Safety Science 79 (2015) 94–104

Contents lists available at ScienceDirect

Safety Science

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

A hybrid risk analysis method for a yacht fuel system safety

Ayhan Mentes *, Emre Ozen

İstanbul Technical University, Faculty of Naval Architecture and Ocean Engineering, 34469 Maslak, İstanbul, Turkey

ARTICLE INFO

Article history:
Received 14 November 2014
Received in revised form 27 May 2015
Accepted 28 May 2015
Available online 14 June 2015

Keywords:
Yacht system design
Yacht fuel system
FMEA
Generalized mixture operators
Ordered weighted geometric averaging
Decision support systems

ABSTRACT

Many current risk assessment methods are used to evaluate, eliminate or mitigate potential risks in an engineering design process. One technique that has been widely used in the design process is known as Failure Mode and Effects Analysis (FMEA). The method assumes failure modes which occur in a system and effects of failures are subsequently evaluated. A risk priority number (RPN) is employed to assess the influence of failures in FMEA. The RPN is a product of three indicators (severity, occurrence and detection) on a numerical scale from 1 to 10. However, the RPN approach has been criticized for its several shortcomings. The assumption that the RPN factors are equally weighted leads to over simplification. Furthermore, the RPN has high duplication rates and does not consider ordered weight rules. An integrated methodology based on ordered weighted geometric averaging (OWGA) and generalized mixture operators (GMOs) is proposed to overcome the inherent shortcomings of RPN and improve design safety. A case study, which assesses the critical causes of failures of a motor yacht fuel system, is presented to demonstrate the applicability of the proposed approach. Obtained results showed that the methodology overcomes duplicated RPN values, and gets a more accurate, reasonable risk assessment in engineering design phases.

1. Introduction

A design process for safety is a combination of hazard identification, risk assessment and control methods to eliminate or mitigate risks. The process is the earliest opportunity to incorporate safety into a design project. Design for safety is an essential process and considered to avoid loss of time, customer dissatisfactions as well as rework in the early design stage in industrial projects. A key to safe design process is choosing the most appropriate risk assessment method (or combination of methods) for the situation at hand. The project manager needs to decide the right approach for the job to eliminate or decrease risks.

There are many different analysis techniques and models that have been developed to aid in conducting risk assessments. These techniques are classified as qualitative, quantitative or hybrid techniques (qualitative–quantitative, semi-quantitative). The qualitative techniques are based both on analytical estimation processes and safety teams' ability. The qualitative approaches are easiest to apply but provide the least degree of insight. Conversely quantitative techniques are most demanding on resources and skill sets, but potentially deliver the most detailed understanding and provide the best basis if significant expenditure is involved (HSE, 2002). The hybrid techniques, present a great complexity due to their ad hoc character that prevents a wide spreading (Marhavilas et al., 2011). Several methods for risk assessment are commonly used in marine industry projects. The mostly used methods and their suitability to phases of design projects can be seen in Table 1. The brief description of the methods is listed below.

Preliminary risk a nalysis (PRA):

PRA was originally used by the Department of Defence of the United States of America requested safety studies of missiles in 1966. The PRA is normally used on new or existing facilities to get an overall but not a detailed view of where the major areas of hazardous concerns exist (Hyatt, 2004). The method can be described as inductive and qualitative technique and the results of the PRA are often presented in a tabulated form (Mentes and Helvacioglu, 2011a).

Checklist analysis:

Checklist analysis is a systematic and detailed examination of the process plant by applying experience of everyday operations and previous incidents in similar plants. It is used primarily to provide structure for interviews, documentation reviews and field

* Corresponding author. Tel.: +90 212 285 6393; fax: +90 212 285 6454.
E-mail address: mentes@itu.edu.tr (A. Mentes).

http://dx.doi.org/10.1016/j.ssci.2015.05.010
0925-7535/

inspections of the system being analysed (ABS, 2000). Checklist analysis is frequently used as a supplement to or integral part of another method (especially what-if analysis) to address specific requirements. The method is useful for most risk assessments, but should not be the only risk identification approach except for standard installations whose risks have been studied in more detail elsewhere (HSE, 2002).

What if analysis:

What-if analysis is a creative brainstorming methodology and employed to evaluate any aspect of a process (HSE, 2005). The technique uses broad, loosely structured questioning to (1) postulate potential upsets that may result in mishaps or system performance problems and (2) ensure that appropriate safeguards against those problems are in place. This technique relies upon a team of experts brainstorming to generate a comprehensive review and can be used for any activity or system (Marhavilas et al., 2011).

