Reliability Engineering and System Safety 120 (2013) 27–38

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems

Jonas Johansson [a,c,*], Henrik Hassel [b,c], Enrico Zio [d,e]

[a] Department of Industrial Electrical Engineering and Automation, Lund University, Box 118, SE-221 00 Lund, Sweden
[b] Department of Fire Safety Engineering and Systems Safety, Lund University, Box 118, SE-221 00 Lund, Sweden
[c] Lund University Centre for Risk Analysis and Management (LUCRAM), Sweden
[d] Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy-Electricite' de France, at Ecole Centrale Paris & Supelec, France
[e] Dipartimento di Energia, Politecnico di Milano, Milano, Italy

ARTICLE INFO

Available online 21 March 2013

Keywords:
Reliability analysis
Vulnerability analysis
Risk management
Critical infrastructures
Power systems

ABSTRACT

Society depends on services provided by critical infrastructures, and hence it is important that they are reliable and robust. Two main approaches for gaining knowledge required for designing and improving critical infrastructures are reliability analysis and vulnerability analysis. The former analyses the ability of the system to perform its intended function; the latter analyses its inability to withstand strains and the effects of the consequent failures. The two approaches have similarities but also some differences with respect to what type of information they generate about the system. In this view, the main purpose of this paper is to discuss and contrast these approaches. To strengthen the discussion and exemplify its findings, a Monte Carlo-based reliability analysis and a vulnerability analysis are considered in their application to a relatively simple, but representative, system the IEEE RTS96 electric power test system. The exemplification reveals that reliability analysis provides a good picture of the system likely behaviour, but fails to capture a large portion of the high consequence scenarios, which are instead captured in the vulnerability analysis. Although these scenarios might be estimated to have small probabilities of occurrence, they should be identified, considered and treated cautiously, as probabilistic analyses should not be the only input to decision-making for the design and protection of critical infrastructures. The general conclusion that can be drawn from the findings of the example is that vulnerability analysis should be used to complement reliability studies, as well as other forms of probabilistic risk analysis. Measures should be sought for reducing both the vulnerability, i.e. improving the system ability to withstand strains and stresses, and the reliability, i.e. improving the likely behaviour.

1. Introduction

Continuous supply of critical infrastructure services, such as electric power, water, information and transportation, is essential for people, public and private organizations, and for the security and economy of the society as a whole [1]. The importance of critical infrastructures has been demonstrated in numerous infrastructure breakdowns for example: the U.S. blackout in 2003, Hurricane Katrina in 2005 and the storms Gudrun and Per in Sweden in 2005 and 2007, respectively [2].

Critical infrastructures have undergone and are currently undergoing large changes. They are becoming more dependent and interdependent on each other [3]. In addition, they are increasingly connected across geographical borders and thus become more large-scale. These trends make the critical infrastructures more efficient but at the same time more complex and more vulnerable, and the potential for large-scale disruptions increases.

The aspects described above in combination with the extensive societal dependence on critical infrastructures, stress the importance of systematically managing risks and vulnerabilities. The traditional risk management approach has been the prevailing one in ensuring continuous services provided by critical infrastructures. Here, the traditional risk management approach is seen as encompassing the identification of hazards and threats that can affect the system, the estimation of the probabilities of various risk scenarios and their negative consequences, and the mitigation of the risks. Risk mitigation is often implemented as protection of the system from hazards and threats to a level of risk that can be deemed acceptable or tolerable. In this paper, we argue that the

* Corresponding author at: Lund University, Department of Industrial Electrical Engineering and Automation, IEA, LTH, Box 118, SE-221 00 Lund, Sweden. Tel.: +46 0 46 222 31 05.
E-mail addresses: jonas.johansson@iea.lth.se (J. Johansson), henrik.hassel@lucram.lu.se (H. Hassel), enrico.zio@ecp.fr (E. Zio).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.02.027

traditional risk management approach needs to be complemented with a vulnerability management approach. A vulnerability management approach is here seen as including the evaluation of the ability of the system to withstand strains and the mitigation of the identified vulnerabilities by implementing system changes. This approach can compensate inherent limitations of the traditional risk management approach. These viewpoints are further elaborated throughout the paper.

The cornerstone of any effort to manage the risks and/or vulnerabilities of critical infrastructure systems is good knowledge and understanding regarding the function, operation, capacity, and limitation of the systems. Such knowledge can then be used as guidance towards improvements.

