Reliability Engineering and System Safety 145 (2016) 215–220

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Ignoring scenarios in risk assessments: Understanding the issue and improving current practice

Terje Aven *

University of Stavanger, Norway

ARTICLE INFO

Article history:
Received 3 March 2015
Received in revised form
16 August 2015
Accepted 21 August 2015
Available online 29 August 2015

Keywords:
Risk assessment
Scenarios
Events
Probability

ABSTRACT

In risk assessment we are typically faced with a huge number of potential scenarios and events, and in practise some of these are ignored, either because they are not identified or because of judged low probability. However, a scenario or an event may occur despite being extremely unlikely. Considering a large population of such scenarios and events, the occurrence probability is not necessarily negligible. In this paper we take a closer look at this challenge, the main aim being to clarify the issue and provide some recommendation on how to best handle it in practise. A main conclusion is that the risk assessment should be placed in a sufficiently broad framework, ensuring that the outcome and main event spaces are complete, and sufficient focus is placed on the hypotheses and assumptions supporting the detailed scenarios that are identified.

1. Introduction

We are often surprised when a specific scenario occurs; we meet a person, John, on holiday whom we have not seen for 20 years, or an accident occurs where we experience a combination of conditions and events that is considered so unlikely. Think about the Deepwater Horizon accident. Here this combination can be summarised as [16]:

- Erroneous assessments of the results of pressure tests.
- Failure to identify that the formation fluid penetrated the well, in spite of the fact that log data showed that this was the case.
- The diverter system was unable to divert gas.
- The cutting valve (Blind Shear Ram, BSR) in the Blow Out Preventer (BOP) did not seal the well.

If a judgement of this set of events had been made before the accident, an extremely low probability would have been assigned. Yet it occurred. Is the explanation that this is just "one out of a million" scenarios that could occur and before the accident all these scenarios were possible? It may not be surprising that one of these scenarios occurs, when we do not specify which of them. Aristotle (384–322 BC) pointed to this phenomenon more than two thousand years ago when stating that "it is probable that improbable things *will* happen". As we know from probability calculus, the probability of a union of a set of disjoint events is the sum of the probabilities of these events. The occurrence of one event in a population may be quite likely even if the probabilities for each event, seen separately, could be very low. If you select a person you know before your holiday it would not be probable that you would meet him or her, but if your event of consideration is any person you know, it may not be so unlikely that this event actually occurs.

A main task in risk assessment is to identify scenarios that may occur and assess the risk related to their occurrences. The number of scenarios could be very large and not all are considered for further analysis. Broadly we can distinguish between the following categories of scenarios:

a. Not identified (an unknown unknown, i.e. a type of event that is not known; or an unknown known, i.e. an event type known by some but not by the analysts conducting this risk assessment).
b. An identified scenario, and included in the risk assessment – its likelihood and risk are assessed, the scenario is followed up and measures to meet it are discussed.
c. An identified scenario, and included in the risk assessment – its likelihood and risk are assessed and found negligible. The scenario is not further studied.

But on what basis should we determine what is a negligible probability or risk related to a scenario? As discussed above for the Deepwater Horizon and holiday examples, we need to be careful in removing scenarios on the basis of isolated risk and probability judgements. Very unlikely events may occur.

This discussion is closely related to the concepts of common causes and special causes referred to in the quality discourse [20,21,5,6]. These two concepts refer, respectively, to variation that

* Tel.: +47 832267; fax: +47 51831750.
E-mail address: terje.aven@uis.no

http://dx.doi.org/10.1016/j.ress.2015.08.012

is predictable in the view of the historical experience base and to variation that is unpredictable and outside the historical experience base (it always comes as a surprise).

This paper discusses this issue – ignoring scenarios in risk assessments. The topic has been addressed by many scholars, from Aristotle to researchers in statistics, quality management and risk assessments, see e.g. March and Shapira [12], Klinke and Renn [10] and Metzger [14], in addition to the references mentioned above. Of special interest here is the concept "completeness uncertainty" discussed in the probabilistic risk assessment (PRA) community, and in particular in nuclear contexts. Completeness uncertainty relates to risk contributors that are not accounted for in the PRA model; it may be categorized as either being known, but not included in the PRA model, or unknown [17]. Examples of sources of these types of incompleteness include the following [17]:

- The scope of the PRA does not include some classes of initiating events, hazards, modes of operation, or component failure modes.
- The level of analysis may have omitted phenomena, failure mechanisms, or other factors because their relative contribution is believed to be negligible.
- Some phenomena or failure mechanisms may be omitted because their potential existence has not been recognized or no agreement exists on how a PRA should address certain effects, such as the effects on risk resulting from ageing.

