Reliability Engineering and System Safety 169 (2018) 312–320

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Bayesian network application for the risk assessment of existing energy production units

Miroslav Sýkora[a,*], Jana Marková[a], Dimitris Diamantidis[b]

[a] Czech Technical University in Prague, Klokner Institute, Solinova 7, 166 08 Prague, Czech Republic
[b] Ostbayerische Technische Hochschule Regensburg, Faculty of Civil Engineering, Galgenbergstrasse 30, 93053 Regensburg, Germany

ARTICLE INFO

Keywords:
Availability
Bayesian networks
Failure probability
Production unit
Risk analysis
Societal risk
Uncertainties

ABSTRACT

The assessment of existing infrastructures in the energy sector is of great economic significance worldwide. Fossil power stations are reaching their design service life and rational decisions concerning extensions of service life, maintenance and replacements of devices should be based on updated information of the actual conditions of the energy devices and their components, and on cost-benefit analysis using risk analysis and probabilistic optimisation procedures.

The contribution provides an integrated framework for probabilistic reliability and risk assessment of existing energy production units considering availability and human safety criteria. An extensive case study focused on risks of an energy production unit in a fossil power station is provided to support practical applications. A Bayesian network is thereby implemented to assess the risks of the selected production unit. Special emphasis is given to the input data consisting of failure rates obtained from recorded data and expert judgements. The influence of uncertainties in the considered performance indicators on the availability of the unit is analysed. It is shown that a reasonably simplified framework can provide a valuable assessment of the influence of individual devices and their components on availability and societal risk, identifying thus the major risk contributors.

1. Introduction

The assessment of existing infrastructures in the energy sector is an important issue of great economic significance worldwide, since a major part of investments is associated with the maintenance or rehabilitation of existing systems. In fact, numerous fossil power stations are reaching the limits of design service life. Until recently, most operators have been assessing the remaining service lives and the risks of technological devices in production units on the basis of long-term experience and related inspection programs. Insufficient attention paid to analysis of limited monitoring data has then been compensated for by conservative (non-optimal) maintenance and investment plans.

Due to economic requirements and constraints, plant operators nowadays tend to optimise total operational costs including maintenance, inspections and availability of key components. Consequently, they usually introduce modern monitoring systems which are able to provide useful information about performance indicators describing the actual states of technological devices. Such information can be treated by implementing statistical methods in order to deal with uncertainties related to the available data.

Rational decisions concerning extensions of service life, maintenance and replacements of devices should be based on:

- Updated information of the actual conditions of individual energy devices and their components
- Cost-benefit analysis using methods of risk analysis and probabilistic optimisation, based adopted utilisation plan.

Risk analysis is often a demanding but important step of the decision process. In many practical cases in the past, qualitative or semi-quantitative methods have been applied only. Such methods rely heavily on expert judgements and therefore the direct inclusion of measurement results may represent a difficult task. This is why in practice, quantitative risk assessments are currently being implemented. However, it seems that the application of these methods have so far been focused mostly on individual devices [1,2].

Based on the general methodologies [3,4], the present contribution provides an integrated framework for probabilistic reliability and risk assessment of existing energy production units considering availability and human safety criteria. An extensive real case study focused on risks of an energy production unit in a fossil power station demonstrates a practical application of the theoretical principles:

* Corresponding author.
E-mail addresses: miroslav.sykora@cvut.cz (M. Sýkora), jana.markova@cvut.cz (J. Marková), dimitris.diamantidis@oth-regensburg.de (D. Diamantidis).

https://doi.org/10.1016/j.ress.2017.09.006
Received 9 March 2017; Received in revised form 11 July 2017; Accepted 22 September 2017
Available online 23 September 2017

1. Key devices of the production unit are selected in order to cover major risk contributors and maintain a reasonable complexity of risk analysis.
2. A Bayesian network is applied to estimate economic and societal risks, illustrating how statistical data and expert judgements can be included in the analysis procedure.
3. Risk acceptance criteria are justified for the power unit under consideration.
4. The effect of statistical uncertainties is quantified by Bayesian updating.

In the next few years, managers of the plant will have to decide on the extension of its working life or shut-down and the results of the risk analysis described herein deliver the basis for such a decision.

2. State of the art

2.1. Risk analysis framework

Risk analysis is indispensable in order to identify hazards, assess vulnerabilities of the infrastructure and evaluate the associated impact – consequences on assets, infrastructures or systems taking into account the probability of the occurrence of the identified hazards. This is a critical element that differentiates a risk assessment from typical consequence assessment methodology. Following ISO 13824 on general principles of risk assessment [5], the risk related to a hazard is a combination of the probability of occurrence of this hazard, and the consequences of the hazard situation, given its occurrence. When for mutually independent hazard scenarios situations H_i (hazards) the failure F of the component given a particular hazard situation H_i occurs with the conditional probability $\mathrm{P}(F|H_i)$, then the total probability of failure P_f is given by the law of total probability [3–5] for small probabilities as:

