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

in time and backward in time. FMEA does not capture information to justify the causal links between a failure mode and its causes and effects.

The Fishbone diagram is a backward method for root cause analysis, which allows causes to be logically and hierarchically structured using pre-defined categories. It has been noted that it does not let users distinguish between necessary and sufficient conditions for the occurrence of an event (Gano, 2007). Another typical criticism of this method is that placing causes in pre-defined categories, e.g., Manpower, Method, Material, Machine Measurement and Environment, does not provide a complete understanding of the causal relationships because it forces the analyst to fit causes into categories which do not always provide accurate description of a failure (Gano, 2007). Despite these limitations, the method is still frequently applied in industry; a recent example of application is the Toyota Motor Corporation Unintended Acceleration Investigation (NASA, 2011).

The FTA is a backward method for root cause analysis typically employed to analyse, using Boolean logic, an undesired state of a system and its causes (Ferry, 1988). FTA is an analytical tool for establishing relations between events but it does not give guidance as to what information to gather.

It is noteworthy that none of the root cause analysis methods discussed thus far (FMEA, the Fishbone diagram and FTA) provides justification for the nodes of a causation chain. That is, they do not support the capture of rationale and evidence to explain why it is believed that an event occurred and led to an effect. This is considered important information for validating a root cause analysis and ensuring that future designs will be able to make use of the lessons-learned from the analysis.

Differently, the next two methods considered in this review (Cause Map and Apollo Root Cause Analysis) do support the analyst in documenting justifications for the nodes of a causation chain, and on this basis they are compared more closely. The Cause Map is a method to visually explain why an event occurred by connecting individual cause–effect relationships to reveal the system of causes for an issue (ThinkReliability, 2014), see Fig. 1a. To help visualise the analysis, evidence can be documented directly on the Cause Map. Evidence refers to information about how it is thought that an event occurred, and can be derived from many sources such as a statement or testimony, a diagram, a historical trend, an experiment or test results. During the analysis, evidence may also disprove a particular cause. When this happens, the evidence that disproves the cause is placed below the cause and the cause is crossed out, but not removed from the Cause Map. This helps capture the causes that were considered, but ultimately determined not to be related to the incident. A limitation of this method is that it does not capture the rationale justifying the degree of certainty that an event occurred and led to an effect.

Apollo Root Cause Analysis is a method for failure analysis that consists of drawing a cause–effect tree (Gano, 2007), see Fig. 1b. It is rooted in four principles of causation: causes and effects are the same thing; causes and effects are part of an infinite continuum of causes; each effect has at least two causes in the form of one or more actions and one or more conditions; and an effect exists only if its causes exist at the same point in time and space. In the Apollo Root Cause Analysis method, causes are distinguished between action causes and condition causes, see Fig. 1b. An action cause is described as 'a cause that interacts with a condition to cause an effect', while a condition cause is described as 'a static cause that exists over time prior to an action bringing them together to cause an effect' (Gano, 2007). Hence, action and condition causes are linked by an AND logic relation. In the Apollo root cause analysis method, evidence can be captured in the form of a short piece of text, see Fig. 1b, with pre-selected options available including observation, written document, verbal statement, heard sounds, as well as smelled, tasted and touched evidence. Additional textual evidence can be captured as a reference but it is not displayed in the main tree. Rather it pops up in an additional window when needed. Similarly to the Cause Map, this method captures the evidence for an event but it falls short of documenting the rationale for why it is thought that an event occurred and led to an effect.

Looking back on the class of traditional methods reviewed, it can be seen that they all rely on tree-like causation structures and as a result they tend to explain failure using a linear logic. In addition, these methods are rarely used to understand non-technical causes (Leveson, 2004) such as management. To address the limitations of traditional methods, a new class of systemic methods (Svedung and Rasmussen, 2002; Leveson, 2004) is emerging, which represent accidents as complex socio-technical systems phenomena (Salmon et al., 2012). Although evaluation of systemic methods is receiving increasing attention, little is currently known about the use of these methods by practitioners (Underwood and Waterson, 2013; Underwood et al., 2016). The Accimap is an example of a method from this class used to graphically represent system failures, decisions and actions involved in accidents. Accimap analyses, based on Rasmussen's risk management framework (Rasmussen, 1997), typically focus on failures across six levels: government policy and budgeting; regulatory bodies and associations; company management; technical and operational management; physical processes and actor activities; and equipment and surroundings. Similarly to Rasmussen's framework, STAMP views accidents in complex systems as resulting from pressures at multiple levels including physical, social and economic (Leveson, 2004). STAMP focuses on safety as a control problem. Hierarchical safety structures with multiple control levels and constraints imposed on the behaviour and interaction of system components are used to describe systems (Leveson, 2004). The events leading to losses are consequently due to inadequate control or enforcement of constraints on the development and operation of systems.

2.2. Functional modelling

Functional modelling has long been applied in engineering to support failure prevention. FMEA is an example of a method for failure prevention involving functional analysis in the early phases of method implementation (Otto and Wood, 2001). There have, however, also been more sophisticated applications of functional modelling in failure prevention (Kmenta et al., 1999; Hari and Weiss, 1999; Stone et al., 2005a, 2005b; El Ariss et al., 2011). One of these is the Function Failure Design Method (FFDM) (Stone et al., 2005a, 2005b). Compared to FMEA, FFDM aims to guide failure prevention during conceptual design using a functional model known as the function structure (Pahl et al., 2007). The function structure is a form-independent functional model (i.e., a model which does not rely on product structure or geometry to model functions) (Aurisicchio et al., 2012; Aurisicchio and Bracewell, 2013b) consisting of specifying the overall function of the product under development and then of determining and mapping the sub-functions involved as blocks and the flows of matter, energy and signals as arrows. Despite this work, there is no evidence in the literature that functional modelling has been used to support root cause analysis in the aftermath of an accident. However, we propose that explaining the behaviour of structures during failure in this manner could prove to be an useful addition to existing root cause analysis methods.

2.3. Summary

Overall, current event chain methods for root cause analysis were found to lack explicit documentation of either the rationale

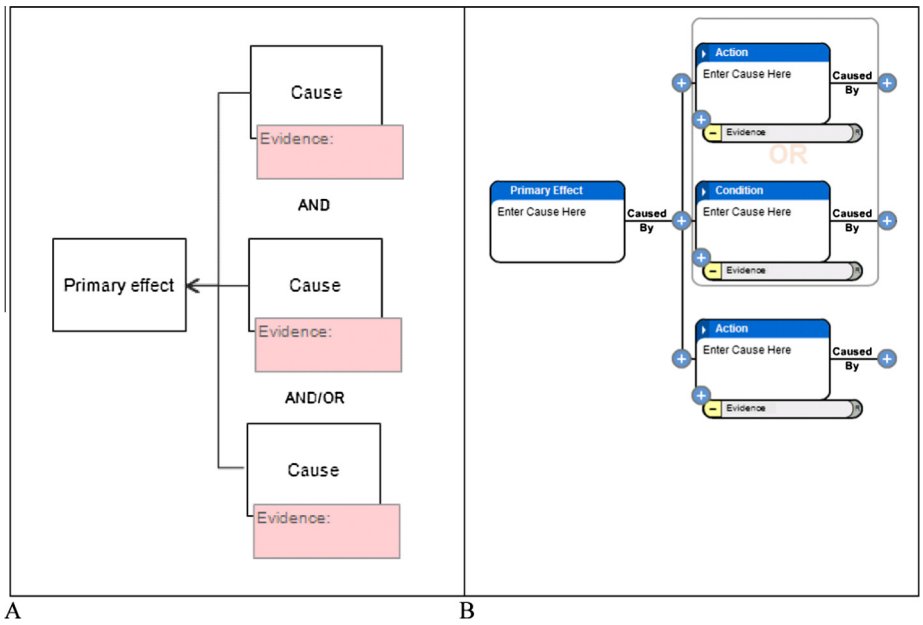

Fig. 1. Cause Map by ThinkReliability (A); Apollo Root Cause Analysis (B).

and evidence for accident occurrence (e.g., FMEA, Fishbone diagram and FTA), or just the rationale (e.g., Cause Map and Apollo Root Cause Analysis). The ability to explain non-linear interactions between systems components was also identified as a limitation of the methods. Additionally, it was found that there is no methodological support to use functional modelling during after-the-fact root cause analysis.

3. A new approach to root cause analysis: IBIS and FAD

This section introduces the IBIS and FAD methods as the main components of the proposed approach to root cause analysis introduced in this article, and designVUE as the software through which the methods were implemented.

3.1. Issue Based Information System (IBIS)

In general, the design and diagnosis of complex systems require engineers and other stakeholders to make decisions by exploring alternative options and arguing for their merits and demerits. As a result the need for argument-based approaches in engineering has long been recognised, and argumentation has been successfully applied in engineering design, reliability engineering and safety engineering through methods such as design rationale charts (Marashi and Davis, 2006; Bracewell et al., 2009; Aurisicchio and Bracewell, 2013a), safety cases (Kelly and McDermid, 2001) and Conclusion, Analysis, Evidence (CAE) diagrams (Johnson, 2001). Each of these methods employs a different notation for argument modelling, which is specific to its context of application.

