Reliability Engineering and System Safety 156 (2016) 203–209

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM

Torbjørn Bjerga [a,*], Terje Aven [a], Enrico Zio [b]

[a] University of Stavanger, Norway
[b] Ecole Central Paris, France, Politechnico di Milano, Italy

ARTICLE INFO

Article history:
Received 28 October 2015
Received in revised form
10 August 2016
Accepted 12 August 2016
Available online 18 August 2016

Keywords:
Complex systems
Uncertainty
Risk analysis
FRAM
STAMP

ABSTRACT

Several approaches to systems thinking have been proposed to understand and model complex socio-technical systems and potential accidents, including the System-Theoretic Accident Model and Processes (STAMP) with the associated hazard analysis method System Theoretic Process Analysis (STPA), and the Functional Resonance Analysis Method (FRAM). It is argued that these approaches are suitable for the risk analysis of complex socio-technical systems. The purpose of this paper is to look more closely into this thesis, with a special focus on the treatment of uncertainty and potential surprises linked to the operation of such systems. A key finding is that these approaches may, indeed, reduce the potential for surprises by increasing the system and risk understanding but need to be supplemented with other approaches to adequately support the decision-making on risk issues.

1. Introduction

A major contemporary issue for risk analysts and managers is how to deal with unexpected potential accidents (or more broadly, 'unintended consequences') in complex systems, such as the power grid and the financial system. Such complex systems are affected by pervasive uncertainty, which may lead to surprising behavior; see for example Meadows [39], Helbing [20] and McDaniel and Driebe [38].

An underlying characteristic of complex systems, as defined by for example Ottino [43], Dulac [17], Mitchell [41], Perrow [45], Weaver [53] and Johansen and Rausand [27], is that such systems do not allow the understanding of the system logic and the prediction of the system behavior based on the understanding and prediction of the behavior of its components.

A potential accident in a complex system cannot, then, be adequately predicted by looking at the series of component failures (event chains) that may occur [32,33]. Such a view of accidents as event chains is a key idea in traditional risk analysis tools, e.g. the Domino model [19], the Swiss cheese model [47], and related techniques such as Failure Mode and Effect Analysis (FMEA), fault trees and event trees.

An important issue with modeling accidents using event chains is that dependencies (interactions) among components are not adequately taken into account. These dependencies can be of linear but also non-linear nature and may contribute to escalating systemic consequences. To illustrate, consider a financial crisis. Banks are one type of component in the financial system. One bank associated with escalating the 2007–8 US subprime mortgage crisis into a global financial crisis is Lehman Brothers when filing for bankruptcy in 2008 [40]. The consequences when Lehman failed extended far beyond Lehman's financial value or the many Lehman employees losing their jobs. The effects cascaded throughout the worldwide financial system, bringing it to its knees and spreading to other major sectors like the car industry. The banks are all tightly connected in large and intricate networks of dependency, with interdependency links to other sectors.

Various approaches have been proposed in the literature to try to meet the challenges of complex system risk analysis; see for example Rasmussen [46], Apostolakis and Lemon [2], Brown et al. [13], Mohaghegh and Mosleh [42], Kröger and Zio [30], Hollnagel et al. [25], Leveson [33] and Hollnagel [23]. In this paper the focus is on two main current approaches, the:

- Functional Resonance Accident Model/Functional Resonance Analysis Method (FRAM) [22,23], referred to as 'the FRAM approach', and the
- System Theoretic Accident Model and Processes (STAMP) with the associated hazard analysis method System Theoretic Process Analysis (STPA) [32,33], here referred to as 'the STAMP approach'.

* Corresponding author.
E-mail address: torbjorn.bjerga@uis.no (T. Bjerga).

http://dx.doi.org/10.1016/j.ress.2016.08.004
0951-8320/

Both of these approaches give attention to dependencies, and aim to cover a range of system aspects, such as of technical and social character. Indeed, the analysis methods FRAM and STPA produce potential accident scenarios and hazards that extend beyond more traditional tools; cf. Leveson [33], Leveson et al. [35], Hollnagel [24], Ishimatsu et al. [26], Belmonte et al. [10], Song [49] and Rosa et al. [48].

The FRAM and STAMP approaches have been complementary to more traditional risk analysis approaches [10,29], and in the planning and execution processes for various complex systems and operations. As will be made clear though, the approaches architects, Leveson and Hollnagel, are very dismissive of the use of probabilities in relation to complex-socio technical systems [23,33,34]. Traditionally, probability has been a cornerstone in risk analysis [28], but many researches along with Leveson and Hollnagel acknowledge challenges and limitations on its use, see for example Aven and Zio [7].

However, from a decision-maker's perspective one might ask: 'which of the identified accident scenarios is more likely? Are there uncertainties? Can we have surprises? ' Some judgments have to be made during the analysis on what is likely and what is less likely. The STAMP and FRAM approaches can imply not resorting to probability, but is this a sound judgment, and what is the alternative proposed? It can be gathered that the alternative advocated in these two approaches is to focus on understanding and identification of potential accidents (and remedies) in complex systems. The claim is that a better model and more comprehensive list of systemic accidents is what matters to better understand the system and, thus, prevent failures and surprises. However, limiting the use of probabilities and focusing only on the model of systemic behavior and accidents does not entirely eliminate uncertainties, nor does it avoid the fact that surprises may still occur.

