Reliability Engineering and System Safety 167 (2017) 536–543

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

How some types of risk assessments can support resilience analysis and management

Terje Aven

University of Stavanger, Norway

A B S T R A C T

Resilience has become an important concept in safety and risk research and applications. There are many definitions, but the fundamental idea is that resilience has to do with the ability of a system to sustain or restore its functionality and performance following a change in the condition of the system (referred to as an event). Describing or measuring the degree of resilience is challenging as it is not obvious what events should be considered; also unknown types of events occurring need to be taken into account. Considerable efforts have been made to understand and describe the resilience concept and its relationship to risk, and the purpose of the present paper is to contribute to this work by arguing that to analyse and manage resilience, risk considerations and assessments can provide useful input. Resilience management is not depending on risk considerations and assessments to be effective, but could benefit from such considerations and assessments if properly conducted. They need to extend beyond traditional quantitative risk assessments; broader qualitative or semi-quantitative risk considerations and assessments are needed which highlight uncertainties and the knowledge and strength of knowledge that the uncertainty judgments are based on.

1. Introduction

There is a strong and growing literature on resilience, addressing the challenge how we can make a system able to sustain or restore its functionality and performance following a change in the condition of the system (disruption, threat, opportunity) (e.g. [8,12,18,21,22,24,28,31,35,36,41]). In the following such changes are referred to as events. By a system it is understood a collection of elements or components that are forming a unified whole for example organised for a common purpose. The resilience management (engineering) can be conducted without considering risk. For example having redundancy in the system may be an effective resilience management strategy, and it does not require assessing specific events and associated risk, to be implemented. This is the great attraction of resilience management. We do not need to know what type of events that can occur and express their likelihoods as needed in traditional risk assessments. In situations with large uncertainties, this is important as risk assessments then are not able to produce reliable probability estimates. It is of special relevance for complex systems, where it is acknowledged that surprises will occur. Resilience analysis and management are especially suited for confronting unknown and uncertain categories of events, and both quantitative and semi-quantitative approaches for resilience assessment have been proposed (e.g., [11,15–17,30]). Traditional risk assessment is not a part of the methodology used in these studies.

The links between resilience and risk have been discussed by several authors, see e.g. [18], [2], [33] and [32]. The present paper seeks to bring the discussion forward by making a careful study on how risk considerations can support resilience analysis and management. The main aim of the paper is to argue for the thesis that risk assessments can provide useful input to the resilience analysis and management. These assessments are not traditional quantitative risk assessments searching for accurate probability estimates, but broad qualitative assessments of events, recovery (return to the normal condition or state) and uncertainties. The objectives of these assessments are to obtain insights by

i) Making a judgement of the type of events that can occur, what we know and do not know (highlighting key assumptions and justified beliefs).
ii) Making a distinction between known types of events, unknown types of events, and surprising events.
iii) Assessing the probability for these types of events whenever found meaningful (using subjective probabilities or subjective interval probabilities).
iv) Assessing the strength of knowledge supporting these judgements. How can the knowledge be strengthened?
v) Conducting assessments to reveal unknown and surprising events.

Assessing the degree of resilience is difficult. As an example think about the human body. It is commonly considered resilient “in its ability to persevere through infections or trauma. Even through severe disease, critical life functions are sustained and the body recovers, often adapting by developing immunity to further attacks of the same type” [31]. An example of a critical life function is breathing. However, the human

E-mail address: terje.aven@uis.no

http://dx.doi.org/10.1016/j.ress.2017.07.005
Received 16 August 2016; Received in revised form 1 March 2017; Accepted 10 July 2017
Available online 12 July 2017

body can also be considered vulnerable – history has shown that, if medical advances like penicillin had not been made, the consequences of some bacterial infections would have been devastating.

This may suggest a characterisation of the human body as *quite resilient* but not *highly resilient,* but how should we distinguish between quite resilient and highly resilient? Or, in more general terms, how should we measure the degree of resilience?

A number of methods and metrics have been suggested for this purpose; see for example [20], [12] and [23]. Some of these methods and metrics are simple, others very complicated as these papers show. As an illustration of a simple metric, consider the definition by Hashimoto [19], who defines the resilience of a system as the conditional probability of a satisfactory (i.e. non-failure) state in time period $t+1$ given an unsatisfactory state in time t.

Many authors have argued that resilience cannot simply be measured in a single unit metric, for example [18]. According to Haimes, the question "What is the resilience of system x" cannot be answered as it would require knowing whether system x would recover following any attack (event) y (also unknown types of events). What can be done, however, is to study how the system functions – what are the outputs (the consequences) of the system – for any specific inputs (events).