3.1.1. IBIS for design

Design rationale charts (Bracewell et al., 2009) are based on the Issue Based Information System (IBIS) notation (Kunz and Rittel, 1970), which allows capturing argument-based rationale for an answer to an issue. The notation is composed of four fundamental elements called issue, answer, pro argument and con argument. In design, the argumentation process starts by formulating an issue in the form of a design question, see Fig. 2 (left example). The next step consists of listing possible answers in the form of solutions. The answers are then weighed against each other using arguments. At this point a choice has to be made between the possible answers in order to select 'the best' one.

In root cause analysis the argumentation process still starts by formulating an issue but this time in the form of a why-question or diagnosis question, see Fig. 2 (right example). The next step consists of identifying possible answers in the form of causes. The answers are then assessed on the basis of argument-based rationale and supporting evidence. At this stage further why-questions can be asked in relation to the identified causes to understand if lower-level causes emerge. The result is a causation tree that captures all of the possible causes along with the supporting rationale and evidence. Note that in Fig. 2 the first why-question is explicit (why does the car not start?), while the subsequent why-question (why is the battery flat?) is implicit and the lower-level cause (lights were left on) is linked directly to that identified at the higher level (battery is flat).

3.1.2. IBIS for root cause analysis

IBIS has been extensively applied in engineering design (Marashi and Davis, 2006; Bracewell et al., 2009; Aurisicchio and Bracewell, 2013a) but the literature does not report applications to support root cause analysis, with one exception by Bracewell et al. (2009). This work, considered a pre-cursor to the current project, used IBIS to diagnose an in-service problem to a civil aviation gas turbine, see Fig. 3. The method used by Bracewell et al. (2009) can be classed as an enhanced form of event chain, and combined features of FTA and design rationale capture tools (Kunz and Rittel, 1970). In particular, FTA was effective at clearly delineating cause–effect relationships, and contributed the rigor of Boolean logic to map cause–effect chains with explicit AND and implicit OR relations. The design rationale capture aspect was, instead, responsible for the argument-based approach to justify causation chains. As it can be seen in Fig. 3, the root of the causation tree is a diagnosis question that is answered by identifying six possible causes and articulating rationale in support for or against each hypothesised cause. It is noteworthy that the nodes of the tree have colour-coded states indicating the likelihood that a cause has contributed to the causation mechanism of an accident.

Specifically the map in Fig. 3 shows that a debonding problem occurred to a panel of the fan case of a civil aviation gas turbine, and a range of causes were identified including engine vibration,

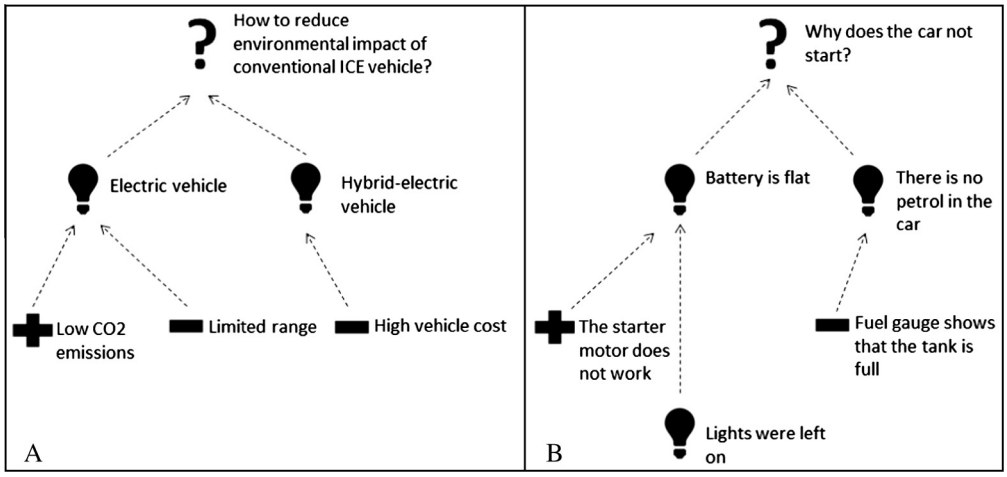

Fig. 2. IBIS notation for design problem solving (A) and root cause analysis (B).

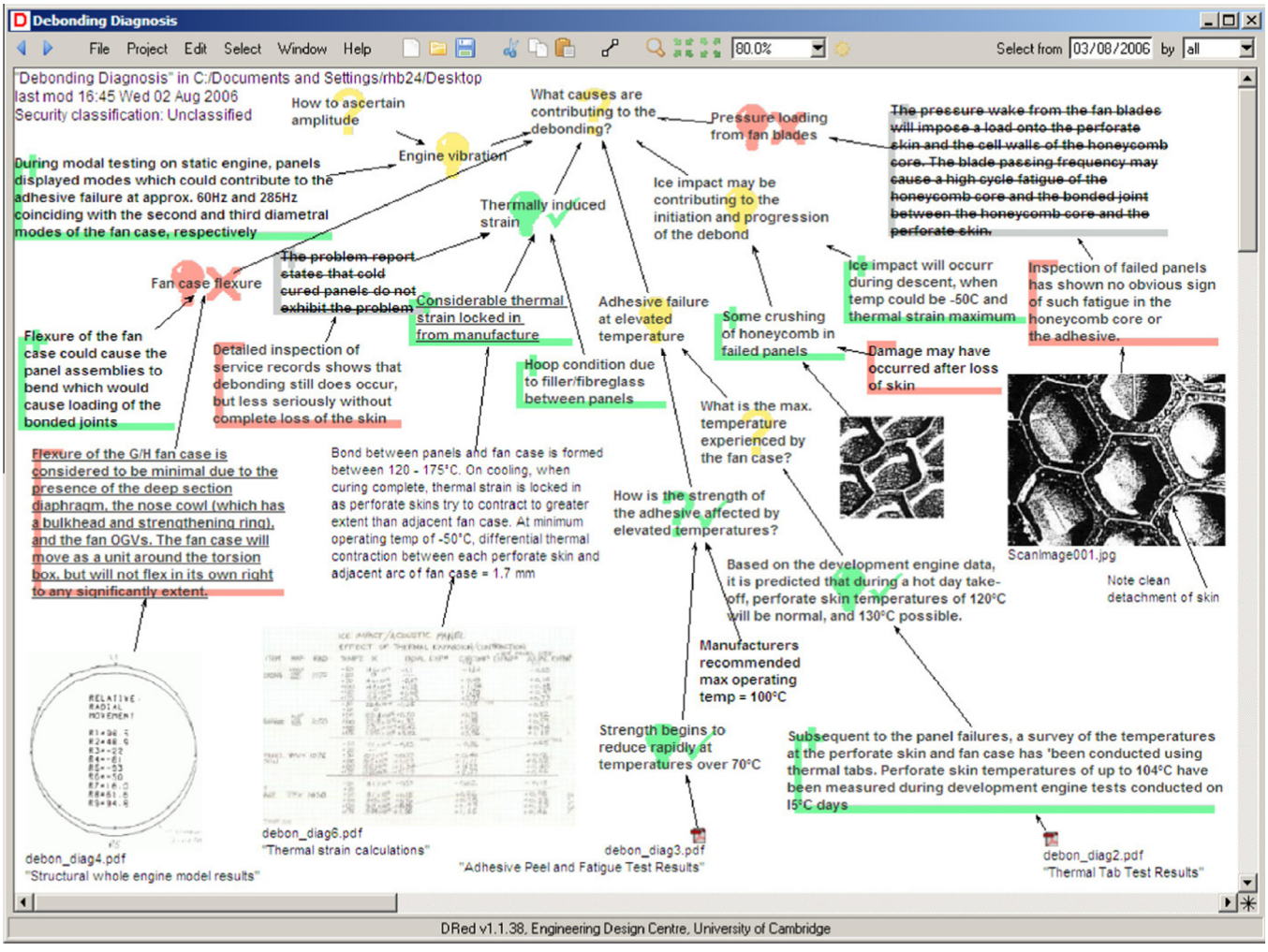

Fig. 3. IBIS notation for root cause analysis as implemented in the DRed tool (Bracewell et al., 2009).

fan case flexure, thermally induced strain, adhesive failure at elevated temperature, ice impact and pressure loading from the fan blades. As can be seen, two causes were rejected (fan case flexure and pressure loading from the fan blades) as indicated by the red[1] answer icon (light bulb with X); one cause was accepted (thermally induced strain) as indicated by the green answer icon (light bulb with checkmark); and, three causes are in the open status (engine vibration, adhesive failure at elevated temperature and ice impact) as indicated by the yellow answer icon (light bulb).