This paper discusses the use (or abandonment) of probability in the FRAM and STAMP approaches and more generally how uncertainties and potential surprises are treated. The thesis is that the FRAM and STAMP approaches may reduce the surprise potential and uncertainty in complex systems, but some degree of it still remains and is not adequately handled in the analysis nor communicated to a decision maker in current practice.

The remainder of this paper is structured in the following way. Section 2 presents briefly the FRAM and STPA methods. Section 3 investigates the use/abandonment of probability in the FRAM and STAMP approaches. Section 4 discusses the findings and recommends some possible improvements. Section 5 concludes the paper.

2. The FRAM and STAMP approaches

To explain the FRAM and STAMP approaches we will look into an expedient risk analysis case involving a complex system. The case is constructed, and can be considered fictive, but is inspired by a major disturbance in the European electrical grid that took place in 2006, c.f. UCTE [51] and Castle [14]. The setting is as follows.

A large ship sailing down a river has to pass under a transmission line mounted on two pylons on each side of the river. There is little clearance between the line and the ship, and there is obvious risk associated with the high voltage current. Therefore, the line has to be switched off, while the ship is passing underneath. The captain has to request the switch-off prior to passage and also inform the controller about when the ship is in the clear. The controller of the line, responsible for the off- and on-switching, relies on a technical switchboard and technical sensors signaling the status of the line. The case involves different human/organizational and technical elements (and also natural elements) and dependencies between the elements.

Before introducing the two approaches, it is in place to say that even though they are both used in relation to risk analysis of complex systems, there are some key overall differences. FRAM can be considered a method to develop a model of the system and system behavior, including potential accidents, while STAMP is a generic accident model that can be used for analyzing potential accidents using the hazard analysis method STPA, c.f. Hollnagel [23]. Note also that the two approaches can be used for accident analysis (ex-post), though the attention here is a risk analysis context (ex-ante).

2.1. FRAM

The key elements of FRAM used for risk analysis are [23]:

1. Identify and describe essential system functions
2. Assess variability for each function
3. Assess how the variability of multiple functions can be coupled and lead to non-linear outcomes (what is referred to as functional resonance).
4. Identify countermeasures

Step 1 of the method essentially provides a qualitative, textual model of the system in question and how it operates in a daily ('accident free') manner. The model is constructed around the concept of 'functions' (rather than components). In the FRAM analysis for the case considered, transmission of electricity is one function, provided by the transmission lines, and control of the transmission is another function, provided by the line operator. Dependencies between the functions are referred to as 'couplings' in the FRAM world. Couplings are not fixed in the model, i.e. there can be many ways in which the functions can couple under given circumstances. Nevertheless, usual couplings in daily operations are made visible, for example information-couplings and control-action-couplings between the transmission of electricity and its operation. The model can be illustrated as in Fig. 1. Hexagons illustrate functions, lines illustrate couplings.

In steps 2 and 3, functional variability is central, including the sources and outcomes of this variability, and how multiple functions' variability can be coupled (non-linearly) and cause an accident. Functional (performance) variability, in particular for humans and organizations, is smooth adjustments that aim to deal

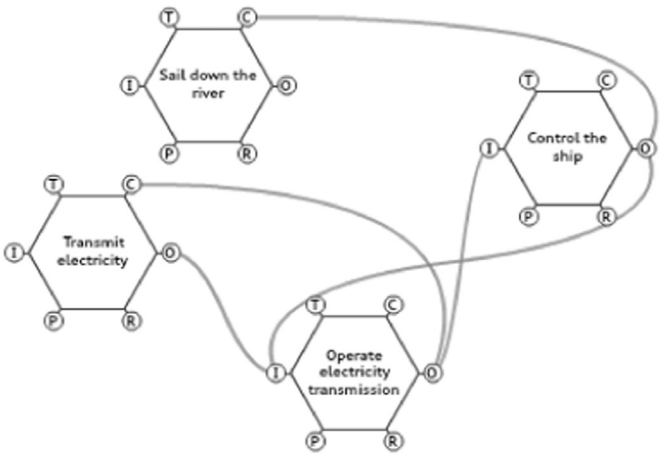

Fig. 1. Illustration of the FRAM model (in case of an accident there will be a coupling between sailing (function embedded in the ship) and the transmission of electricity (function embedded in the transmission line)). Built using the free software: FRAM Model Visualizer. T: time, P: preconditions, I: input, R: resources, O: output and C: control.

with every day challenges in a complex world [23]. These adjustments can sometimes be well intended to ensure safety and reliable deliveries, but there will be uncertainties about the outcomes of such adjustments, and sometimes, despite good intentions, the very source for why things goes wrong.