Hazard and operability study (HAZOP):

HAZOP is a systematic hazard identification approach which is a team-based method and it allows the team members for brainstorming. The methodology is structured to ensure a thorough and consistent coverage of any system design (Arslan and Er, 2008). The HAZOP analysis is an inductive technique which is an extended FMEA and which can be applied by a multi-disciplinary team using a checklist to stimulate systematic thinking for identifying potential risks and operability problems, particularly in the process industries (Pillay and Wang, 2003).

Fault Tree Analysis (FTA):

The FTA has been extensively used as a powerful technique in risk analysis studies since it was developed in 1962 at Bell Telephone Laboratories in USA. A fault tree is a logical and graphical description of various combinations of failure events to estimate the probability of an accident (Lee et al., 1985). This technique is used to determine the root causes and probability of the occurrence of a specified undesired accident. The failure of a system is considered as a top event of a fault tree. Logical signs, such as "OR" and "AND" gates, are used to represent relationships among various events (Mentes and Helvacioglu, 2011b).

Petri net analysis (PNA):

PNA is an analysis technique for identifying hazards dealing with timing, state transitions, sequencing, and repair. The PNA consists of drawing graphical Petri net (PN) diagrams and analysing these diagrams to locate and understand design problems (Ericson, 2005). The graphical representation of the method may become too complex and the representation of priorities or ordering is hard to manage.

Cause–consequence analysis (CCA):

CCA is an analysis methodology for identifying and evaluating the sequence of events resulting from the occurrence of an initiating event. CCA utilizes a visual logic tree structure known as a cause–consequence diagram (CCD) (Ericson, 2005). The method combines a hazard identification and quantification methodology of fault tree analysis with event tree analysis. With the use of the event tree methodology cause–consequence analysis is able to investigate the incident past the hazard (e.g. item rupture) to the possible consequences (e.g. fire). The methodology is graphical, and once completed the consequences can be related back to their causes (HSE, 2005).

Failure Mode and Effects Analysis (FMEA):

FMEA is a widely used engineering technique for defining, identifying and eliminating potential failures or problems (Chang et al., 2013). A design failure mode and effects analysis (DFMEA) is an analytical method employed by a responsible team to find out the potential failure modes and their associated causes. The DFMEA process begins by developing a listing of what the design is expected to do, and what it is expected not to do (Ford FMEA Handbook, 2011). A designer must show evidence of systematic risk assessment process and provide a report to a person commissioned for design. A good FMEA is an ongoing process whereby it is continuously updated and revised over the life of the process.

Limitations and specifications of risk analysis methods listed above are illustrated in Table 2. Qualitative methods can provide a very useful and effective approach where cost and time are the concerns but quantitative approaches provide higher accuracy. The qualitative risk analysis is an integral part of a risk assessment process in design projects, in practice, but the analysis should be combined with the quantitative technique. Only this combination can ensure that risks, which occur in a design process, are viewed comprehensively. Specialist advice may be needed to choose and apply the most appropriate method; many of the methods can only be used effectively by suitably qualified and experienced assessors (HSE, 2003). Not all of the methods shown in Table 1 are appropriate for design purposes but mainstream design approach tends to rely on with the combinations of brainstorming or Delphi technique (Summerhayes, 2010). Brainstorming involves the assembling of a group of people, who are presented with a specific problem that needs to be solved. These people express any ideas of how to solve the problem they are able to come up with and these ideas are written down (Korombel and Tworek, 2011).

Table 1
Suitability of risk assessment techniques to phases of design projects.

	Concept	Process	Design	Commissioning	Operation	Modification	Decommissioning	Nature of results
PRA	√	√	o	x	x	x	o	Qualitative
Checklists	o	o	√	√	√	√	√	Qualitative
What if	o	o	√	√	√	√	√	Qualitative
HAZOP	x	x	√	√	√	√	√	Qualitative
FTA	√	√	√	√	√	√	√	Both
FMEA	√	√	√	√	√	√	√	Both
Petri-nets	×	√	o	×	×	×	×	Qualitative
CCA	o	o	o	√	√	√	√	Both

√: most suitable.
o: suitable (if used with another method).
×: not suitable.