Since its development, the root cause analysis method shown in Fig. 3 has gained extensive acceptance and application in engineering practice at Rolls-Royce plc (Eng et al., 2012). The current research expands on this work (Bracewell et al., 2009) by

[1] For interpretation of color in Figs. 3 and 4, the reader is referred to the web version of this article.

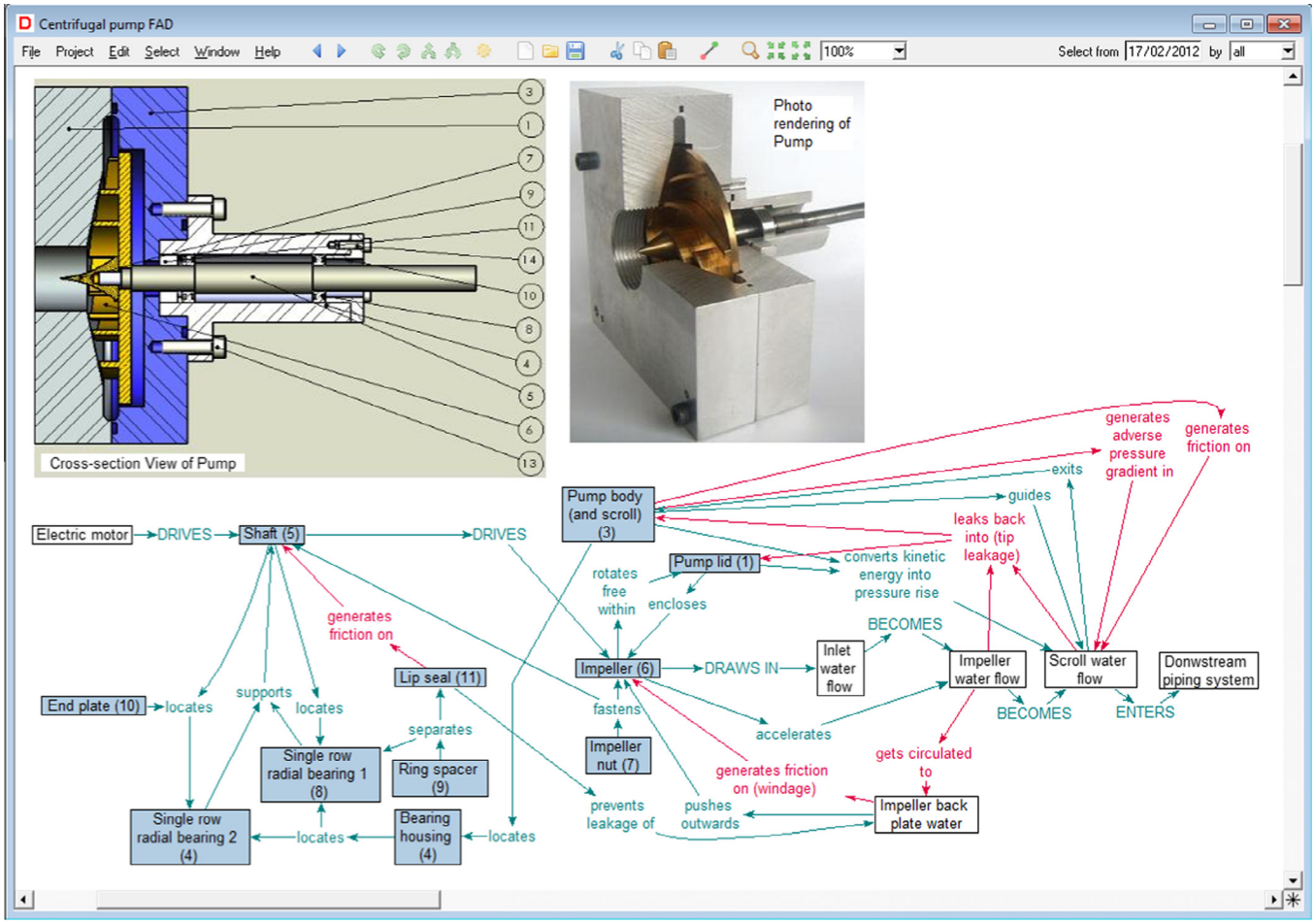

Fig. 4. FAD notation as implemented in the DRed tool (Aurisicchio et al., 2012; Aurisicchio and Bracewell, 2013b).

demonstrating the modelling characteristics of the IBIS method by means of a more comprehensive case study.

3.1.3. The role of argument-based rationale in root cause analysis

We propose that argument-based rationale plays three important roles in root cause analysis. First, it can explain why a cause can or cannot lead to an effect reported at a higher level of a causation tree. In this case, it validates or confutes a cause–effect link. Second, it can explain why a proposed cause to an effect may or may not have occurred. In this case, it validates or confutes a node in a causation tree. It is noteworthy that in these two cases arguments may be used either to support or oppose. For an argument to be valid, empirical or experimental evidence gathered as part of an investigation has to be linked to it to explain on what knowledge basis it stands. When evidence is not documented an argument is weakened and its validity is questionable. As an example see how in Fig. 3 the hypothesis that ice impact may contribute to the de-bonding of the honeycomb panel is supported by a pro argument stating that some failed panels were found to be crushed, which is in turn backed up by photographic evidence. Finally, a third role is that arguments can be used to explain and justify why costly tasks, such as building a test rig to prove or disprove a hypothesis, have to be carried out.

3.2. Function Analysis Diagram (FAD)

Building on the premise that functional modelling can have an important role in explaining the behaviour of a failing structure, this research investigates the application of a form-dependent functional model (i.e., a model which relies on product structure or geometry to model function) known as the Function Analysis Diagram (FAD) (Aurisicchio et al., 2012; Aurisicchio and Bracewell, 2013b) to model system functionality in normal and failure states. We propose that FAD is particularly suitable to supporting reasoning during investigations for two main reasons. The first is that its notation represents functions together with the physical structure of a system, which is important to contextualise troubleshooting in an existing system. The second is that it is the only functional model with notation to represent undesired and harmful functions, which are important to explain the propagation of failure resulting in an accident.

The FAD method consists of drawing a network of *blocks* to represent the physical structure and other resources, and *relations* in the form of an arrow with a label (strictly a relation node with one or more arrows in and out) to represent either useful or harmful actions, see Fig. 4. The diagram in Fig. 4 shows an application of the FAD method to a centrifugal water pump. The blocks in blue background are structural components of the pump, while those in white background represent various states of the water. Useful relations are typically presented in green but shown here as solid lines, e.g., lip seal *prevents leakage of* impeller back plate water, while harmful ones are typically in red but shown here as solid lines, e.g., impeller back plate water *generates friction on* impeller. The concept of graphical mapping of useful and harmful actions between the components of a physical structure was originally published as part of a patent application filed by the TRIZ vendor

Invention Machine Corporation (Devoino et al., 1997). The method was subsequently implemented in the Techoptimizer (now known as Goldfire) software and represented using five elements: component, super-system and product as types of block, and useful and harmful actions as types of relations.

3.3. Rationale for combined use of IBIS and FAD

Both traditional event chain and newer systemic methods for root cause analysis involve investigation of the physical system that failed. Typically during an investigation each analyst has a gradually developing mental model of how the system worked in normal operation, and how the adverse circumstances and events might have impacted that operation. As the analysis proceeds they do their best to keep their individual mental models in synchronisation by various modes of inter-personal communication, but the models remain essentially implicit until documented in narrative text in successive drafts of the accident report. Simultaneous use of the IBIS and FAD methods was perceived as an opportunity to support the event-centric view of root cause analysis employed by traditional methods with a perspective centred on the analysis of components and functions. In particular, this approach is expected to help: (i) create a shared mental model of the system operation; (ii) contextualise the analysis in the engineering problem, (iii) inform root cause analysis with functional reasoning (i.e., the ability to derive and explain the functions of structure) and functional language to achieve improved specification of the events, and (iv) understand and reason with the multiple non-linear interactions exchanged between the components of a system.

3.4. Software implementation of the IBIS and FAD methods

The IBIS and FAD methods were implemented in a software application, known as designVUE, to draw information models (in this article also referred to as maps and trees) mostly consisting of nodes (depicted as boxes with or without icons) and links (depicted as arrows) among them (Baroni et al., 2013). Each model is stored in a separate file. Its Graphical User Interface (GUI) consists primarily of a main window, which contains the menu bar, the toolbar and the editor canvas. The programme does not impose any restriction as to the way in which a model can be drawn. It is up to the user to confer any meaning to a model. Two of the model types supported by designVUE are the IBIS and FAD. In this respect designVUE can be considered an IBIS-derivative tool such as DRed (Bracewell et al., 2009) and Compendium (Buckingham Shum et al., 2006). Its advantages over Compendium and DRed are respectively that it implements an evolved version of the IBIS notation, see Fig. 5, and it is free and open source software (desginVUE, 2015). Another feature of designVUE is that it allows users to create mono-directional hyperlinks between files and external resources, as well as bi-directional hyperlinks, known as *wormhole links*, between its files. In the context of this research, this functionality is considered important to provide access to relevant documents (such as event reports or test results), and connectivity between root cause analysis activities spread across multiple files either because a model is too large to be managed as one entity or because different model types are employed. For example, such functionality has allowed the creation of integrated graphical models, making explicit the teams' developing understanding of both the normal operation and the failure of the system, traceably linked to the growing event tree as they aim to identify root causes and to the emerging redesign solutions as they are proposed.

