ARTICLE IN PRESS

Safety Science xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Safety Science

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

Design of procedures for rare, new or complex processes: Part 2 – Comparative risk assessment and CEA of the case study

Marko Gerbec [a,*], Gabriele Baldissone [b], Micaela Demichela [b]

[a] Jozef Stefan Institute, Jamova 39, 1000 Ljubljana, Slovenia
[b] Politecnico di Torino, Dept. of Applied Science and Technology, Corso Duca degli Abruzzi, 24, 1029 Torino, Italy

ARTICLE INFO

Article history:
Received 11 May 2016
Received in revised form 19 September 2016
Accepted 25 October 2016
Available online xxxx

Keywords:
Risk assessment
Human reliability assessment
Bayesian networks
Dynamic decision analysis
Cost effectiveness analysis

ABSTRACT

The paper provides the comparative risk assessment for the case in related paper Design of Procedures for Rare, New or Complex Processes: Part 1 - An Iterative Risk-Based Approach and case study (this issue), where the optimization of the pressure testing procedure for an LPG storage sphere is discussed. Both the 'Original' and the 'Optimized' procedure alternatives were the subject of a double comparative risk assessment using two different methods, namely, Bayesian Belief Networks using the HUGIN programme and Integrated Dynamic Decision Analysis (IDDA) using the SPACCO programme. Results suggest that the outputs from both methods/programmes were essentially the same, while the differences are mainly related to the results visualization and their subsequent use. In addition, the adoption of the methods has shown a reduction of the overall failure probabilities considering the 'Original' and 'Optimized' procedural alternatives respectively. The results of the comparative cost effectiveness analysis between both alternatives suggest that the initial investment on developing and optimizing the procedure is easily compensated by direct savings in implementation costs, as well as by the further savings in delay risks, occupational safety risks and process safety risks. Pertaining uncertainties in the analysis are also discussed. The results were found valuable for the site management on the "how and why" of developing a rare and potentially hazardous test procedure.

1. Introduction

The classical risk assessment approach to the system safety builds on methods and techniques based on different applications of the logic theory. It is recognized that classical sequential approaches modelling initiating events as failures or successes propagating to the outcome events of interest, using techniques such as fault trees and event trees (and bow-ties), have serious deficiencies if dependent/interrelated events (e.g., via latent conditions) are important (Podofillini et al., 2010; Badreddine and Ben Amor, 2013; Vinnem et al., 2012). In addition, most of the risk assessments in the process industry are focused on the "regular" production oriented activities (being either continuous, semi-continuous, or of a batch type), while periodic inspection & maintenance procedures are assessed scarcely, however, indisputably important (Okoh and Haugen, 2013; Vinnem et al., 2012; Weber et al., 2012). Furthermore, the human and organisational factors are usually neglected in the traditional risk assessment approaches, and are analysed separately, usually only when a need rises because of regulations, production requirements or accident occurrence. This results in a loss of completeness and of synergetic effects in risk analysis and thus to less effective decision-making.

This paper is a continuation of Gerbec et al. (this issue), which discussed the proposed approach to design, assess and optimize rare risky and initially undefined procedures for inspection & maintenance in process industry. The approach combines different methods for the description and analysis of plant and operations, including Task Analysis, 4D process simulation, hazard analysis and Pareto optimization, and iterates through them to generate a final procedure. The proposed approach has been demonstrated on an industrial case study related to planning of infrequent cold water pressure testing of LPG storage tanks, and the process and results of this case study are presented and discussed. The plant management was provided with a detailed list of the main tasks (22), sub-tasks (115), the specific risks identified (26, considering

Abbreviations: BBN, Bayesian Belief Network; CEA, cost effectiveness analysis; GDP, Gross Domestic Product; IDDA, Integrated Dynamic Decision Analysis; LPG, Liquefied Petroleum Gas; SPACCO, Solutore Probabilistico Accoppiato a Calcolo delle COnseguenze (Probabilistic Solver Coupled with Consequences Evolution); VAR, value at risk.

* Corresponding author.
E-mail address: marko.gerbec@ijs.si (M. Gerbec).

http://dx.doi.org/10.1016/j.ssci.2016.10.015
0925-7535/© 2016 Elsevier Ltd. All rights reserved.

procedural delays, occupational safety and process safety) and the specific recommendations (20) for safety and time optimization of the planned testing procedure. A short summary of the case study is provided in Table A.1.

While it was not possible to carry out the actual field-testing procedure in order to compare the performance with the tasks and recommendations in mentioned paper, a comparative risk assessment and cost effectiveness analysis is needed. In this paper, the risk assessment of the original procedure and the optimized one are reported, comparing the results of two different approaches, using Bayesian Belief Networks (BBNs) and Integrated Dynamic Decision Analysis, that will be briefly described in the next section.

