Reliability Engineering and System Safety 129 (2014) 10–18

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Functional failure modes cause-consequence logic suited for mobile robots used at scientific facilities

Douzi Imran Khan [a,*], Seppo Virtanen [a], Pierre Bonnal [b], A.K Verma [c]

[a] Reliability Engineering and Maintenance Group, Department of Engineering Design, TUT, Finland
[b] Directorate of Accelerators, CERN, Geneva, Switzerland
[c] Stord/Haugesund University College, Haugesund, Norway

ARTICLE INFO

Article history:
Received 4 September 2013
Received in revised form
11 March 2014
Accepted 31 March 2014
Available online 24 April 2014

Keywords:
Cause-consequence logic
Functional failure modes
Mobile robots
RAMS
Risk
Safety
Simulation

ABSTRACT

The scientific facilities emitting ionizing radiation may have some significant failures and hazard issues, in and around their infrastructure. Significantly, this will also cause risks to workers and environment, which has led engineers to explore the use and implementation of mobile robots (MR), in order to reduce or eliminate such risks concerned with safety issues. Safe functioning of MR and the systems working at hazardous facilities is essential and therefore all the systems, structures and components (SSC) of a hazardous facility have to correspond to high reliability, availability, maintainability and safety (=RAMS) demands.

RAMS characteristics have a causal relationship with the risks related to the facility systems availability, safety and life cycle costs. They also form the basis for the operating systems and MR performance, to carry out the desired functions. In this paper we have developed and presented a method for how to consider and model a SSC with respect to its desired functions and also the computer-supported modeling and analysis of functional failure modes cause-consequence logic of a complex system, to ensure its RAMS characteristics during design and development phase, with an application approach to MR power outage. On the basis of experience and assisted by the modeled cause consequence logic it becomes possible to identify the problem areas, which during the design and development phase may reduce the RAMS performance and delay its design and development time.

1. Introduction

When a new technology is applied to the design solution of technical systems, or when a known technology is applied to a new application, it brings some risk. The risk also exists in operation and development of maintenance services without understanding of how an identical system has functioned in similar applications in the same period of time and what type of safety and availability problems and costs it has caused.

The mobile robot used in scientific facilities emitting ionizing radiation must be highly reliable and safe, so that the workers do not have to enter into hazardous area either to repair the facility systems or components, or to repair/replace the failed robot itself. The usage of unreliable and unsafe MR or systems at such facility may not only damage the facility infrastructure but could also raise the risks to workers, who intend to do some maintenance or installation tasks.

Fig. 1 shows the artistic view of iMORO (Iha Mobile Robot) mobile robot at Large Hadron Collider (LHC) of CERN (the European Council for Nuclear Research). iMORO is currently being developed at the Intelligent Hydraulics and Automation (IHA) department of Tampere University of Technology (TUT), as the part of the PURESAFE (Preventing hUman intervention for incREased SAfety in inFrastructures Emitting ionizing radiation) project. Our team is consistently working on the design and development of iMORO and its Reliability, Availability, Maintainability and Safety (RAMS) characteristics, by considering the requirements set by CERN, Geneva and FAIR (Facility for Anti proton and Ion Research), Germany.

RAMS characteristics of the mobile robot will necessarily be affected by errors in the design and development phase that can no longer be fixed during manufacturing or operation phases, or their correction may become extremely expensive. Modeling and analysis of causes and consequences of the mobile robot's functional failure logic form a foundation for qualitative and quantitative investigation of its RAMS performance and risks related to its design entity during the design and development phase. The general term "design entity (DE)" can stand for function, system, structure, component, or any kind of part.

* Corresponding author. Tel.: +358 408490957; fax: +358 400300247
E-mail addresses: imrankhan.douzi@tut.fi (D. Imran Khan), seppo.virtanen@tut.fi (S. Virtanen).

http://dx.doi.org/10.1016/j.ress.2014.03.012
0951-8320/

Fig. 1. iMORO mobile robot at the LHC of CERN, Geneva.