For each of the functions in our case there can be variability, and for many different reasons. For example, for the control-the-ship-function, the captain can be late in requesting a switch-off due to sleep deprivation. The electricity-transmission-operation-function can miss responding to the request when there is stress and competing tasks. For the electricity-transmission-function, a sensor can indicate that the line is off when it is not, due to technical failure under high loads. High loads can also mean that the lines are sagging. Now, each of these variabilities may not be an issue by themselves, these are just 'normal' variations, but occurring simultaneously they can produce excessive variability and an accident.

Step 3 investigates potential realistic accident scenarios, called instantiations, as excessive coupled variability under some realistically assumed conditions (e.g. high loads) and realistically assumed individual variability (e.g. sagging). Changing assumed conditions and variability will give different instantiations. The future occurrence of a specified instantiation is however uncertain. What are realistic/likely conditions and variability assumptions is based on a wider knowledge base, including understanding of the system and the situation in hand, and experience with similar systems. The method (FRAM) produces a model of the system and specific potential systemic accident scenarios (instantiations). This model and scenarios, along with countermeasures, can be presented to the decision maker.

2.2. STPA

STPA analysis has the following structure (based on Leveson [33], and Leveson et al. [35]):

1. Identify the accidents to be considered, the system level hazards, safety constraints and functional requirements
2. Create a model of the functional control structure for the system in question
3. Identify the potential unsafe control actions (unsafe control of the system)
4. Determine how each potentially hazardous control action from step 3 could occur, i.e. the scenarios leading to unsafe control

To exemplify, we return to the risk analysis case considered. In step 1, we can identify that the high voltage line represents a system hazard to the ship. Therefore, the safety constraint is that the transmission line be switched off before passage. An accident can occur if this safety constraint is not upheld. The next steps essentially revolve around the safety constraint and how it can fail to be upheld. To investigate this, the control structure of the system is derived in step 2. Fig. 2 is a simple illustration of the control structure for the high voltage line in this case. Dependencies are illustrated by lines.

Step 3 is to identify potential inadequate control actions that could lead to hazardous states. Four generic types of hazardous states can occur [33]:

1. Control action not provided or not followed
2. An unsafe control action is provided
3. A potentially safe control action is provided too late or too early or in wrong sequence
4. A control action is stopped too soon or applied too long

Table 1 below illustrates the control action of switching the transmission line on and off, and when it becomes unsafe.

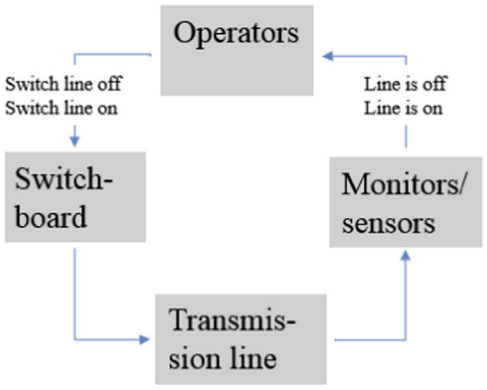

Fig. 2. Control structure diagram.

Step 4 is to identify further how potentially hazardous control actions can occur, i.e. identify the causes. For each hazardous control action, the control loop in Fig. 3 is circled; compare with the similar control structure in Fig. 2. Many of the generic causes depicted in Fig. 3 are relevant to, say, the unsafe control action: 'line-switch on while ship is underneath'. Under point 3 in the Figure, we can identify 'feedback delays' and 'incorrect process models' as relevant causes of an unsafe line switch-off. In step 4, considerations should also be made for how controls could degrade over time (cf. Dekker [15]), but the time span in the example is too short for it to be considered here.

The result of the analysis is essentially a list bearing scenarios of hazardous control actions, conditions for when they become unsafe, and causes of these hazards (potentially accompanied by judgments on, for example, severity and mitigation potential). The list can be used to suggest and evaluate mitigating measures. In last instance, the list including mitigating measures is handed over to the decision maker.

3. Probability and uncertainty in FRAM and STAMP

Section 2 recalled briefly the FRAM and STAMP (STPA) approaches, with reference to the risk analysis case above defined. Central in both approaches are models of the system and potential accidents. A key output provided by the application of these methods is potential accident scenarios/hazards, which can be presented to a decision maker. But how likely (uncertain) are the scenarios? A list/model of scenarios or hazards in itself indicates little on this matter, though some likelihood judgments are inevitably made, in the decision process, on which scenarios to consider. The information about uncertainty should be conveyed to the decision maker. The information can be useful for deciding how to prioritize scenarios to consider, and how much of the resources should be spent to prevent some scenarios or hazards. In risk analysis, it is usual to resort to probabilities to say something about the uncertainty linked to scenarios and hazards. However, the STAMP and FRAM approaches largely exclude the use of probability.

Indeed, STAMP/STPA's architect and proponent, Leveson, is very skeptical regarding the use of probabilities in relation to complex systems, largely because of uncertainties (for example when going to Mars), and biases:

> "While severity can usually be evaluated using the worst possible consequences of that hazard, likelihood is almost always unknown and arguably, unknowable for complex systems…" ([33], p.320).

Table 1
Hazardous system behavior.