Table 1
Information sources.

Source	Date
Report to the President on the Space Shuttle Challenger Accident (Rogers, 1986a)	06 June 1986
Report to the President Actions to Implement the Recommendations (Rogers, 1986b)	14 July 1986
Report to the President Implementation of the Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident (Rogers, 1987)	__ June 1987
Power to Explore: A History of Marshall Space Flight Center 1960–1990 (Dunar and Waring, 1999)	1999

4. Application of the new IBIS and FAD-based approach

This section introduces the Space Shuttle Challenger case study, and demonstrates application of the enhanced (IBIS and FAD) approach to root cause analysis proposed in the research.

4.1. Introduction to the case study

The Space Shuttle Challenger disaster occurred in January 1986. The spacecraft broke apart 73 s into its flight leading to the death of its seven crew members. Disintegration of the vehicle began after an O-ring seal in its right solid rocket booster (SRB) failed at lift-off. The O-ring failure caused a breach in the SRB joint it sealed

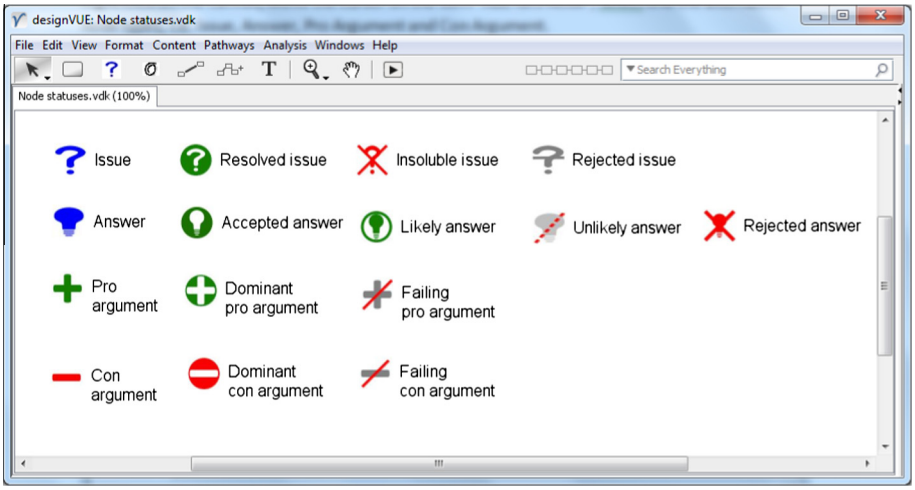

Fig. 5. IBIS notation in designVUE.

allowing pressurised hot gas from within the solid rocket motor to reach the outside and impinge upon the adjacent SRB attachment hardware and external fuel tank. The Space Shuttle Challenger disaster case is probably the most detailed investigation of a modern technological complex system and of the organisation that developed it. The fact that the Space Shuttle Challenger disaster has been studied extensively and from various perspectives makes it an interesting case to evaluate our approach and contrast it to previous work.

4.2. Case study data

Engineering data about the Space Shuttle Challenger disaster was predominantly collected from the publications listed in Table 1 but other sources were used where noted to provide further insights for the analysis. A reverse engineering approach was employed to model the data using the IBIS and FAD methods. The models of the Space Shuttle Challenger root cause analysis presented in the case study were developed using designVUE and rely on the hyperlinking functionality mentioned in Section 3.4 to create an integrated space of root cause analysis and redesign information.

4.3. IBIS-based root cause analysis of the Space Shuttle Challenger disaster

The IBIS-based root cause analysis of the Space Shuttle Challenger disaster is shown in Fig. 6. At a high level the root

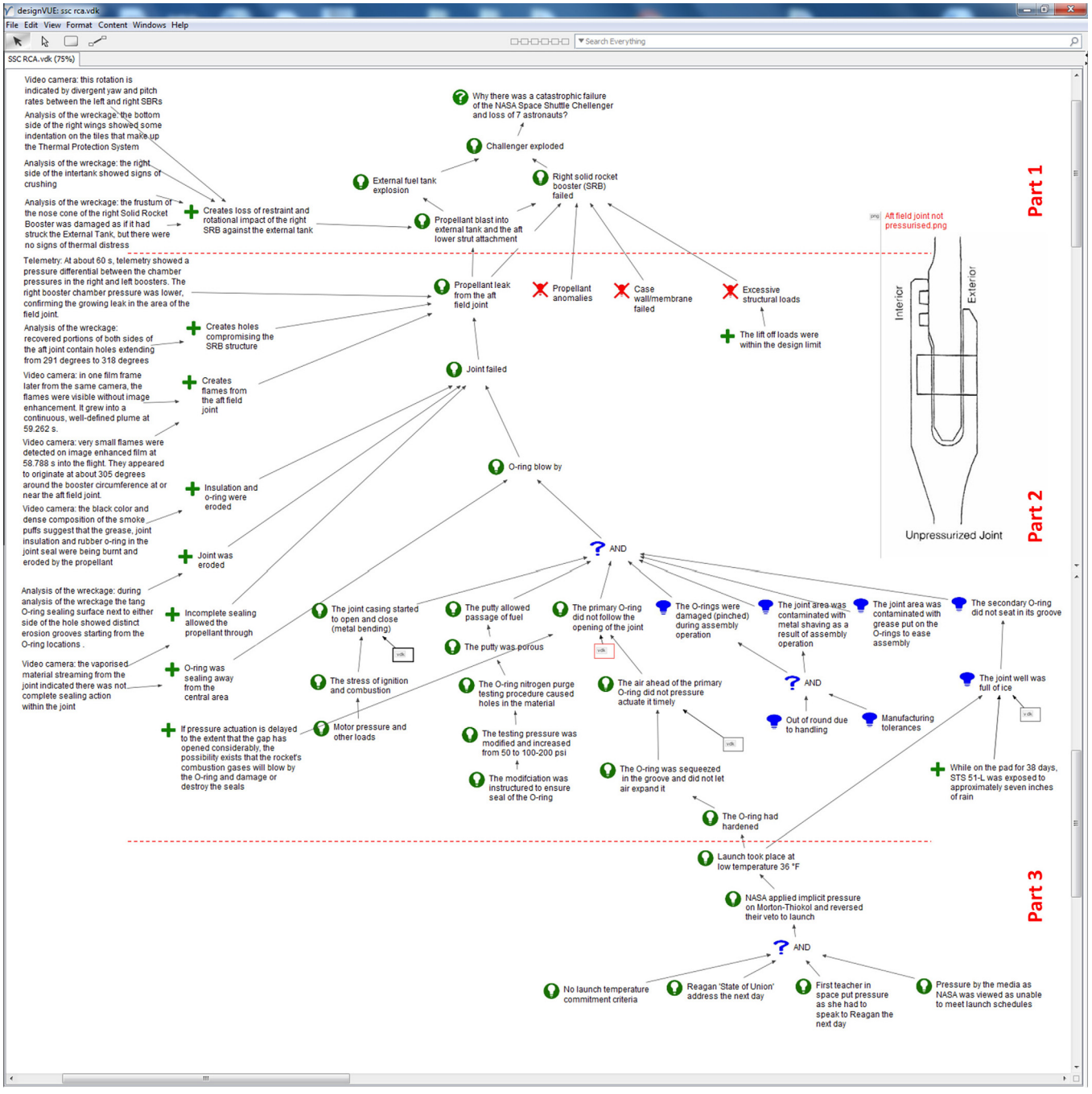

Fig. 6. IBIS-based root cause analysis of the Space Shuttle Challenger disaster.

