risk analysis

4.1.1. Identification of threats and attack scenarios

For the railway case, attacks can be carried out on hardware systems like computers, servers and communication media, or on software systems covering for example safety programs, system backups and diagnostic programs, and system programs like operating systems and protocols. An example of a scenario is that a terrorist group attacks the railway system by sending viruses on the "train present signal" to make a specific train vanish in the railway system (we refer to this scenario as scenario s).

Different techniques are available for identifying threats and scenarios. Historical data is the traditional one. However, a historical data-based approach would not be sufficient as these would normally not cover all relevant events. This is also emphasised by Hollnagel (2007) who states that anticipating what may happen (criterion III) "must go beyond the classical risk assessment, and consider not only individual events but also how they may combine and affect each other. This is, of course, associated with some uncertainty, but failing to think ahead will inevitably leave a system unprepared, hence more vulnerable." The more we lack data, the

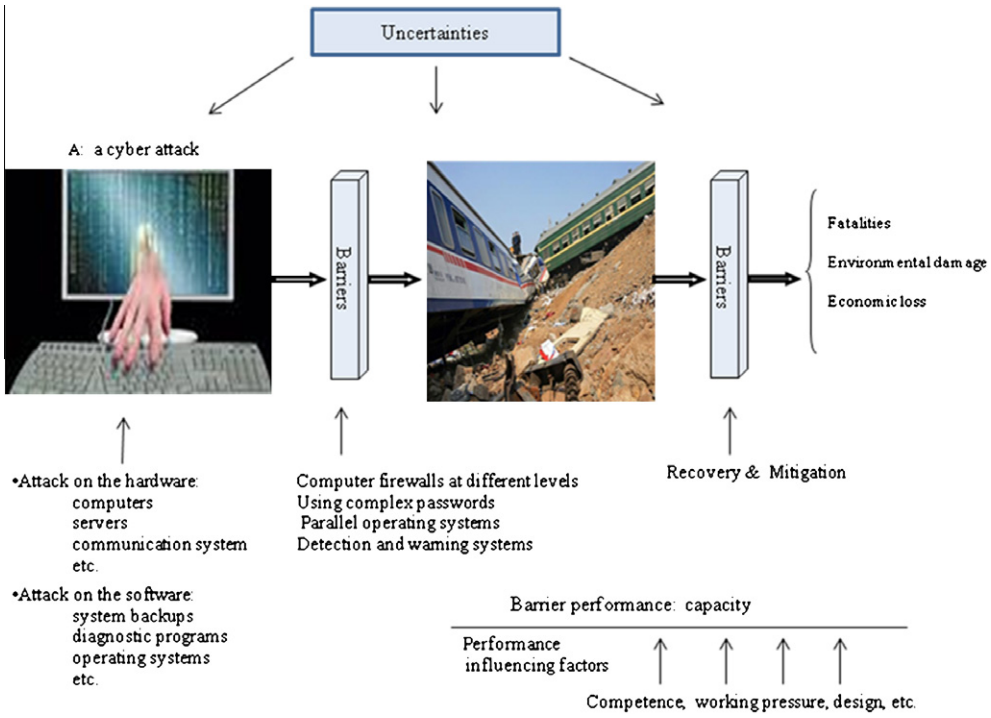

Fig. 2. Illustration of key concepts in the case of a cyber attack on a railway system.

larger need there will be for alternative approaches such as brainstorming and Delphi-type exercises (Aven and Renn, 2009b). An important task is to stimulate the imagination and also come up with attack situations that have not happened before, but have a high degree of plausibility if the context conditions change in the direction of the imagination. A broad set of tools are required, as would be the case when adopting an (A, C, U) type of perspective (Aven and Renn, 2009b).

This analysis element obviously relates to both criteria II (ability to monitor what is going on) and III (ability to anticipate risk events and opportunities in the long run), but also to criterion I (the ability to respond to attacks) as the ability to respond depends strongly on which attacks are identified and followed up.