Control action	Not providing	Providing	Too early, too late, or out of order	Stopped too soon or applied too long
Switch line off	While ship is underneath	Not hazardous	Too late: While ship is underneath	Too soon: While ship is underneath
Switch line on	Not hazardous	While ship is underneath	Too early: While ship is underneath	Too long: While ship is underneath

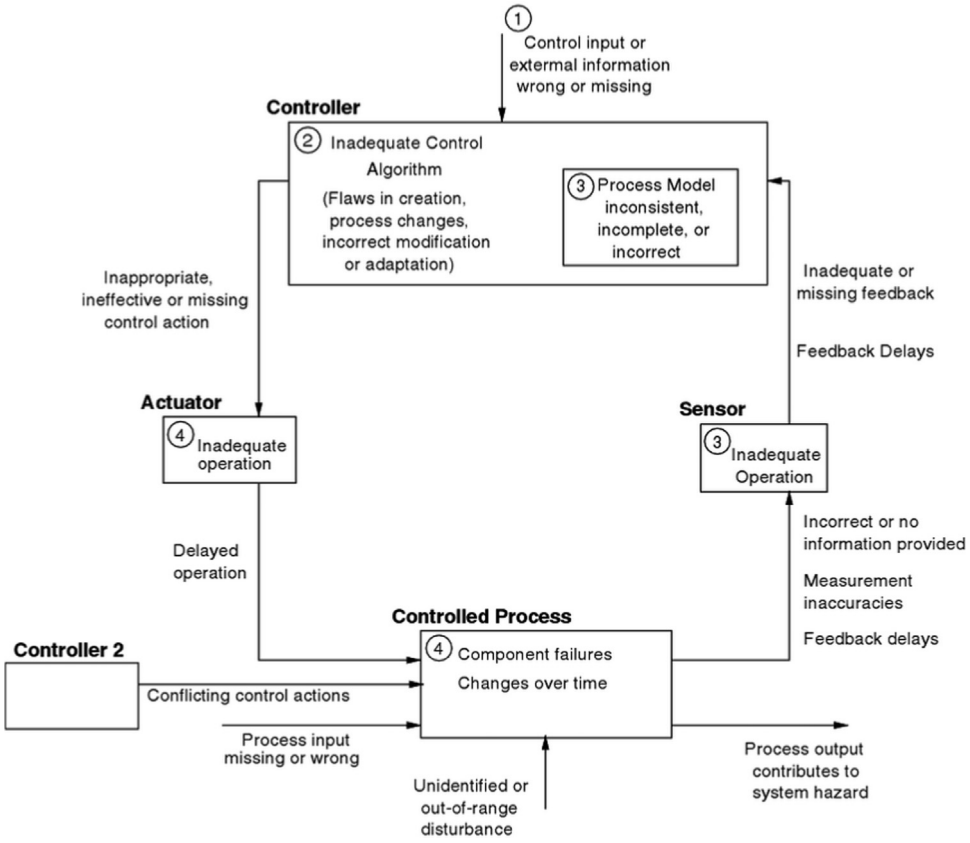

Fig. 3. Causal factors leading to hazards [32].

Further down Leveson states:

> "There are no known or accepted rigorous or scientific ways to obtain probabilistic or even subjective likelihood information using historical data or analysis in the case of non-random failure and system design errors… When forced to come up with such evaluations, engineering judgment is usually used, which in most cases amount to pulling numbers out of the air, often influenced by political or nontechnical factors" ([33], p.320).

Leveson's practical conclusion is that, in many cases, one should abandon probability altogether and rather focus on the understanding of accidents and use, for example, severity and mitigation potential for decision support [33].

As for FRAM, one motivation for its development stems from the claimed inadequacy of many Probabilistic Risk Assessments (PRAs) and Human Reliability Assessments (HRAs) for analyzing human errors and computing human error probabilities (HEPs). Many technical components can be viewed as performing in a stable manner and with fixed dependencies among components. Many components can be adequately represented as in a state of failure or not, and probabilities for each of the states can be calculated. However, humans and organizations do not usually fail as such, nor perform in a stable manner, or have fixed relations. Rather, there is continuous performance variability to adapt to a changing environment. The purpose of FRAM is to represent the performance variability of the system rather than to calculate some failure probability [23].

In FRAM, variability is described using qualitative descriptions, including qualitative likelihood judgments on variability outcomes:

> "There is no established tradition for [expressing variability quantitatively] in PRA or HRA, which at best supply probabilities with uncertainty intervals (lower and upper bounds). An uncertainty interval is however an expression of range rather than variability" ([23], pp.93–94).

Hollnagel's conclusion is essentially that it is inappropriate to talk about human error; hence, human error probability and quantification of likelihood (probability) may also not be useful in the FRAM world.

We will argue that both Leveson and Hollnagel have some valid points concerning probabilities and issues linked to their use in risk analysis of complex systems [8,56]; yet, their practical conclusion of effectively abandoning probability is not sound, as the consequence can be that important aspects of risk and uncertainty are ignored, thus leading to poor decision-making.

To elaborate further, we need to indulge in the use and meaning of probability, which has different schools. It is possible to distinguish between probabilities used to:

i. Describe variation in large populations (thought constructed or real)
ii. Represent uncertainty, also about variation (i.) and performance variability

Variation (in a large population of similar constituents) is often referred to as stochastic/aleatory/irreducible uncertainty, and uncertainty as epistemic/reducible uncertainty in a risk context. The distinction is, however, instrumental; all uncertainty is epistemic and reducible [1,54]. In a risk assessment, there are essentially two ways to understand a probability: as a frequentist probability or as a subjective (knowledge-based, judgmental) probability [3]. These are linked to variation and uncertainty, respectively.

Note that variability and variation are two closely linked terms. For example when searching for 'variability' in the Merriam-Webster dictionary, it returns 'variable' and defines it as 'able or apt to vary: subject to variation or changes <variable winds> <variable costs>[52]'. The outcome of a dice throw, or the performance of technical tools and equipment is subject to variation, so is also human and organizational behavior. A sharp distinction can however be made, on the variation in a large population of similar constituents with known outcome space, and variation of a more rare/unique, and often unprecedented character. Typically, repeated dice throws is an example of the former, and relative fractions representing the variation can be established for the different outcomes (1-6 pips). For other cases, for example human performance, it can be much more difficult to specify in advance all the performance outcomes, and to establish accurate fractions for different performances.

A frequentist probability $P_f(A)$ is the fraction of times an event/outcome A occurs if the experiment is repeated a huge number of times under similar conditions (e.g. dice throws). Usually the fraction $P_f(A)$, is unknown and must be estimated (as noted in Leveson [33], referring to the fraction as likelihood). The estimate can be hard to justify when there is little relevant data, as is the case when going to Mars.

Frequentist probability models can be used to model variation in complex systems, at both the component level and the system level. See e.g. Hines et al. [21] and Lewis [36] for the latter. Variation can be illustrated, for example in the number of outages of a certain size in an electrical grid. Say over six years we observe a series of (3, 4, 3, 0, 2, 6) outages. The number of outages is not the same from year to year; there is variation. Assuming independence between the years, we can use a Poisson model and calculate, say $P_f(0)$, which is the fraction of years in the long run with zero outages. It is, however, clear that 'similar conditions' require a somewhat stable process; cf. Bergman [11]. This is the case for many technical components but, in comparison, not for humans and dependencies. A frequentist probability model may be hard to justify.

The other meaning of probability is a subjective (knowledge-based, judgmental) probability, P(A), which expresses the assessor's degree of belief that A will happen with reference to an urn standard [28,37]. For example $P(A)=0.1$ expresses that the assessor's uncertainty about A occurring is comparable to drawing a favorable ball out of an urn containing one favorable and nine unfavorable balls. The event A can also be a proposition about a variation pattern, a parameter or performance variability. There is no reference to a true fraction that is unknown, as is the case for the frequentist interpretation. Subjective probabilities can be used for technological endeavors with no historical data or variable human performance, i.e. even unique cases.

The subjective probability, P(A), expresses uncertainty, but conditioned on some background knowledge, K, in the form of expert opinions, phenomenological understanding, assumptions, models and data. This dependency can be denoted as $P(A|K)$, and K can contain 'hidden' risks. Likelihood judgments on performance variability can serve to illustrate. Say we assume that it is very unlikely, i.e. a very small probability, that the operator of the lines misses operating the off-switch when there is little stress. Effectively, this is not an interesting scenario to either develop or safeguard against. This can of course be wrong: the operator could intentionally want to cause an accident to the ship, something that would mean that an inadequate off-switch is very likely. The (tacit) assumption that the probability judgment condition on, is that the operator is not a terrorist.

4. Discussion

As explained in Section 3, there are many reasons why probability can be discarded. In fact, communicating probabilities when these reasons are valid seems futile and can seriously misguide a decision maker. But the underlying issue of risk is essentially also about uncertainty and this cannot easily be swept under the carpet. It can be argued that the FRAM and STAMP approaches reduce the uncertainty, by generating more insightful models of the system behavior/accidents, causality and variability. If probability is used as a model of variation which is inadequate/inaccurate, it can be discarded in favor of a better model of variation, causality, or both; cf. Winkler [54].

However a model is exactly that: a model, and not the system it represents. There will always be uncertainty about how well the model matches the system behavior. Assumptions have to be made on resolution, system boundaries, etc. In FRAM for example, many assumptions about reasonable variability and conditions are made. A STAMP analysis will also make many assumptions, for example about how a system is, or will be, organized (see also [34]). Nevertheless, an assumption may not be as sound as initially thought. In one of the largest power outages ever recorded in Europe on November 4th, 2006 [14,51], a transmission line operator assumed deliberately under high stress that a certain grid-action would lead the grid to behave in one way (redirect the current), yet the opposite happened, causing a cascade of tripping lines.

Shaky assumptions are only one of several issues. STAMP/STPA is, for example, used in relation to novel technology endeavors. Clearly, these are cases with very limited operational experience and little or no data, and perhaps depending on inaccurate models of, say, the environment on Mars. Shaky assumptions, little data and inaccurate models are epistemic uncertainty factors that should be important to account for when making a decision. Knowledge-based probability is a tool that can be used to characterize this type of uncertainty, yet the issues of limited data and shaky assumptions imply that little weight can be given to an assigned number (it can in some way be considered 'a number pulled out of the air'). Nevertheless, the solution when using probability to describe uncertainty is not to make better models and descriptions to reduce uncertainty as such but to de-camouflage and characterize uncertainty better.

We can contrast two views on how to proceed in the case of an uncertain/inadequate probability model:

A. Reduce uncertainty by better modeling of the system
B. Characterize uncertainty better

In case A, the accuracy of the model is important, but there will always be uncertainty about how well the model matches the system's behavior. In case B the key focus is exactly this uncertainty; the accuracy of the model is of less importance, yet better models of a system are of course sought and applauded. In practice both A and B are needed. A model's accuracy in predicting

scenarios or hazards cannot be judged without taking into account the uncertainty about how well the model with scenarios/hazards matches the system. The FRAM and STAMP approaches in its current form essentially targets A, and so there will be uncertainties and potential for surprises that are not addressed or communicated to the decision maker. Better understanding and modeling of the system and variation is the key aim in many complex systems, e.g. using (improved) stochastic jump processes in the financial industry to better predict future stock prices.

In theory, for case B, one could still use a probability model of human variability, and for complex technological endeavors with little data. But along with the model there has to be a statement on uncertainties, to judge its accuracy. One way of doing this is presented in Bjerga et al. [12]. In that paper, the difference between the true variation pattern F (which can be known with time) and the probability model of variation G(X) (X being a parameter) is called the model error, i.e. the model error is F-G(X), and the uncertainty about the magnitude of the model error is called model uncertainty. Based on model uncertainty analysis, a model can be accredited or remodeled, or at the very least the analysis produces a statement on the uncertainties which can be presented to the decision maker. Different models can also be compared on the basis of the model uncertainty analysis. In the case of qualitative models, conceptually the model error still exists, but it is difficult or impossible to quantify it. Yet, the uncertainty level can still be addressed using a more qualitative approach, for example by addressing and making judgments on the strength of the background knowledge [4,18]. Aspects considered in such a judgment are [6]:

- The degree to which assumptions made represent strong simplifications
- The availability of relevant data
- The degree of agreement/consensus among experts
- The degree of understanding of the phenomena involved
- The existence of accurate models

The issue with complex systems is that they cannot be understood on the basis of components, even if components can be 'perfectly' modeled, e.g. by a probability model. In other words, the whole is more than the sum of the parts. Missing in the summation are interconnections or relationships among parts. These relationships can be of linear or non-linear nature and may contribute to escalating systemic consequences. Another thing omitted from the summation is a system's function or purpose. Also, many technical risk assessments are oriented towards technical components, giving less weight to organizational and human factors. Parts (of any nature), interconnections and functions are all important determinants for system behavior [39]. The FRAM and STAMP approaches address many of these issues. However, also missing in the equation is the uncertainty linked to what we know about dependencies, the system behavior, components, and purposes, which may be limited. It could therefore be useful to address the knowledge strength for different aspects. Table 2 is a first attempt, which can be used for that purpose and communicated to the decision maker.

Assumptions are of particular importance in FRAM and STAMP, for which, there can be separate assessments of assumption-deviation-risk [4]. Assumptions for example about variability or dependencies need to be stated and then evaluated as to: what deviations can occur, how likely the deviations are, potential consequences, and the strength of the background knowledge. Other qualitative approaches are also available to address assumptions, e.g. Assumption-Based Planning by Dewar [16], cf. Leveson [34].

Table 2
Strength of knowledge addressing different aspects of complex systems.

Is the strength of knowledge on dependencies (linear/non-linear) good?
Is the strength of knowledge on parts (of any nature) good?
Is the strength of knowledge on functions/purposes good?
Is the strength of knowledge on the system's environment good?
Is the strength of knowledge on variation/variability in the system good?
Is the strength of knowledge on the system as a whole good?

It can also be relevant to address potential surprises relative to the knowledge/beliefs held. If the surprises carry extreme consequences, they are called black swans [5,50]. These can be addressed using, for example, red teams, and monitoring of signals and warnings [6,44]. A red team in a risk analysis would consist of an 'outside' analysis group, whose job is to challenge the models, assumptions and judgments made by the initial group. A list of potential black swans can then be handed to the decision maker. Practice have shown that a red team exercise can be very beneficial, but that the usefulness of red teams can easily be impaired, for example by a corporate culture that does not appreciate criticism [31]. It is a research area how to improve and use these methods in practice.