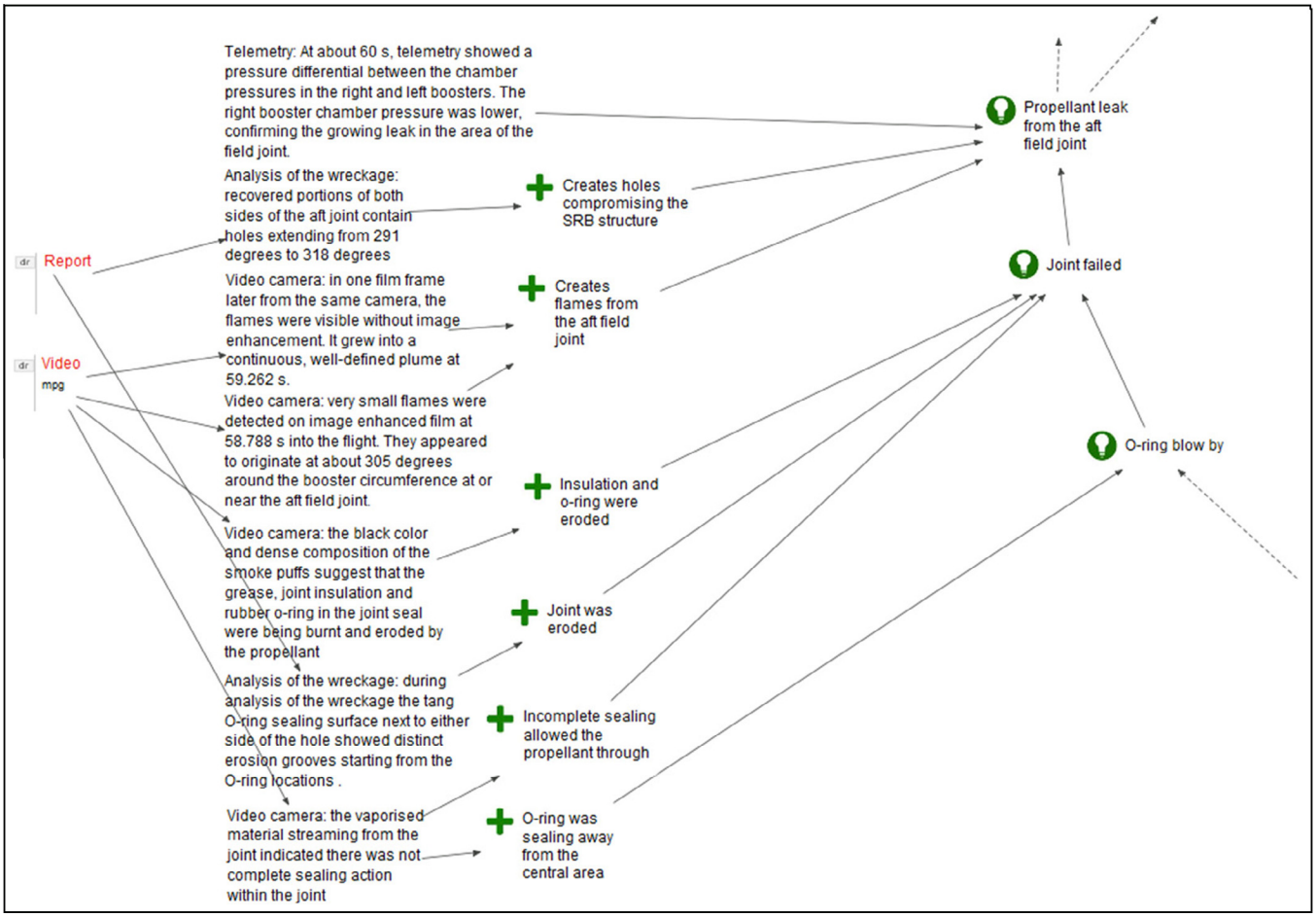

Fig. 7. Detail of the IBIS-based root cause analysis.

cause analysis can be broken down into three main parts: (1) consequences of the joint failure; (2) joint failure; and (3) events leading to the launch, see Fig. 6. Part 1 explains how the seal failure propagated through the space shuttle causing its disintegration. Part 2 focuses on events related to the aft field joint failure. Finally, part 3 is centred around the decision to launch the space shuttle and the pressures exerted on NASA personnel on the launch day. These three aspects involved tracing a combination of technical and management causal factors.

The cause–effect tree starts with an issue node questioning '*why there was a catastrophic failure of Space Shuttle Challenger*', and then develops by mapping various chains of events through answer nodes with linked argument-based rationale and evidence nodes. As it can be seen from the tree in Fig. 6, the method is predominantly based on the answer nodes with issues nodes infrequently used. This is because issues nodes, which would consist of asking why-questions between consecutive answer nodes, are made implicit to simplify the representation. The cause–effect tree shows that at the various levels of the analysis multiple hypotheses were made. Accepted answers at the same level are typically both able to trigger the higher level event, and therefore are linked to each other by an implicit OR relationship. When accepted answers at the same level need to take place concurrently to trigger the event at the higher level an explicit AND relationship is captured, see part 2 of Fig. 6. An important characteristic of the method is the icon graphics and colour coding, which make both the path of accepted causes leading to the root cause and those towards the rejected causes very clear and easy to identify, see Fig. 6. Coloured icons are also used to distinguish if an argument supports or opposes a cause.

In the analysis in Fig. 6 the arguments are laid out to the left of the main cause–effect chain and evidence statements are linked to them or directly to the cause effect chain. This layout was chosen purely for the purpose of making it easier to read the tree. Users can apply alternative layouts to fit their understanding and communication needs. It is noteworthy that in this example for the sake of image clarity the argument and evidence nodes are mapped for a limited number of answer nodes in part 2 of Fig. 6.

An example of the role of argument-based rationale and evidence in root cause analysis is shown in Fig. 7, which zooms on a segment of the root cause analysis presented in Fig. 6 (notably three nodes within part 2) focusing on the O-ring failure. As it can be seen, the first node states that pressurised propellant leaked from the aft field joint. In support of this hypothesis there is telemetry evidence confirming that the pressure of the right solid rocket booster was lower than that of the left solid rocket booster. In addition to this evidence, there are also pro arguments explaining why the propellant leak led to a blast against the external tank and the aft field joint lower strut attachment. Specifically, it can be seen that the growing propellant leak generated flames from the right solid rocket booster and holes in its structure. These pro arguments are supported by evidence statements originating from video-recordings of the shuttle take-off and the wreckage analysis report. Hyperlinks to the files presenting these forms of evidence are also provided from the statements (see video mpg and report pdf files).

4.4. FAD-based failure analysis of the Space Shuttle Challenger aft field joint

The FAD method was used in parallel to IBIS to help trace the part of the root cause analysis tree focusing on the aft field joint behaviour. In addition to modelling the aft field joint during the launch and ignition phase, we have modelled it during the assembly and seal testing phases (see Fig. 8) because the Space Shuttle Challenger investigation showed that concerns emerged in relation to the assembly and seal testing procedures (Rogers, 1986a). Both the intended and actual behaviour during launch and ignition were modelled to identify deviations from expected behaviour.

The FAD model of the actual operation of the aft field joint is presented in Fig. 9. During launch and ignition various interactions occurred in the aft field joint, which contributed to its behaviour and performance. As it can be seen, these were modelled over a schematic of the aft field joint geometry using blocks and relations. The blocks were used to represent the physical structure of the aft field joint (e.g., the primary O-ring, the inside clevis segment, the tang segment, etc.), the fluids and other conditions (e.g., the temperature at launch, and the water captured in the joint due to the overnight rain), while the relations were used to model useful and harmful interactions, see Fig. 9. For example, it is known that on the day and time of the launch the external temperature

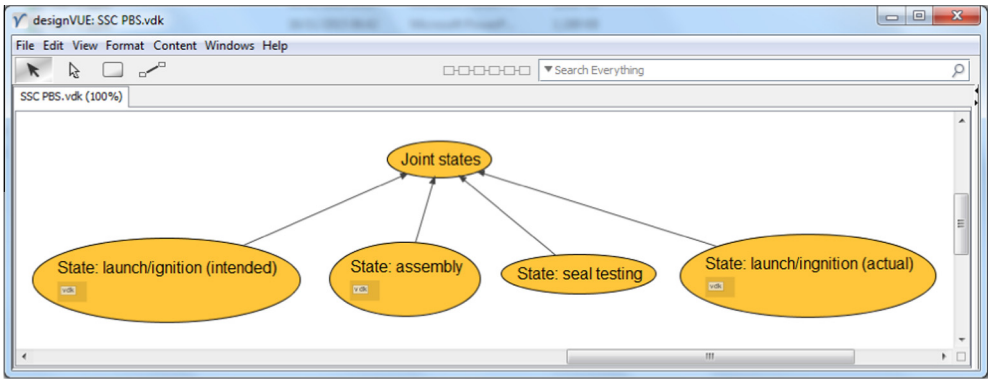

Fig. 8. FAD: aft field joint states.