Concerning criterion IV (ability to learn from experience), Hollnagel (2007) writes "Learning requires more than collecting data from accidents, incidents, and near-misses or building up a company-wide database. Some organisations unfortunately seem to confuse data with experience. But whereas data are relatively easy to amass and can be collected more or less as a routine or procedure, experience requires the investment of considerable effort and time in a more or less continuous fashion." By using a broad approach to this analysis step as indicated above, which extends beyond the historical data, we obtain an improved basis for learning from experience, revealing relevant threats and attack scenarios to be followed up in the vulnerability and resilience analyses.

4.1.2. Cause analysis

The cause analysis is closely related to step 1: identification of threats and attack scenarios, and in many cases no further study is conducted to trace A to specific events and conditions. In this paper, we are mainly concerned about the resilience dimension – attacks may occur and we need to be able to maintain the functioning of the system.

Many different techniques are used in cause analysis, such as fault trees and influence diagrams (Aven, 2008). These techniques provide system insights, and uncertainty/probability/frequency indices can be computed. These indices can be based on generic data or more specific data for the relevant system being studied. However, often data are lacking and expert judgments are required. Recently, a number of methods have been developed which take into account organisational factors, see e.g. I-Risk (Papazoglou et al., 2003), ARAMIS (Duijm and Goossens, 2006), the BORA project (Aven et al., 2006), the SAM approach (Pate-Cornell and Murphy, 1996) and the Hybrid Causal Logic Method (Mohaghegh et al., 2009; Røed et al., 2009).

This analysis element relates to criterion II (ability to monitor what is going on), and to criterion III (ability to anticipate risk events and opportunities in the long run) as the cause analysis may reveal new threats and threat scenarios. It also relates to I and IV as discussed in step 1.

When adopting a more traditional statistically based approach to risk, the cause analysis is typically reduced to a frequency analysis of the identified events A. The quantitative analysis is, to a large extent, based on historical data and consequently such an analysis has a reduced ability to reflect the criteria I–IV.

4.1.3. Vulnerability (consequence analysis) given the occurrence of A

An attack event and scenario A can lead to different consequences C, with respect to, for example, fatalities, environmental damage and economic loss, depending on the existence of barriers and their performance B. Examples of such barriers in our case are computer firewalls at different levels, complex passwords to gain access to the control system, parallel operating systems, and detection and warning systems. The performances of the barriers are influenced by factors such as the competence of the operators, training, operational procedures and time pressure. In the scenario "s" introduced in the analysis step 1, the consequences of a train vanishing in the railway system could be catastrophic if it causes a collision accident (as the Ghotki rail crash on July 13, 2005). However, effective barrier systems (for example "train detectors" in the track sections that can identify specific trains) would keep track of which trains are where within the system and avoid the occurrence of such a consequence.

Many different techniques are used to analyse the vulnerabilities (consequences), and many are based on modelling of the consequences using event trees, fault trees and influence diagrams (Aven, 2008). See also the methods mentioned in the previous step analysing organisational factors. These techniques provide system insights and informative uncertainty/probability/frequency indices as indicated in step 2. For a system in operation as in our railway case, indices (indicators) can be defined reflecting various operational features of the system, such as alarms of different types and procedure violations.

This analysis element relates to criterion I (ability to respond) through the barrier analysis and criterion II (ability to monitor what is going on) through the barrier and consequences indices (indicators) used. To some extent, it also relates to criterion III (ability to anticipate risk events and opportunities) as the consequence analysis may reveal vulnerabilities. The vulnerability analysis is also of course dependent on the ability to learn by experience (criterion IV). For example, it is likely that operators with experience from many attack situations have an increased ability to deal with a new type of attack A.

When adopting a more traditional statistically based approach to risk, the quantitative analysis is, to a large extent, based on historical data and, consequently, also the consequence analysis has reduced ability to reflect the criteria I–IV.