Returning to probabilities, it can for complex systems be very challenging to give precise probabilities, say $P(A)=0.16$, where A is some event. The number may seem too precise, given the uncertainty linked to complex systems. It is possible to use qualitative scales and statements, for example. 'unlikely', 'possible', 'likely', as in Hollnagel [23]. But what does, for example, 'possible' mean? In usual parlance, 'possible' could mean that the probability is above zero, or that it is some narrower unspecified range. The point is that qualitative probability scales without being linked to specified intervals and meaning, can be vague and difficult to use. An alternative is to use imprecision intervals, say [0.1,0.3], with the upper and lower assignments interpreted as subjective probabilities: the assigner states that his/her degree of belief in A occurring is greater than the urn chance of 0.1 (the degree of belief of drawing a specific ball out of an urn containing 10), and less than the urn chance of 0.30. The analyst is not willing to make any further judgments. Imprecise probability intervals capture some uncertainty beyond precise probability assignments but still conditioned on some background knowledge, which also needs to be addressed.

Another quantitative alternative is fuzzy set theory and fuzzy logic after Zadeh [55] which have been proposed as descriptions of variability in FRAM [23]. It is a research question if and how fuzzy descriptors can be used in practice. The interpretation of fuzzy descriptions are difficult as discussed in Bedford and Cooke [9].

Lastly, a relevant question is, if the decision makers in reality want the information about uncertainties and potential surprises, and if it in practice makes a difference to decision making. From the perspective of a risk analyst the aim should be to communicate both what is known and what is not known-both the model and the model uncertainties. It is from that perspective of less importance how the decision-maker chooses to make use of the information, though the position taken in this paper is that good risk decision making is based on proper understanding and treatment of uncertainties. It is however, a research challenge how to convey both what is known and lack of knowledge to the decision-maker in a best possible way. It is also a general research question how a manager should think and act when facing uncertainty. And of course it is a question about the manager's values and priorities.

5. Conclusion

This paper has considered complex system risk analysis and the use of the FRAM and STAMP approaches. Focus has been on the treatment of uncertainty in these approaches, as probability is

largely discarded. Rather, the focus of the FRAM and STAMP approaches is on better qualitative modeling and description of systemic behavior and accidents, giving due attention to dependencies. Better modeling can be a way to gain better understanding of the system and potential systemic accidents, and thus reduce uncertainty. Yet, without addressing uncertainties the models and descriptions of potential scenarios and hazards identified should not be confidently used by a decision maker. Both better modeling and identification of possible complex system accidents using tools like FRAM and STAMP, and better characterization of uncertainties are advocated. Some ways to address and characterize uncertainties, knowledge aspects and surprises, also in qualitative ways, have been discussed in relation to that.

Acknowledgements

The authors are grateful to four reviewers for useful comments and suggestions that helped improve the paper. The work has been partly funded by the Research Council of Norway - as a part of the Petromaks 2 program (grant number 228335/E30). The support is gratefully acknowledged.