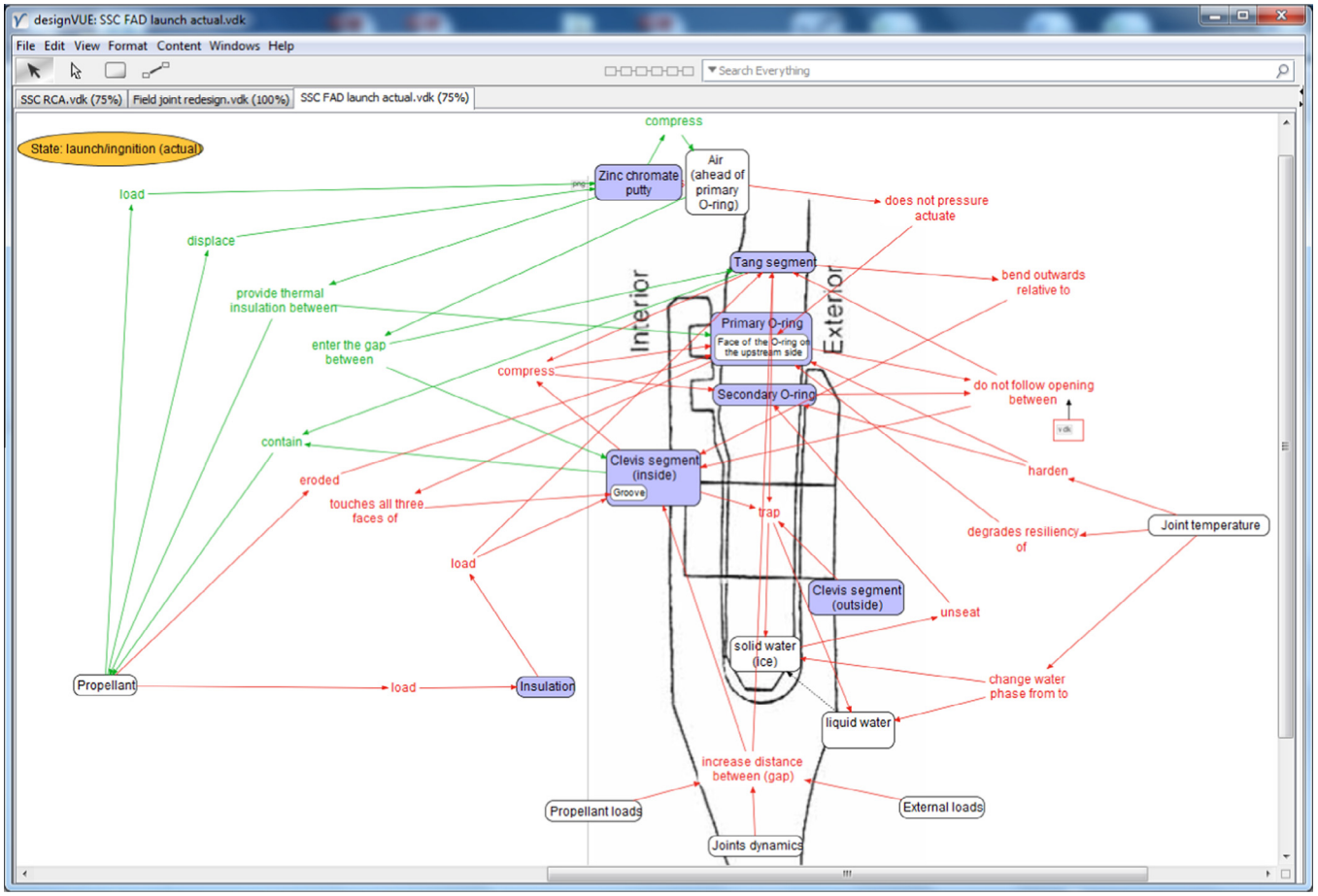

Fig. 9. FAD: aft field joint at launch and ignition.

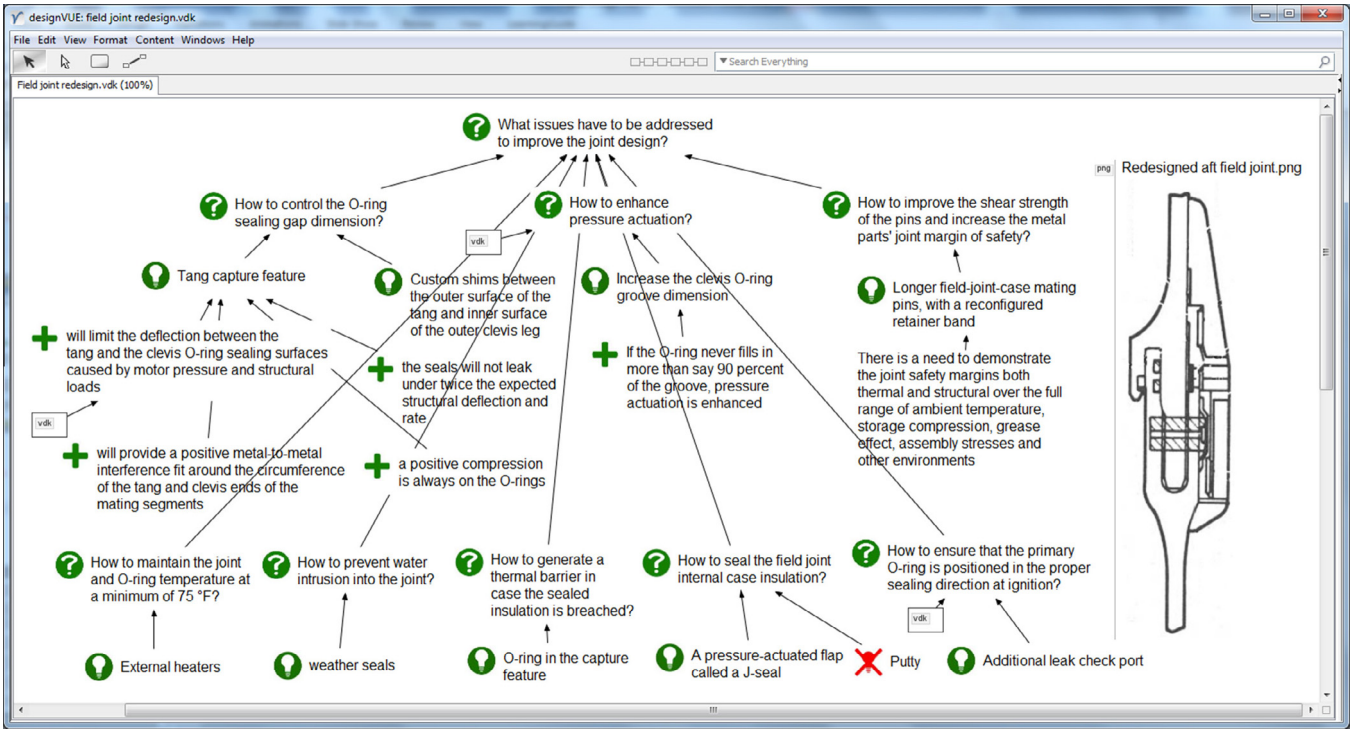

Fig. 10. IBIS-based design rationale of the aft field joint redesign.

hardened and degraded the resiliency of the O-rings. As shown in Fig. 9, to model the behaviour of the aft field joint at a more granular level some of the blocks are provided with nested sub-blocks detailing features of components. For example, the inside clevis segment shows the groove feature. The inclusion of this feature has been important to explain that at launch and ignition the primary O-ring was touching all of the three faces of the groove, i.e., it was not pressure actuated as expected and it did not follow the opening of the aft field joint.

Placing the blocks in proximity of their actual location on the aft field joint geometry was found to be useful to contextualise, understand and reason with the multiple non-linear interactions exchanged in the aft field joint. Hence, the FAD method supported functional reasoning in failure investigation and, in particular, the use of functional language to express the nodes of the IBIS-based root cause analysis. It is noteworthy that harmful interactions in the FAD model are also answer nodes in the IBIS root cause analysis tree presented in Fig. 6 and are bi-directionally hyperlinked to enable traceability. For example, note that in Fig. 9 the harmful action '*did not follow the opening between*' the tang and inside clevis segments has a bi-directional hyperlink next to it which can be navigated to an answer node in part 2 of Fig. 6 which states '*the primary O-ring did not follow the opening of the joint*'. If the user hovers with the cursor on the hyperlink, information about the destination file is provided.

4.5. IBIS-based rationale for the Space Shuttle Challenger aft field joint redesign

The IBIS method was also used to map the recommendations for improved safety and explain how the joint redesigns proposed after the accident will prevent recurrence of the problem. Fig. 10 shows that a number of design questions were formulated, captured in the form of issues, and grouped under a higher-level issue. For example, see that an issue node is used to capture the question '*how to control the O-ring sealing gap dimension*' and a solution is proposed through an answer node to introduce '*a tang capture feature*'. It can also be seen that four pro arguments are used to justify why this solution is adequate. In particular, one of these states that the capture feature '*will limit the deflection between the tang and the clevis O-ring sealing surfaces caused by motor pressure and structural loads*'. In this specific example the pro argument is not backed up by engineering evidence as this was not available in the data analysed but this is thought to be an important practice that should be followed in the method application. It is, however, important to point out that this argument is also hyperlinked to an answer node in the IBIS root cause analysis in Fig. 6, which states that the '*joint casing started to open and close*'. This practice is important as it demonstrates that a problem that emerged during the investigation is addressed by redesign and shows how traceability is maintained between the problem solving and the root cause analysis documents.