The point made by Haimes is important. We cannot see resilience independently of the events. Say that a system can be subject to two types of events, A_1 and A_2. The system is resilient in relation to event A_1 but not to A_2. Now suppose A_2 will occur with a probability of 0.000001% and A_1 with a probability 0.999999%. Is the system resilient? Yes, with high probability. If we allow for unknown and surprising types of events, we cannot conclude in the same way as there is no basis for making the probability judgements. Haimes' statement on the difficulty of measuring resilience is thus reasonable. We are faced with a basic problem, which events to include in the resilience judgements? With respect to some events, the system considered may have shown itself to be resilient in the sense that it was able to recover and sustain its performance. However, for other events the system may not have shown itself to be resilient, and when facing the future it may turn out that the system will also experience recovering problems when faced with other events, of known or unknown type.

As the above redundancy example indicates, we can still perform effective resilience management without the need for quantifying or expressing probabilities. We know that resilience can be improved in many ways – key instruments are strengthening of structures and processes within the system to defend it against events (like the immune system of the body), diversification, flexible response options, and the improvement of conditions for emergency management and system adaptation [35]. We do not need to identify all possible events and assess their likelihoods to understand that a specific resilience arrangement or measure will be useful in many situations. However, there is a need for ways of describing and comparing the resilience for alternative arrangements and measures. Resource limitations mean that we have to prioritise – where should we improve the resilience? There could be a huge number of areas in which the resilience can be improved, but which should be selected and given weight? Many resilience metrics exist as mentioned above, but what events will in fact occur? For the above example with the two events A_1 and A_2, we can think of a specific arrangement that could significantly improve the resilience with respect to event A_2, but its effect on risk (interpreted in a wide sense) could be marginal. The arrangement could still be justified, but some type of considerations of risk seem useful, also in the case that we have difficulties in assessing likelihoods and being accurate on what type of events that will occur, as we always need to make prioritisations. The question is rather how can we make these considerations of risk informative? The present paper provides some ideas and guidance on how to think in relation to this challenge.

The present paper argues that resilience analysis can benefit from recent risk analysis developments which highlight the knowledge and strength of knowledge judgments supporting the probability judgments. Subjective probabilities (and subjective interval probabilities) can always be assigned and used, even if the uncertainties are large – however, they should be supplemented with strength of knowledge judgments. The idea is that any probability judgment is conditional on some knowledge and this knowledge could be more or less strong, and even erroneous, and the risk assessment needs to take this into account (refer to Appendix for details). In the same way the paper argues that the resilience analysis needs to incorporate such judgements in their analyses.

Risk assessment and management supplement resilience analysis and management by addressing the potential occurrences of events. Through such analysis new insights may be gained, for example, unknown and potentially surprising types of events could be identified, and new "cause-effect" relationships can be revealed. Concrete and more effective measures can then be developed to meet these events. By studying why certain infections occur, more effective measures can be developed than if the focus is limited to how to make the body withstand infections in general. When using the term resilience analysis it is referred to all type of activities with the purpose of understanding and characterising the resilience (including understanding how the system performs when subject to specific events), whereas resilience management captures all activities conducted to change (normally to improve) the resilience, for example the implementation of a measure to strengthen the resilience.

When studying resilience we may distinguish between being resilient and performing resiliently, in the same way as distinguishing between being safe and performing safely. In the present paper we talk about the system being resilient but the discussion also applies to the system performing resiliently, for example when considering the operation of a system.

The paper is organised as follows. In the coming Section 2 the meaning of key risk and resilience related concepts are clarified. We use the recent conceptual ideas and definitions from the Society for Risk Analysis [37] as the basis for this analysis. Then two examples to illustrate the analysis are presented (Section 3), covering a safety and a security application, respectively. Section 4 follows up the previous sections with some further discussion on the link between resilience and risk, and the final Section 5 provides some conclusions. The Appendix presents some fundamental ideas about probability, which are useful for the discussion in the coming sections.

2. Understanding resilience and risk

We consider a future activity (interpreted in a wide sense to also cover, for example, natural phenomena) and are concerned about the consequences (effects, implications) C of this activity with respect to something that humans value. The consequences are often seen in relation to some reference values (objectives, planned values, etc.), and the focus is often on negative, undesirable consequences. Concrete examples of C are the number of fatalities and deviations from a specified objective.

The activity could be the operation of a system, for example a technical system or the human body of an individual, or a defined population of human beings during a specific period of time.

The risk of the future activity is associated with C, the consequences of the activity, and related uncertainties U [37]. We may think of a population of human beings subject to a type of disease during a specific period of time – C is the consequences of this disease for the people of this population, and U, the associated uncertainties: what will C be? C could be zero people affected by this disease, one person ill, one fatality, two people ill, two fatalities, etc. Today, before the activity is "run", C is uncertain, unknown. We write risk = (C,U). When we would like to highlight the occurrence of events A preceding C, we write (A,C,U). An example of A in the above human body example is "attract a disease" . To describe or characterise the risk, we need to specify A and C, and use a measure (interpreted in a wide sense) of the uncertainties, as will be illustrated by the examples studied in the coming sections. The common uncertainty measure is probability, but it should be supplemented with