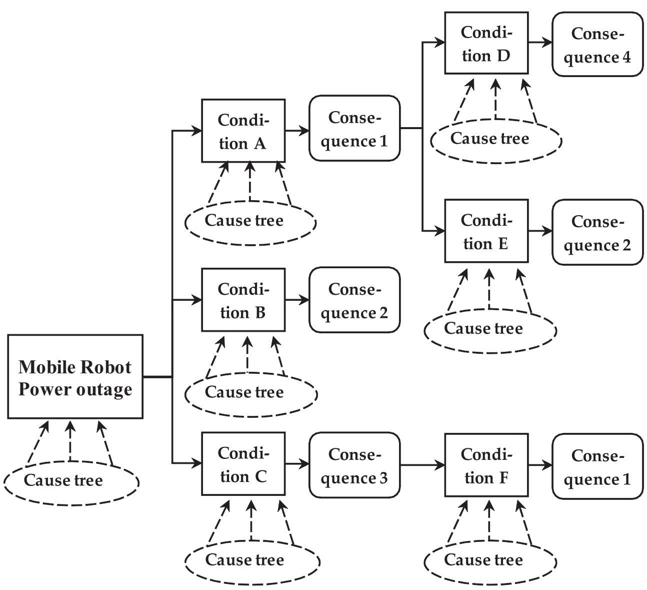

Fig. 2. Structure of functional failure mode cause-consequence tree.

A “cause tree” consists of well-defined causes and interconnected causalities that can lead to the occurrence of a selected event to be studied, which is often called a TOP-event. Thus, a cause tree structure forms a basis for a functional failure logic model of the design entity in question. A “consequence tree” describes the possible chains of consequences initiated from the selected TOP-event. A consequence may further cause other consequences, either exclusively or independently. Finally, a combination of cause trees and consequence trees will be called as “functional failure modes cause-consequence tree”.

An example of functional failure mode cause-consequence tree is shown in Fig. 2. A cause-consequence tree may for example contain several separate chains of events that lead to the same consequence. Note the chains to consequences 1 and 2 in Fig. 2.

Since 1996 the reliability engineering and maintenance research team at TUT has produced design methods, simulation models and software to integrate the RAMS aspects into complex systems and service design and development process. Based on experience and assisted by these methods, it becomes possible to identify the problem areas, which during the design stage may reduce the system and service availability and safety, increase the system life-cycle costs, and delay its development. Ramentor (www.ramentor.com) has successfully developed and refined these models and methods to a commercial software ELMAS (Event Logic Modeling and Analysis Software).

Probabilistic modeling and stochastic simulation have been the main tools in the area of RAMS engineering. In numerous industrial research projects, the provided solutions have usually been mathematical models and methods, as well as large computer-aided calculation and simulation schemes. The research work has been carried out together with Finnish industrial companies, The Finnish Defense Forces and the Finnish Funding Agency for Technology and Innovation (Tekes). The design methods, simulation models and software developed in the research work consist of the following three parts: (1) modeling and analysis of failure cause-consequence logic; (2) how to define and allocate RAMS design requirements, and (3) simulation, calculation and analysis of design solution to fulfill requirements set for RAMS performance.

In this paper we present a computer-supported method for modeling and analyzing cause-consequence structure of functional failure modes, with an application approach to the iMORO mobile robot. In the next two papers we will first describe the application of the functional failure modes structure for the management of RAMS requirements and then how to seek out and select the best design solutions which will fulfill requirements set for its RAMS performance.

The structure of the paper is as follows: Section 2 is a short literature review. In Section 3, we discuss the concept of modeling and analyzing cause consequences structure of functional failure modes of MR design requirements. In Section 4, the developed cause-consequence structure of functional failure is introduced with an application to mobile robot power outage, its simulation and results. Section 5 presents the conclusion and proposes future work.

2. Literature review

Large scale scientific facilities and especially those emitting ionizing radiation, could be dangerous for human, infrastructure and the environment, and this has led engineers to explore the implementation and use of mobile robots. The mobile robot used in such facilities must be highly reliable and safe, so that the workers do not have to enter into the dangerous area to repair the facility systems/components or to repair/replace the failed robots itself. Unfortunately, most mobile robots built and currently being designed have poor reliability levels because of unexpected failures, requiring frequent maintenance and repair. The literature data reveals that they are either broken or under repair most of the time and do not provide proper means for predicting and analyzing failures, [1–3].

A failure is defined as the inability of the mobile robot to function normally under stated conditions, which in return would incur some loss(es). Both complete breakdowns and noticeable degradations in performance must be included in the failure logic. The literature data reveals that there are very few mobile robots that have operated for as long as a year without any repair and hence the use of mobile robot(s) in the hazardous scientific facilities without a prior failure analysis is not safe. In today's scenario within the field of mobile robots, model based methods are predominant and they use explicit models of the normal behavior of the mobile robot to detect and diagnose the fault conditions, [4,5]. The common methods for dealing with failures