5. Evaluation of the new IBIS and FAD-based approach

This section assesses the new IBIS- and FAD-based approach by investigating how it compares to an established root cause analysis method and how it satisfies evaluation requirements for root cause analysis methods that have been established in the literature.

5.1. Evaluation against the Cause Map

To evaluate the root cause analysis approach proposed in this article, we compare it to the Cause Map method. Among the root cause analysis methods presented in Section 2.1, the Cause Map was selected because of its wide application in industrial settings and because of its explicit support for evidence documentation. The comparison focuses on modelling information to justify the nodes of an event chain using IBIS-based root cause analysis and the Cause Map.

Fig. 11 shows a Cause Map for the Space Shuttle Challenger accident as published in (ThinkReliability, 2015). Although more

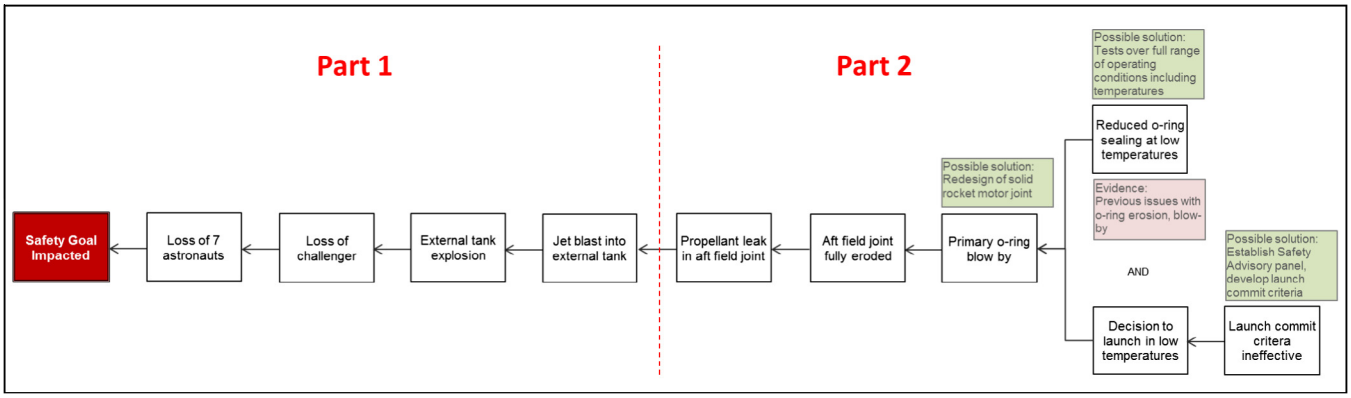

Fig. 11. Challenger Cause Map (ThinkReliability, 2015).

detailed versions of the Challenger Cause Map were developed by ThinkReliability as shown in Galley and Griffith, 2014, these were deemed not important for the argument made in this section.

The node labelled "Safety Goal Impacted" to the far left of Fig. 11 (in dark-colour background) is the root of the tree. The chain of nodes linked to the root (in white-colour background) visually explains the sequence of events that occurred. The nodes with headings *evidence* and *possible solution* (in light-colour background) capture respectively evidence and redesign solutions.

The first point of comparison between the Cause Map and the IBIS-based root cause analysis method is the event chain generated with each approach. It is noteworthy that there is very close correspondence between the two approaches as can be seen by comparing the nodes of the Challenger Cause Map in Fig. 11 to the IBIS map in Fig. 6. Specifically, the first three nodes in part 2 of Fig. 11 (propellant leak in aft field joint; aft field joint fully eroded; and primary O-ring blow by) correspond to those for the IBIS map in Fig. 7.

Another similarity between the two methods is their ability to capture evidence. For example, the Cause Map (Fig. 11) includes a statement of evidence citing previous issues with O-ring erosion and the IBIS map (Fig. 7) shows examples of evidence based on analysis reports and video clips of the shuttle take-off. However, it is noted that even though the Cause Map does allow for the capture of evidence statements, the sample event chain shown in Fig. 11 includes only one instance, suggesting that the degree to which evidence is documented may be dependent on the analyst (note that this applies also to the detailed Challenger Causal Maps in Galley and Griffith, 2014). In this research we have, instead, shown how arguments and evidence can be systematically captured using the IBIS map.

One main difference between the Cause Map and IBIS map involves the capture of argument-based rationale, or the reasons for why an event occurred and why it was believed that it could or could not lead to the effect reported at a higher level of the causation tree. The Cause Map does not support the documentation of argument-based rationale, whereas the IBIS map enables the analysts to justify the nodes of the event chain adding 'pro' or 'con' arguments. For example, recall that in Fig. 7, it was shown that there were two arguments that supported the hypothesis that there was a propellant leak from the aft field joint (the leak generated flames and holes in the structure).

Another difference between the two methods lies in how redesign information is captured. Fig. 11 indicates that the Cause Map method mixes root cause analysis and redesign information within the same canvas with the risk of cluttering the map and compromising its legibility. This is in contrast to the approach proposed in this article, in which these two aspects of the analysis are captured in separate files, which are then hyperlinked for the purpose of providing traceability. It is believed that separating root cause analysis and redesign information is beneficial because these are separate activities often carried out by different engineering teams. In addition, as we have shown, this practice allows capturing a detailed redesign information space including accepted and rejected solutions together with their design rationale.

Finally, the current approach is unique in that it supplements the event chain documentation with the FAD component. As has been argued previously, this is advantageous because it can help contextualise the analysis with functional reasoning and supports understanding of non-linear interactions between system components.

Overall, the comparison between these two methods shows that while both produce similar event chains, the IBIS method introduces a systematic practice for capturing argument-based rationale and evidence, which provides important information to explain why events in a causal chain occurred and led to specific effects. In sum, it is argued that the IBIS approach yields richer, more useful, and reusable information.

5.2. Evaluation against requirements for root cause analysis methods

Another route to evaluate the proposed IBIS- and FAD-based root cause analysis approach is to compare it to established root cause analysis method requirements available in the literature. Reviews of requirements used for this purpose can be found in Gano, 2007, and Katsakiori et al., 2009. The six criteria proposed by Gano (Gano, 2007) and five requirements identified by Katsakiori et al. (2009) are presented in Table 2. A major difference between the two sets of requirements is that Gano focused on aspects specific to the root cause analysis process, while Katsakiori considered a broader set of aspects including, for example, the application field of the method and the training required. Comparing the two sets it was found that some requirements overlap, and a total of eight unique requirements was identified, see Table 2, which will be used to evaluate the IBIS- and FAD-based approach proposed in this research.

The proposed approach, involving the concurrent use of the IBIS and FAD methods, is now evaluated against the eight requirements. Before presenting the evaluation it is worth stating that the IBIS method has been extensively used in Rolls-Royce to support the root cause analysis of advanced propulsion systems for aerospace applications (Aurisicchio and Bracewell, 2013a). Despite being used to support the investigation of aerospace systems, there is nothing in the IBIS method that would prevent it from being used in other domains as the content is not specific. The origins of the IBIS method as used in this particular application can be

Table 2
Evaluation requirements for root cause analysis methods.

Requirement	(Gano, 2007)	(Katsakiori et al., 2009)
R1: descriptive I	Clearly defines the problem and its significance to the problem owner	
R1: descriptive II	Clearly delineates the known causal relationships that combine to cause the problem; clearly establish causal relationships between the root cause(s) and the defined problem	Provides a detailed description of the accident
R3: revealing		Searches for underlying causes
R4: evidence	Clearly presents the evidence used to support the existence of identified causes	
R5: consequential	Clearly explain how the solutions will prevent recurrence of the defined problem	Generates recommendations for improved safety
R6: reporting	Clearly documents criteria 1 through to 5 in a final root cause analysis report so others can easily follow the logic of the analysis	
R7: validation		Has been validated
R8: practical		Requires *minimal* education and training in order to use

Note that two requirements proposed in (Gano, 2007) are classed as descriptive II; and the *application field* and *theoretical origin* requirements proposed in (Katsakiori et al., 2009) are omitted because they are more descriptive in nature than evaluative.

traced to FTA, which is not based on any specific accident model (Katsakiori et al., 2009). Hence, IBIS does not carry a distinct theoretical view on accident causation.

Requirement 1: descriptive I (Clearly define the problem). This requirement entails specifying what happened when and where. In the proposed approach, the major problem, i.e., the loss of the Space Shuttle Challenger and its crewmembers, is formulated and captured by means of an issue node, which is also the root of the IBIS tree structure. The significance of the problem statement can be supported by linking arguments and evidence. For example, event reports can be linked to the root of the tree to inform the initial investigation of the problem. It is important to mention that while the IBIS tree-structure enables the capture of this information, there is nothing in the approach that guides users to capture specific information categories. It is rather up to the analyst to determine how to achieve this.