4.1.4. Resilience analysis

Whereas the vulnerability analysis studies the performance of the system given specific events A (cyber attack), the resilience analysis investigates the system without specifying the events As. The focus of the analysis is on how the system works following any type of cyber attack – can key functions and operations be sustained?

The use of models like event trees and fault trees for many types of socio-technical systems could lead to poor predictions as the phenomena are not linear (events develop in a pre-defined sequence). Following a systemic view (Hollnagel, 2004), an accident (in our case the development of undesirable outcomes given an attack, for example a train crash) is due to unexpected combinations of actions rather than action failure, and a non-linear combination of performance variability is a key risk contributor. FRAM (Functional Resonance Analysis Method) is an example of a method based on the systemic view (Hollnagel, 2004). In the analysis, the essential functions of the system are identified and the potential variability is characterised. Then, dependencies (couplings) among the functions are studied through so-called functional resonance which is the detectable "signal" that emerges from the unintended interaction of the weak variability of many "signals".

STAMP is another method based on a similar motivation (Levenson, 2004).

This analysis element relates to criteria I–IV in a similar way as for the vulnerability analysis.

4.2. Risk description and characterisation

The above analyses and findings are summarised, reflecting risk, vulnerability, barrier performance and resilience.

Compared to the traditional approach to risk, the (A, C, U) type of approach is not restricted to historical data – the set of relevant

events (disturbances, stress, etc.) is much larger, which is necessary in order to be proactive and obtain resilience. The traditional approach requires some sort of stability of the activity studied in the sense that we need to construct a very large (in theory infinite) population of similar situations (Section 2) which is not feasible for many socio-technical systems. The systems and activities are unique. In the (A, C, U) type of approach, such populations are not a foundational pillar as in the traditional approach. Also, in the (A, C, U) perspective, we may introduce stochastic models (with parameters) expressing variation in populations of similar units (often referred to as aleatory or stochastic uncertainty). However, such models need to be justified, and if introduced they are to be considered as tools for assessing the uncertainties about A and C. The estimation of the parameters of the models is not the end product of the analysis as in the traditional analysis (Aven, 2003).

A fundamental problem in analysing and characterising risk and resilience for many types of situations, in particular socio-technical systems, is that it is difficult to determine the probabilities; we are unable to give strong arguments for specific probability assignments. Yet, a probability can always be assigned based on the available knowledge. This knowledge changes and so do the probabilities. An extended risk assessment acknowledges this and considers a set of methods, both qualitative and quantitative to reflect this (lack of) knowledge. Addressing uncertainties and knowledge, we obtain a stronger focus on the factors that are important for obtaining resilience (I–IV).

We will argue that an extended risk assessment supports risk management and the resilience engineering better than isolated processes based on resilience analysis alone. The extended processes ensure a broader perspective, link risk, vulnerability and resilience and provide insights from different traditions and perspectives. Methods based on causal chains and event modelling (like event trees) may produce poor predictions in some cases, but still these methods may provide insights and reveal interesting features of the system. They are also simple and easy to understand, which are attractive properties. All models have limitations and constraints, yet they can be useful. In our view, different perspectives are required to obtain safe and resilient systems.

5. Conclusions

In this paper, we have presented a framework which links risk and resilience, and provides a conceptual framework for resilience engineering. The risk perspective adopted means a shift in thinking from probability estimation to uncertainty assessments. To many, this perspective represents a new approach in that it allows for questions to be asked concerning existing knowledge, methods and established "truths". The aim of the risk assessments is to reveal uncertainties and describe them. Such a perspective is completely different from the traditional perspective and is, in our view, more suited for assessing and managing risk and resilience of socio-technical systems. This perspective does not make it easier to take a stand on what is the "right level" of risk, safety and resilience, but the framework is more suitable for risk management and resilience engineering as it allows for and encourages broader knowledge processes, as indicated by the analysis in the previous section. The four criteria defined by Hollnagel (2007) for obtaining a resilient system are far better supported by an (A, C, U) type of perspective compared to a traditional perspective. Of course, the risk perspective per se does not ensure resilience, much more is required, but as we have seen from the discussion in Section 4, the basic ideas of resilience engineering can be supported by the (A, C, U) perspective. The traditional risk assessments based on historical data fail in this regard.