References

[1] Apostolakis G. The concept of probability in safety assessments of technological systems. Science 1990;250:1359–64.
[2] Apostolakis GE, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Anal 2005;25:361–76.
[3] Aven T. How to define and interpret a probability in a risk and safety setting. Discussion paper with G. Reniers. Saf Sci 2013;51(1):223–31.
[4] Aven T. Practical implications of the new risk perspectives. Reliab Eng Syst Saf 2013;115:136–45.
[5] Aven T. On the meaning of a black swan in a risk context. Saf Sci 2013;57:44–51.
[6] Aven T. Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management. Abingdon: Routledge; 2014.
[7] Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliab Eng Syst Saf 2011;96(1):64–74.
[8] Aven T, Baraldi P, Flage R, Zio E. Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods. Chichester: John Wiley & Sons; 2014.
[9] Bedford T, Cooke R. Probabilistic risk analysis: foundations and methods. Cambridge: Cambridge University Press; 2001.
[10] Belmonte F, Schön W, Heurley L, Capel R. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: an application to railway traffic supervision. Reliab Eng Syst Saf 2011;96(2):237–49.
[11] Bergman B. Conceptualistic pragmatism: a framework for bayesian analysis? IIE Trans 2008;41(1):86–93.
[12] Bjerga T, Aven T, Zio E. An illustration of the use of an approach for treating model uncertainties in risk assessment. Reliab Eng Syst Saf 2014;125:46–53.
[13] Brown T, Beyeler W, Barton D. Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems. Int J Crit Infrastruct 2004;1(1):108–17.
[14] Castle S. Europe suffers worst blackout for three decades. The Independent, Monday 6th Nov. ⟨http://www.independent.co.uk/news/world/europe/europe-suffers-worst-blackout-for-three-decades-423144.html⟩; 2006 [accessed 13.04.15].
[15] Dekker S. Drift into failure: from hunting broken components to understanding complex systems. Aldershot: Ashgate Publishing Ltd; 2012.
[16] Dewar JA. Assumption-based planning: a tool for reducing avoidable surprises. Cambridge: Cambridge University Press; 2002.
[17] Dulac N. A framework for dynamic safety and risk management modeling in complex engineering systems.Cambridge: Massachusetts Institute of Technology; 2007.
[18] Flage R, Aven T. Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA) *Reliability and Risk Analysis: Theory & Applications*. 2009;2(13):9–18.
[19] Heinrich HW. Industrial accident prevention. NY: McGraw-Hill; 1931.
[20] Helbing D. Globally networked risks and how to respond. Nature 2013;497:7447.
[21] Hines P, Apt J, Talukdar S. Trends in the history of large blackouts in the United States. In: Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE; July 2008. p. 1–8.
[22] Hollnagel E. Barriers and accident prevention: or how to improve safety by understanding the nature of accidents rather than finding their causes. Hampshire: Ashgate; 2004.
[23] Hollnagel E. FRAM: The functional resonance analysis method: modelling complex socio-technical systems. Farnham: Ashgate Publishing Ltd; 2012.
[24] Hollnagel E. An application of the functional resonance analysis Method (FRAM) to risk assessment of organisational change. Stockholm: Swedish Radiation Safety Authority; 2013.
[25] Hollnagel E, Woods DD, Leveson N. Resilience engineering: concepts and precepts. Aldershot: Ashgate Publishing Ltd; 2006.
[26] Ishimatsu T, Leveson NG, Thomas JP, Fleming CH, Katahira M, Miyamoto Y, Hoshino N. Hazard analysis of complex spacecraft using systems-theoretic process analysis. J Spacecr Rockets 2014;51(2):509–22.
[27] Johansen IL Rausand M. Defining complexity for risk assessment of socio-technical systems: A conceptual framework. In: Proceedings of the Institution of Mechanical Engineers, Part O: J Risk Reliab, 228(3); 2014. p. 272–290.
[28] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal 1981;1:11–27.
[29] Kazaras K, Kirytopoulos K, Rentizelas A. Introducing the STAMP method in road tunnel safety assessment. Saf Sci 2012;50(9):1806–17.
[30] Kröger W, Zio E. Vulnerable systems. London: Springer Science & Business Media; 2011.
[31] Laracy JR, Leveson NG. Apply STAMP to critical infrastructure protection. In: Proceedings of the 2007 IEEE conference on technologies for homeland security. IEEE; May 2007. p. 215–220.
[32] Leveson N. A new accident model for engineering safer systems. Saf Sci 2004;42(4):237–70.
[33] Leveson N. Engineering a safer world: systems thinking applied to safety. Cambridge: The MIT Press; 2011.
[34] Leveson N. A systems approach to risk management through leading safety indicators. Reliab Eng Syst Saf 2015;136:17–34.
[35] Leveson NG, Dulac N, Barrett B, Carroll J, Cutcher-Gershenfeld J, Friedenthal S. Risk Analysis of NASA Independent Technical Authority. Cambridge, MA: MIT; 2005.
[36] Lewis TG. Book of extremes. Switzerland: Springer; 2014.
[37] Lindley DV. The philosophy of statistics. Statistician 2000:293–337.
[38] McDaniel RR, Driebe DJ, editors. Uncertainty and surprise in complex systems: questions on working with the unexpected. Berlin, Heidelberg: Springer Science & Business Media; 2005.
[39] Meadows DH. (Edited by Wright D.) Thinking in systems: A primer. VT: Chelsea Green; 2008.
[40] Mishkin FS. Over the cliff: From the subprime to the global financial crisis. The Journal of Economic Perspectives 2011;25(1):49–70.
[41] Mitchell M. Complexity: a guided tour. New York: Oxford University Press; 2009.
[42] Mohaghegh Z, Mosleh A. Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: principles and theoretical foundations. Saf Sci 2009;47(8):1139–58.
[43] Ottino JM. Engineering complex systems. Nature 2004;427(6973) 399-399.
[44] Paté-Cornell E. On "black swans" and "perfect storms": Risk analysis and management when statistics are not enough. Risk Anal 2012;32:1823–33.
[45] Perrow C. Normal accidents: living with high risk technologies. Chichester: Princeton University Press; 1984.
[46] Rasmussen J. Risk management in a dynamic society: a modelling problem. Saf Sci 1997;27(2):183–213.
[47] Reason JT. Managing the risks of organizational accidents, Vol. 6. Aldershot: Ashgate; 1997.
[48] Rosa LV, Haddad AN, de Carvalho PVR. Assessing risk in sustainable construction using the Functional Resonance Analysis Method (FRAM). Cognition, Technology and Work; 2015. p. 1–15.
[49] Song Y. Applying system-theoretic accident model and processes (STAMP) to hazard analysis. (Master's Thesis) McMaster University; 2012.
[50] Taleb NN. The black swan: the impact of the highly improbable. New York: Random House; 2007.
[51] UCTE. (UCTE, now: ENTSO-E) Final report system disturbance on 4 November 2006; 2007.
[52] Variable. Retrieved 15.02.16, from ⟨http://www.merriam-webster.com/dictionary/variable⟩ (n.d.).
[53] Weaver W. Science and complexity. Am Sci 1948;36(4):536.
[54] Winkler RL. Uncertainty in probabilistic risk assessment. Reliab Eng Syst Saf 1996;54(2):127–32.
[55] Zadeh LA. Fuzzy sets. Inf Control 1965;8(3):338–53.
[56] Zio E, Aven T. Uncertainties in smart grids behavior and modeling: what are the risks and vulnerabilities? How to analyze them? Energy Policy 2011;39(10):6308–20.