In the traditional risk management approach for critical infrastructures, quantitative risk and reliability analysis has been the main approach for acquiring knowledge about the systems of interest. In this, reliability analysis can be seen as part of Quantitative Risk Assessment (QRA), providing the probabilistic input to the risk assessments, i.e. estimating probabilities of various failure scenarios [4–6]. However, in risk and reliability management of critical infrastructures, e.g. electric power systems or water supply systems, the concepts are often treated synonymously, where reliability analysis often also includes estimation of negative consequences. Consider for example the commonly used reliability indices in the electric power system area (e.g. EDNS and EENS – see Section 5 for an explanation of these concepts) which aggregate information about both the frequency and severity of failures. This paper will focus on reliability assessment since traditionally it is the most commonly used concept in the area of critical infrastructures; however, much of the discussion is valid for risk assessment as well.

Reliability as a concept has been used in the context of engineering systems for more than 60 years [7]. A frequently used definition, which is adopted here, of reliability is the probability (or more generally – the ability) of a system, sub-system or component "to perform a required function, under given environmental and operational conditions and for a stated period of time" [4–6]. Similar definitions can be found in for example Allan and Billinton [8] and Murray and Grubesic [9]. When it comes to critical infrastructure systems, reliability thus refers to the ability of the critical infrastructure system to provide its services to its customers (e.g. to provide electric power supply to customers or to enable the transport of people and goods on roads). In the area of power systems, in which the example system considered in this paper falls, the concept of reliability is often operationalized in terms of the reliability indices mentioned in the previous paragraph.

Quantitative risk and reliability assessments both emphasise the importance of estimating the probabilities of failures which are then used to inform risk management decisions, along with estimations of negative consequences. However, many express criticism towards relying too heavily on quantitative probability estimations when making decisions, see e.g. [10–12]. It is claimed that the estimations may be poor because they are based on insufficient knowledge and inappropriate assumptions (e.g. event independence). In addition, "surprises" may occur, e.g. due to unknown failure mechanisms, or calculations may simply be wrong ([10,13–15]). This is especially argued for when faced with large complexity and uncertainty, which definitely are characteristics of critical infrastructures [7,16,17]. It is argued that in such situations one must also look beyond the estimated probabilities, and risk reduction needs to be designed based on principles such as robustness, resilience, flexibility, diversification and defence-in-depth, as well as adding an extra safety margin [17,18], i.e. from a vulnerability perspective. These reduction measures especially need to address the low probability, often high consequence, events, since it is the tail of the probability distributions that are most difficult to estimate accurately [19].

Another approach to acquire knowledge for understanding and improving critical infrastructures is vulnerability analysis, which has been given increased attention in the research community during the last decade. Vulnerability is a term that is used with some different denotations in the scientific literature [20]. In the present context, vulnerability is defined as the inability of a system to withstand strains and the effects of failures, i.e. to absorb the strain and/or to restore the system quickly to full functionality. Haimes has a similar view and defines vulnerability as "the manifestation of the inherent states of the system that can be exploited to adversely affect that system" [21] – stressing that vulnerability is concerned with the inherent characteristics of a system rather than the environment in which the system is situated. In the context of vulnerability analysis, the role of probabilities of failures, threats and hazardous events are less emphasised. When analysing vulnerability, the focus is not on estimating these probabilities but rather to systematically explore the effects of failures and strains in order to identify system weaknesses that may be exploited by some, perhaps unknown or previously unimagined, threats or hazards. Later in the paper three different perspectives of vulnerability analysis are discussed. These perspectives constitute ways of operationalizing the concept in the context of critical infrastructures.

Reliability and vulnerability analyses of critical infrastructures have similarities but also some differences with respect to what type of information they generate about the systems. Few papers exist where the two approaches are discussed and contrasted in parallel, e.g. [22]. However, systematic comparisons with the aim of finding out their specific strengths and weaknesses, and perhaps more importantly how the two approaches can be used as a complement to each other, are lacking.

This paper attempts to pragmatically address the apparent lack of comparative studies by analysing a simple, but representative, example of a critical infrastructure using the two different approaches. The overall aim is to compare and discuss reliability analysis and vulnerability analysis of critical infrastructures, specifically exemplifying the type of results on a numerical example of a test system, and showing how these analyses can provide complementing information and knowledge. The test system selected for the study is an electric power system, the IEEE reliability test system [23], chosen because of its wide use as representative case in the scientific literature. The two types of analyses on the test system are delineated in accordance with their fundamental characteristics and how they are performed within their respective fields, in order to clarify the typical results that they achieve. This leads to the discussion on how these types of analyses and their results can be used to guide decisions in the wider context of management of critical infrastructures, providing the foundation for establishing how reliability analysis and vulnerability analysis can be combined to help understanding the behaviour and limitations of a system.

2. Reliability and vulnerability analyses of critical infrastructures

2.1. Reliability analysis

Reliability analysis is commonly used in the context of critical infrastructures; see [9] for an overview, [24] for an application to gas networks, and [25] for an application to water supply systems. Although the exact procedures may vary between different infrastructures, the main underlying principles are the same.