Acknowledgments

The authors are grateful to an anonymous reviewer for his/her useful comments and suggestions to the original version of the paper.

The work has been funded by The Research Council of Norway through the SAMRISK research programmes. The financial support is gratefully acknowledged.

References

Aven, T., Renn, O., 2009a. On risk defined as an event where the outcome is uncertain. Journal of Risk Research 12, 1–11.
Aven, T., Renn, O., 2009b. The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. Risk Analysis 29, 587–600.
Aven, T., 2003. Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective. Wiley, Chichester.
Aven, T., 2008. Risk Analysis. Wiley, New York.
Aven, T., 2009. Perspectives on risk in a decision-making context – review and discussion. Safety Science 47 (6), 798–806.
Aven, T., 2010. On how to define, understand and describe risk. Reliability Engineering and System Safety 95, 623–631.
Aven, T., Hauge, S., Sklet, S., Vinnem, J.E., 2006. Methodology for incorporating human and organizational factors in risk analyses for offshore installations. International Journal of Materials & Structural Reliability 4, 1–14.
Dijkstra, A., 2007. Resilience Engineering and Safety Management Systems in Aviation. Ashgate, Aldershot, UK.
Duijm, N.J., Goossens, L., 2006. Quantifying the influence of safety management on the reliability of safety barriers. Journal of Hazardous Materials 130 (3), 284–292.
Flage, R., Aven, T., 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. Reliability & Risk Analysis: Theory & Applications 2 (13), 9–18.
Ghotki rail crash, 2005. <http://www.en.wikipedia.org/wiki/Ghotki_rail_crash>, (accessed 20.10.2009).
Hollnagel, E., 2004. Barriers and Accident Prevention. Ashgate, Aldershot, UK.
Hollnagel, E., 2007. <http://www.sites.google.com/site/erikhollnagel2/whatisresilienceengineering%3F> (accessed 7.01.2010).
Hollnagel, E., Nemeth, P.C., Dekker, S., 2008. Remaining Sensitive to the Possibility of Failure, Resilience Engineering Perspectives, vol. 1. Ashgate, Aldershot, UK.
Hollnagel, E., Woods, D., Leveson, N., 2006. Resilience Engineering: Concepts and Precepts. Ashgate, UK.
Levenson, N., 2004. A new accident model for engineering safer systems. Safety Science 42 (4), 237–270.
Lindley, D.V., 2006. Understanding Uncertainty. Wiley, Hoboken, N.J.
Mohaghegh, Z., Kazemi, R., Mosleh, A., 2009. Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: a hybrid technique formalization. Reliability Engineering & System Safety 94 (5), 1000–1018.
Nemeth, P.C., Hollnagel, E., Dekker, S., 2009. Preparation and Restoration Resilience Engineering Perspectives, vol. 2. Ashgate, Aldershot, UK.
Papazoglou, I.A., Bellamy, L.J., Hale, A.R., Aneziris, O.N., Post, J.G., Oh, J.I.H., 2003. I-Risk: development of an integrated technical and management risk methodology for chemical installations. Journal of Loss Prevention in the Process Industries 16, 575–591.
Pate-Cornell, M.E., Murphy, D.M., 1996. Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. Reliability Engineering & System Safety 53 (2), 115–126.
Røed, W., Mosleh, A., Aven, T., Vinnem, J.E., 2009. On the use of Hybrid Causal Logic Method in offshore risk analysis. Reliability Engineering & System Safety 94, 445–455.
Saurin, T.A., Formoso, C.T., Cambraia, F.B., 2008. An analysis of construction safety best practices from a cognitive systems engineering perspective. Safety Science 46, 1169–1183.
Woods, D.D., 2000. Lessons from beyond human error: designing for resilience in the face of change and surprise. Design for Safety Workshop, NASA Ames Research Center.