We build on this literature, aiming at bringing new insights to the topic by

- Reflecting on different types of formulations of scenarios and events. The more detailed a scenario is specified, the more unlikely it is.
- The link between judgements of "negligibility" and overall decision criteria and judgements. We see beyond the traditional criteria in the form of probability based tolerability and acceptance criteria, to also take into account considerations of the strength of knowledge on which the probability judgements are based.
- Precision regarding what probability (likelihood) and risk mean in this context. Meaningful discussions of what are negligible probability and risk require that these concepts are clearly defined and interpreted.

In the coming section we present a general set-up for explaining the problem of ignoring events and scenarios in risk assessment. A simple example is used to illustrate the ideas. Then in Section 3 we explain and discuss in more detail what ignoring events and scenarios means in practise, using the example as an illustration. In this section we also point to and discuss the main challenges we face in this process. Then in Section 4 we provide a guideline on how to improve the foundation and practise of risk analysis in this area. Finally, Section 5 provides some conclusions.

2. A formal set-up

We consider a future activity (interpreted in a wide sense to also cover events such as natural phenomena), for example the operation of a system, and focus on the consequences of this activity with respect to something that humans value. We may for instance have a special interest in a type of events that may occur, such as undesirable events linked to humans' health. Let A be the event occurring. In the oil and gas example presented in the introduction section, A may for example be a major gas leakage leading to some fatalities. In the holiday example, A could be meeting our friend John.

In the risk assessment we specify a set of events that we believe could occur. Let us call this set $A'=\{A_1',A_2', \ldots\}$. The assessment may have a scope and restrict attention to some specific categories of events, for example only events that have the potential to lead to fatalities, or events that are actually defined by the number of lost lives. The sets may for example be like this:

$$A' = \{\text{Uncontrolled discharges of hydrocarbons and fires, including process leaks, well incidents/shallow gas and riser leaks; Structural integrity related incidents such as structural damage, and collisions; Work accidents}\} \quad (2.1)$$

$$A'' = \{0 \text{ fatalities}, \ 1 \text{ fatality}, \ 2 \text{ fatalities}, \ 3 \text{ fatalities}, \ \ldots\} \quad (2.2)$$

In the holiday example the sets could be

$$A' = \{\text{John}, \ \text{Filip}, \ \text{Frank}, \ \text{Lisa}, \ \ldots, \ \text{Jan}\} \quad (2.3)$$

$$A'' = \{\text{relatives}, \ \text{friends}, \ \text{colleagues}, \ \text{others}\} \quad (2.4)$$

These two sets A′ and A′′ are just two sets of events, there is no special meaning attached to the superscript ′ and ′′.

We observe that the actual event occurring may or may not be captured by the specified sets of the risk assessment, A′ and A′′. In the oil and gas example, A′′ defined by formula (2.2) would necessarily include the actual fatality number, but A′ defined by formula (2.1) could lack some events, for example a loss of life due to some heavy storms (man overboard). In the holiday example, we have a similar situation as the name identified may not cover the actual one met, but using the categorisation A′′ (formula (2.4)), all possibilities are necessarily covered.

The use of A′ leads to incompleteness as the specified values are to be considered a model of the real life, and this model has limitations. In the coming discussion, models will play an important role with their link between output quantities (events) and input quantities (events) that together generate more or less detailed scenarios.

Let y denote a risk description (metric) used in the risk assessment (for example the set of events A′ and A′′ with associated assigned probabilities), and let x be a vector of parameters of the total model f used for deriving y. Hence we can write

$$y = f(x). \quad (2.5)$$

As an illustration, consider the example in Fig. 1, linked to the oil and gas case. The model is an event tree with initiating event "major gas leakage" and two branching events: B: ignition and C: explosion. Depending on these events and other factors not explicitly modelled, the outcome is 2, 1 or 0 fatalities.

If A, B and C occur, the number of fatalities (denoted Z) is either 2, 1 or 0, with some probabilities assigned by the risk analysts. If A, B and Not C occur, Z is either 1 or 0, with some assigned probabilities. And If A and Not B occur, Z is equal to 0.

The model provides a link between the event "gas leakage" (A_1') and the number of fatalities (Z and A′′). There is a potential difference between what the model expresses and what the actual quantities and events are if the activity would had been realised; this difference we refer to as the model error. To study the magnitude and importance of this error we need to be precise on the meaning of the probabilities and the use of the assessment in a decision-making context.

First some words about the likelihood dimension. To calculate the probability of two fatalities using this model we use a simple approximation formula, based on conditional probabilities: