Safety Science 85 (2016) 241–257

Contents lists available at ScienceDirect

Safety Science

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

Rationale mapping and functional modelling enhanced root cause analysis

Marco Aurisicchio [a,*], Rob Bracewell [b], Becky L. Hooey [c]

[a] Design Engineering Group, Mechanical Engineering Department, Imperial College London, London, United Kingdom
[b] Rolls-Royce, Derby, United Kingdom
[c] San Jose State University at NASA Ames Research Center, Moffett Field, CA, United States

ARTICLE INFO

Article history:
Received 15 December 2014
Received in revised form 18 December 2015
Accepted 20 December 2015
Available online 15 February 2016

Keywords:
Root Cause Analysis (RCA)
Argument-based rationale
Issue Based Information System (IBIS)
Functional modelling
Function Analysis Diagram (FAD)
Space Shuttle Challenger disaster

ABSTRACT

Objective: The process of understanding the causes of adverse events associated with complex engineered systems can be time consuming and expensive. It often requires substantial human and physical resources ranging from a few engineers up to multiple teams of domain specialists from collaborating organisations. The research presented in this article aims to provide more effective support to the analysts involved in root cause analysis (RCA) by exploring the combined application of the Issue Based Information System (IBIS) and the Function Analysis Diagram (FAD) methods. The first method (IBIS) introduces the concept of argument-based rationale for explicit justification of the nodes of a cause–effect chain as well as of redesign decisions, while the second method (FAD) introduces the notion of structure-dependent functional modelling of complex systems in normal and failure states.
Method: Causation data from publicly available technical reports of the Space Shuttle Challenger disaster was reverse-engineered using a root cause analysis approach based on the IBIS and FAD notations. IBIS and FAD were implemented using a free and open source software tool known as designVUE. The approach was evaluated by comparing it to a method for root cause analysis widely used in industry and assessing how it satisfies generic requirements for root cause analysis.
Results: The results show that the proposed IBIS-FAD approach provides a rich description of the causes for an accident presented in a manner that facilitates information access and understanding. The IBIS notation allowed for explicit modelling of the reasons supporting or refuting failure hypotheses along with evidence. The FAD notation provided a clear and concise method to visualise the complex set of non-linear interactions leading to the failure of a system by annotating graphical schematics of the design with the functions exchanged between its components. Finally, the results show that the approach supports the capture and justification of redesign decisions and ties them to initiating problems in a way that promotes the prevention of accident re-occurrence.
Conclusions: Argument-based rationale with IBIS and FAD-style functional modelling are powerful concepts to extend the tool set available to support the root cause analysis process. The approach proposed in this article provides a unique tool that would be of value to academics, practitioners, and regulators concerned with root cause analysis and opportunities to improve the process of understanding adverse events.

1. Introduction

At present, the pace of technological change is faster than ever and system developers are under constant pressure to reduce the time to market. At the same time, newly engineered systems are increasingly complex and have many unknowns in terms of interaction between components and relationships between humans and automation (Leveson, 2004, 2011). The design of these systems requires significant resources to identify and mitigate risks and to understand potential failure modes. However, despite the application of engineering analysis and failure prevention methods, it remains a major challenge for engineering teams to fully understand system behaviour (Marais et al., 2004) and every year serious accidents are reported across a wide range of industries often

* Corresponding author at: Department of Mechanical Engineering, Imperial College London, Exhibition Road, South Kensington Campus, London SW7 2AZ, United Kingdom. Tel.: +44 (0)20 7594 7095.
E-mail addresses: m.aurisicchio@imperial.ac.uk (M. Aurisicchio), rob.bracewell2@rolls-royce.com (R. Bracewell), becky.l.hooey@nasa.gov (B.L. Hooey).

http://dx.doi.org/10.1016/j.ssci.2015.12.022
0925-7535/

resulting in casualties, environmental damage, financial losses and penalties (Saleh et al., 2010). Root cause analysis is proposed to clarify the causes of accidents and prevent future accidents from happening (Kum and Sahin, 2015) by showing how and why redesign solutions will prevent accident reoccurrence.

The results of accident investigations are typically reported in long and detailed documents, which explain the root cause analysis and present the recommendations that are intended to avoid any recurrence of the failures. The value of the conclusions often depends on the analysis methods employed as well as on the ability of the investigators (Dien et al., 2012; Lundberg et al., 2009). Event chain methods such as the Fault Tree Analysis (FTA; Ferry, 1988) and the Fishbone diagram (Ishikawa, 1982) are the industry standard for root cause analysis and have been applied in industries including aerospace, defence, railway, automotive, oil and gas, chemical processing and nuclear. The construction of event chains by analysts usually requires a deep understanding of the system. Event chain methods, using predominantly linear causality relationships (Leveson, 2004), describe how certain behaviours of the system components combine to result in a system failure. The effectiveness of event chain methods has been frequently questioned (Leveson, 2004). Specifically, it is not known how the understanding of accidents generated through these methods can be extended to explain the reasons of accidents. There is also a need to support analysts in explaining how the physical system worked and understanding non-linear systems behaviours during normal operation and non-normal or failure states. Finally, analysts require a method to support the explanation of how and why redesign solutions will prevent accident reoccurrence.