$$P_f = \sum_i \mathrm{P}(F|H_i)\mathrm{P}(H_i) \tag{1}$$

The conditional probabilities $\mathrm{P}(F|H_i)$ are determined by analyses of the respective hazard scenarios H_i which may lead to several events E_{ij} (e.g. excessive stresses, fatigue of material, unacceptable vibrations or deformations) with adverse consequences C_{ij} related e.g. to the time of an outage of the production unit. The total risk R corresponding to the hazard scenario H_i can consequently be expressed [3–5] as:

$$R = \sum_{IJ} C_{ij}\mathrm{P}\left(E_{ij} \middle| H_i \right) \mathrm{P}(\mathrm{H}_i) \tag{2}$$

The consequences of adverse events E_{ij} may consist of several components denoted as $C_{ij,k}$ including societal consequences (fatalities, injuries), economic consequences (replacement/repair, clean-up costs, business interruption etc.) and environmental impact (for example, considerably increased pollution due to malfunction of a desulphurisation unit). The components R_k of the total risk may be assessed from the relationship [3–5]:

$$R_k = \sum_{i,j} C_{ij,k}\mathrm{P}(E_{i,j}|H_i)\mathrm{P}(H_i) \tag{3}$$

Probabilistic approaches become widely used in various industrial sectors since they support decisions of the operators regarding the future use of plants. Such approaches take into account inherent uncertainties in the description of the influencing parameters, their effect on the actual state of devices and also the estimates of consequences. Input data can be obtained by the interpretation of plant functional diagrams and discussions with the personnel of the plant to identify the functional rules and the components influencing the failure modes through a Failure Mode and Effect Analysis. In many practical cases other methodologies such as event or fault trees are applied. Further information on the probabilistic risk analysis methods can be obtained from [4–8].

2.2. Bayesian network implementation

Available data for risk analyses of engineering systems are often complex and scattered, covering information from different technical fields and combinations of numerical investigations and qualitative expert judgments. Probability theory, implemented through Bayesian (belief) networks, offers a powerful tool to deal with this complexity.

The analysis of a Bayesian network is based on the specification of conditional probabilities of child nodes for given states of parent nodes (connected by causal links), using the concept of conditional probabilities. A network is typically represented by an acyclic directed graph in which nodes represent random variables and arcs (arrows) indicate the direct probabilistic dependencies among them – causal links [9]. Chance nodes denote random variables that can be described by discrete or continuous probabilistic distributions. In addition to the chance nodes, Bayesian networks can include deterministic nodes – decision and utility nodes; the former are used to model a decision-maker's options, while the latter denote variables that contain information about goals and objectives. Risk analysis using Bayesian networks is quite an extensive topic; further information can be found, for instance in [4,7,10–12].

Bayesian networks have proved to be a useful tool in various technical fields; recent applications from a range of technical disciplines include probabilistic assessments in the nuclear industry [13], optimisations of tunnel excavations [14] and tunnel safety measures [15], assessment of flooding risks [16], avalanche modelling [17], risk analysis of transportation networks [18], risk-based decision making [19] and forensic assessments [20,21]. These studies have been motivated by the appealing features of Bayesian causal networks that facilitate:

- Break down of a complex task (a production unit) into smaller subtasks (significant components) that can be analysed separately by individual experts on particular devices.
- Illustrative interpretation of knowledge concerning devices based on results of measurements and expert appraisals.
- Direct implementation of uncertainties with respect to material and geometrical properties, operating conditions, inaccuracy of measurements and also theoretical models applied in analyses of devices.
- Modelling of complicated functional dependencies amongst devices, which cannot be modelled in such detail by fault or event trees.
- Updating of results when new information becomes available.
- Acquisition of all relevant information for decision-making concerning operational processes and their maintenance.
- Identifying likelihoods of causes leading to failures of technical systems in forensic assessments.

2.3. Risk acceptance criteria

If the acceptable or target risk R_{kt} is specified, the risk R_k of devices or the whole production unit can be assessed on its basis, $R_k < R_{kt}$. This supplements the basic reliability requirement $P_f < P_{ft}$, where P_{ft} is the target value of failure probability [5,22,23]. The guidance for the determination of the acceptable risk R_{kt} is provided in recently revised ISO 2394 [22]. When the criterion of the acceptable risk is not fulfilled, it is necessary to modify the system by appropriate interventions aimed at reducing the probability of occurrence of adverse events (prevention measures), or at reducing consequences (mitigation measures).

However, acceptable risk levels cannot be defined in an absolute sense since individuals have their own perception of acceptable risk which – when expressed in *decision theory* terms – represents their own "preferences". In order to define what is meant by "acceptable risk levels", a framework for risk acceptability was adopted [24,25] and implemented in the risk assessment of infrastructure projects of the offshore, nuclear or transportation industry. *F-N* curves represent a popular simplified approach to establish group risk criteria; examples and discussion are provided in [26–28].