With the aim of assessing the probabilities and damages related to the hazards pertaining to the planned cold water pressure testing procedure, the following have to be considered:

a. The safety analysis to date (Gerbec et al., this issue, Section 3.3) found three types of unwanted consequences of the testing procedure: (i) Procedural delays (work delays/ delay risks), (ii) occupational safety risks and (iii) process safety risks.
b. For each consequence type, a probability of occurrence is to be assessed in order to evaluate the risk of potential delays, injuries and damages per procedure execution. Overall consequences shall be aggregated e.g., using monetary values.
c. As for the duration of specific tasks and sub-tasks (Gerbec et al., this issue, Section 3.4), in order to assess all three types of the risks, also the failure probabilities have to be modelled for all the sub-tasks (for example, the 'Optimized' procedure has in total 25 main and 115 sub-tasks).
d. In order to evaluate the gains from the development of operational & safety optimization of the testing procedure, a comparative risk assessment among the 'Original' and 'Optimized' procedures is needed.

Once the objectives and needs of the analysis have been identified, the available information and methods are described as follows. The types of consequences per failure events were identified mainly during the *Task Analysis* and *Safety Analysis* steps (Gerbec et al., this issue). The main interrelated events are related to the task *Decision making* (task 17 in task analysis for 'Optimized' procedure alternative) after visual inspection, about potentially also pursuing Ultrasound testing and X-ray testing, respectively. While that is explicitly noted in the task analysis for the 'Optimized' procedure alternative, that of course applies also to the 'Original' alternative, but was not yet explicitly noted in its task analysis. The presence of interrelated events makes the classical fault tree method not suitable and also tracking of sub-tasks and consequence types during procedure progress is difficult. The event tree method would be in principle possible to use, but its construction with large number of branches (over 50) is deemed unpractical and hard to manage. Therefore, the authors decided to consider two additional promising methods in a comparative way: (a) Bayesian (Belief) Network (BBN) and (b) Integrated Dynamic Decision Analysis.

The paper is thus organized as follows. Section 2 briefly introduces the approach to using the methods in practice and also the related methods and software tools. Section 3 summarizes the results obtained from use of both methods and for both procedure alternatives. Section 4 provides the results of cost comparisons of both alternatives including cost efficiency analysis (CEA) and Section 5 provides overall conclusions. The overall approach is graphically presented in Fig. 1.

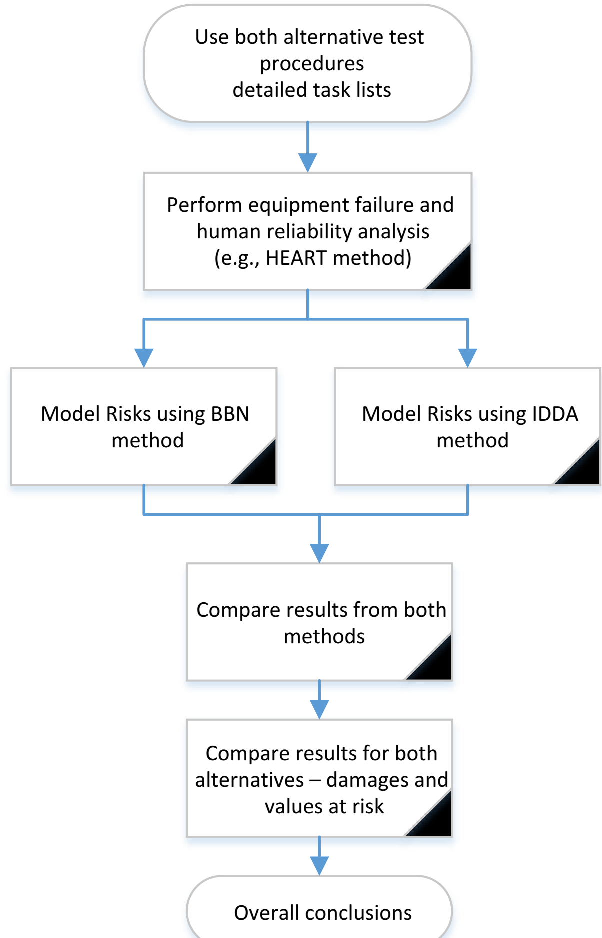

Fig. 1. Graphical presentation of the approach.

2. Approach

2.1. Equipment and human reliability analysis

All the tasks and sub-tasks pertaining to both the Original and Optimized procedure alternatives (Gerbec et al., this issue, Sections 3.3 and 3.4) are classified as either procedural risks, occupational safety risks or process safety risks, if one can occur. It should be noted that the Optimized procedure alternative task numbering was mapped to the numbering in the Original procedure alternative in order to support direct comparisons. The reliability analysis approach consisted of the following steps:

a. As mentioned, specific sub-tasks were subject to a classification of consequences in terms of either procedural delays, occupational safety or process safety. Based on that, the breakdown for the anticipated specific causes (human erroneous actions, equipment failure(s), or both) was done based on the task-based hazard analysis study (Gerbec et al., this issue, Section 3.3) as well as on the recommendations considered for the 'Optimized' alternative (Gerbec et al., this issue, Table 1). If more than one cause was assigned to the specific sub-task, each one was considered separately for the sake of transparency. This resulted in a comprehensive list of 42 sub-tasks/events that can lead to some procedural delays, 20 sub-tasks/events that can lead to occupational accidents and 14 sub-tasks/events that can lead to process

Please cite this article in press as: Gerbec, M., et al. Design of procedures for rare, new or complex processes: Part 2 – Comparative risk assessment and CEA of the case study. Safety Sci. (2016), http://dx.doi.org/10.1016/j.ssci.2016.10.015