To address these issues, the work presented in this article proposes an approach to enable root cause analysis analysts to: justify the nodes of event chain methods; model system behaviour in normal and failure states; and capture and justify redesign solutions while providing traceability of the root cause analyses results. It is believed that a root cause analysis approach that can address these aims would offer the following benefits. First, such an approach would provide deeper understanding of accidents to prevent future re-occurrence. Second, the approach would help analysts to understand how the system components interacted and what system components failed. Third, the approach would allow to link failure modes, useful and harmful functions, and current and redesigned solutions. The proposed approach, that will be presented here, draws on and expands upon current practice in industry to model the causes of complex system failure (Bracewell et al., 2009; Eng et al., 2012). In particular, it employs the Issue Based Information System (IBIS) notation (Kunz and Rittel, 1970; Bracewell et al., 2009) to map causal chains along with argument-based rationale, and the Function Analysis Diagram (FAD) notation (Aurisicchio et al., 2012; Aurisicchio and Bracewell, 2013b) to model system behaviour in normal and failure states. The main aspects of the approach are illustrated using causality data from the Space Shuttle Challenger disaster. Causality information documented in investigation reports was represented using the IBIS and FAD methods as implemented in a software tool known as the design-Visual-Understanding-Environment (designVUE) (Baroni et al., 2013; Hooey et al., 2014). It is believed that the proposed approach offers a promising extension to the tool set currently available to engineers. This work is important to understand how to aid engineers tasked to investigate major adverse events.

The remainder of this article is structured as follows. Section 2 provides background on root cause analysis and functional modelling methods. Section 3 proposes our novel approach to root cause analysis, which combines application of the IBIS and FAD methods. Section 4 presents a case study based on the analysis of the Space Shuttle Challenger disaster using a reverse engineering approach. In particular, publicly available data from the Space Shuttle Challenger disaster was modelled using the proposed methods. Section 5 evaluates the research results showing how the proposed approach compares to an existing method for root cause analysis and meets a set of requirements extracted from the literature. Section 6 discusses the proposed approach and its limitations are presented in Section 7. Section 8 draws the conclusions of the research.

2. Related work

A distinction can be drawn between theoretical models of accident causation and methods for root cause analysis. Theoretical models explain possible causation mechanisms of accidents based on general frameworks or conceptual hypotheses. They describe generic scenarios for accident occurrences irrespective of the specific setting (Katsakiori et al., 2009). Various theoretical models of accident causation have been proposed over time (e.g., Normal Accident Theory, Perrow, 1999; High Reliability Organisations, Rochlin et al., 1987; Weick, 1987; and Reason's Accident Causation (Swiss Cheese) Model, Reason, 1990) and reviews of such models can be found in (Katsakiori et al., 2009; Saleh et al., 2010). Methods, by contrast, provide practical support to investigate and to explain causation mechanisms. Interestingly, not all methods for root cause analysis have a link to a model of accident causation–event chain methods such as FTA are an example of this. This section reviews methods for root cause analysis and applications of functional modelling to support understanding of failure.

2.1. Root cause analysis

This section focuses on methods for root cause analysis used in industry to clarify the causes of accidents and prevent future accidents from happening. However, it also considers methods for failure prevention applied during the design process to foresee possible future failures. These methods are included as they provide insights into modelling causation.

The list of methods for root cause analysis is long. Comprehensive reviews and comparisons of methods for failure analysis have been presented elsewhere (Livingston et al., 2001; Doggett, 2004, 2005; Gano, 2007; Katsakiori et al., 2009). These methods have been classified according to various dimensions including: (i) the stage of the product development process that they aim to support, e.g., design (failure prevention) or in-service (failure analysis); (ii) the level of guidance and structure that they offer during the root cause analysis process; (iii) the type of information that users have to capture; and (iv) the directionality of the search, i.e., forward or backward in time. This review does not aim to cover the whole set of available methods. Rather it focuses on industry-standard event chain methods for failure analysis and selected systemic methods, i.e., those that consider the whole system including social organisational factors, management, regulations policies, etc. Specifically, the methods selected for review are the Failure Mode Effect Analysis (FMEA) (Stamatis, 1995), the Fishbone diagram (Ishikawa, 1982), the Fault Tree Analysis (FTA) (Ferry, 1988), the Cause Map (ThinkReliability, 2014), the Apollo Root Cause Analysis (Gano, 2007), the Accimap (Svedung and Rasmussen, 2002) and Systems-Theoretic Accident Model and Processes (STAMP), (Leveson, 2004). Each of the selected methods is now reviewed in turn.

FMEA is commonly described as a forward method for failure prevention used to identify the effects of a single failure mode of a system. In addition to the consequence (effect) of the failure mode and the failure mode itself, the method also captures information about the antecedent (cause) of the failure mode. Hence, the analysis is conducted by alternating searches that look forward