Requirement 2: descriptive II (Provide a detailed description of the accident). This requirement implies identifying the causal relationships linking the root cause to the problem. The proposed approach addresses this requirement in four ways. First, the IBIS method, albeit dependent on the analyst's skill and ability, captures the relationships between causes at different levels using a clear logic. Second, the IBIS method allows showing the pathway from the initial problem towards its root causes using a clear visual notation. This is expected to help focus the attention of an investigation team on the current most likely hypothesis as well as to communicate the current state of an investigation to stakeholders. Third, the FAD method supports causal thinking in the context of the structure and behaviour of the system being analysed. Given that FAD is also applicable with newer systemic methods, and that it can be used for hierarchical modelling of a whole system structure and behaviour (Aurisicchio et al., 2012), the method addresses the need for more sophisticated analytical tools advocated in previous research (Leveson, 2011). Fourth, the FAD method helps visualise and reason with multiple events which are often best modelled through a non-linear diagram (Leveson, 2004). Hence, the FAD method provides useful information to complement the predominantly linear logic supported by IBIS.

Requirement 3: revealing (Search for underlying causes). This requirement refers to extending analyses beyond technical causes, an issue that has long limited the understanding of accidents. Event chain methods are often criticised because they do not allow fitting all types of causal factors (Leveson, 2004). However, although IBIS for root cause analysis may be considered an event chain method, it does not explicitly make a distinction between immediate and underlying causes. It is up to the user's ability to pursue an investigation until the root causal factors, whether they are related to technical, operator or management issues, are uncovered. The case study has shown that the IBIS method can be used to map both technical and management-oriented causes. Hence, it seems that the method is fit to model most causes and that its outcomes depend on the perspective of the user on accident causation rather than on the method itself.

Requirement 4: evidence (Clearly present the evidence). This requirement refers to explicitly capturing causation evidence, i.e., information about how an event occurred. The IBIS method fulfils this requirement because it can support the capture of evidence. However, it goes beyond evidence documentation as it captures also argument-based rationale, i.e., the reasons for why an event occurred and led to a certain effect. This aspect of the method aligns well with the perspectives reported in (Leveson, 2004), where a shift is advocated from understanding accidents in terms of causes (which have a limited blame orientation) to understanding accidents in terms of reasons to prevent future re-occurrence.

Requirement 5: consequential (Clearly explain how the solution addresses the problem). This requirement refers to formulating specific redesign recommendations for accident prevention. In the proposed approach this requirement is satisfied because the IBIS method is used both to diagnose a problem and to propose solutions while maintaining forward and backward traceability between the maps for root cause analysis and design. This is a distinctive feature of the proposed approach as it ensures that a causal relationship exists between the root causes and the corrective actions.

Requirement 6: reporting (Clearly document the logic for the analysis). This requirement entails documenting the logic for the analysis. It can be considered addressed as the IBIS method leaves users with a justified cause–effect tree and a rationalised design that can be manually converted from a diagrammatic form to a linear narrative such as those in the technical reports commonly produced at the end of failure investigations.

Requirement 7: validation (Has been validated). This requirement is considered a prerequisite for the use of a method. Validation is commonly considered to include two components: reliability and validity. A method is reliable if multiple users use the method and reach the same conclusions, whereas a method is valid if there is correspondence between the results of the analysis and reality (Katsakiori et al., 2009). The proposed approach, like the large majority of the failure analysis methods in the literature (Katsakiori et al., 2009), was not tested for either of these and, therefore, still requires a formal research-based validation. However, the IBIS method as implemented in the DRed tool (Bracewell et al., 2009) has been extensively used by engineers in Rolls-Royce to support the root cause analysis of real world problems. For example, the method was used during the diagnosis of the 2008 British Airways accident (King, 2010), in which a Boeing 777-236ER experienced an engine failure, while carrying out an approach to London Heathrow Airport. The method was used internally by Rolls Royce (the engine manufacturer) to analyse potential causes of the engine failure as well as to support

communication with the airline, the aircraft manufacturer and the aviation authority. A mark of the perceived effectiveness of the method is that it was again used three years later, in the investigation of the uncontained engine failure on Qantas QF32, an Airbus A380 climbing through 7000 ft after departure from Singapore Changi Airport (Research Excellence Framework, 2014). The Rolls-Royce Chief Engineer and the Chief Design Engineer of the Trent 900 engine at the time, and their team of approximately 300 engineers, made extensive use of DRed in conducting the root cause analysis. Once the root cause was established beyond reasonable doubt, DRed was used again to evaluate the design solution (Research Excellence Framework, 2014). On the basis of this acceptance it is argued that the method provides benefits to its users. Differently, the FAD extension requires further acceptance, research, and application to real problems before considering any formal validation.

Requirement 8: practical (Require minimal education and training). This requirement refers to a user's ability to apply the method with minimal education and training. The IBIS-based approach to root cause analysis has been taught in Rolls-Royce through two-hour training sessions. Training has typically consisted of introducing the IBIS notation to users and showing its application to support root cause analysis by means of past accident case studies. The use of IBIS for root cause analysis differs substantially from conventional use in design as the diagram often results in long chains of causal factors underpinned by arguments. The method was developed in close consultation with accident investigation engineers to address the limitations of current practices at the time of the research. Its wide acceptance by the Rolls-Royce accident investigation community can be taken as a measure of its ease of use. The FAD component of the approach is new and, therefore, its training requirements for root cause analysis are not known.

6. Discussion

This research was undertaken to improve the practice of root cause analysis and support effective redesign. The approach presented in this article consists of using the IBIS notation to build a FTA-style event chain with supporting argument-based rationale, and the FAD notation to model the functional interactions between the components of a system in normal and failure states. In this section we reflect on the types of events covered by the proposed approach, the role of argument-based rationale in organisational safety, and the potential to support the collection of a rich causation knowledge base.

6.1. The need to apply failure analysis methods across the entire lifecycle

As stated earlier in this article the proposed approach is fundamentally an event chain with extensions to support argument and functional modelling. A criticism of traditional event chain models is that they concentrate on the events immediately preceding an accident when the foundations of accidents are often laid years before (Leveson, 2004; Dien et al., 2012). This suggests that accident investigations should 'go upstream' and look into the design and development of failed systems. The reason is that after an event, it is important to make sense of what was not appreciated in real time (Dien et al., 2012). In particular, Leveson (Leveson, 2004), based on research in the context of the Space Shuttle Challenger disaster, has argued that to understand why the accident occurred the following four questions had to be answered: Q1 *why was the joint design unsuccessful in imposing the constraint*, i.e., it did not adequately seal the gap; Q2 *why was the joint design chosen* (what was the decision process); Q3 *was there a different design that might have been more successful*; Q4 *why was the flaw not found during development* (Leveson, 2004). In the next paragraphs we explore how to answer these four questions during an investigation, see Fig. 12.

While we acknowledge that our application of the IBIS and FAD methods has focused on events strictly prior to the accident and it has answered just the first question (Q1) proposed by Leveson (see Fig. 12), we agree that the other questions require inquiry and we believe that our previous research in (Aurisicchio and Bracewell, 2013a; Hooey et al., 2014) proposes a solution. Answering the second (Q2) and third (Q3) question requires uncovering the design rationale for the aft field joint, i.e., the reasons why it was designed the way it is and why it was accepted as a solution over other concepts, see Fig. 12. If the initial design rationale was well documented it would be relatively easy to answer those questions. However, in current engineering practice design rationale is rarely documented. Rather it is often stored in the heads of the engineers who developed the design (Bracewell et al., 2009; Aurisicchio and Bracewell, 2013a). To support the capture of design rationale the authors of this article have proposed to use the IBIS method (Aurisicchio and Bracewell, 2013a; Hooey et al., 2014) as shown for the joint redesign, see Fig. 10. In the context of a failure investigation of a system for which the design rationale was not documented, IBIS could still be used to model it retrospectively and link the tree to the root cause analysis.

Answering the fourth question (Q4) requires reconstructing the development process of the design, see Fig. 12. For example, it is known that during the development and in-service life of the Space Shuttle Challenger, important events occurred well before the accident itself. The outcomes of development processes and in-service experience often exist as data but the understanding and knowledge derived from the interpretation of such data is rarely captured. To support this it is envisaged that the events preceding an accident could be captured through a specific IBIS-based root cause analysis diagram, which is then linked to the main event chain.

process steps	Design phase	Development phase	In-service phase
events	Design events	Development events	Events prior to accident
questions	Q2, Q3	Q4	Q1
methods	IBIS-DR	IBIS-RCA	IBIS-RCA & FAD

LEGEND
IBIS-RCA (root cause analysis); IBIS-DR (design rationale); FAD (function analysis diagram)

Fig. 12. Extending root cause analysis beyond the events strictly prior to an accident.

6.2. The role of argument-based rationale in organisational safety for real-time decision making

In Section 3.1 we proposed that argument-based rationale has important roles in root cause analysis including explaining causal relationships and justifying the investment of costly testing resources. We now want to reflect on additional roles that argument-based rationale can have in organisational safety. To this end we revisit the decision to launch the Space Shuttle Challenger, which was informed by testing data collected during the development phase. This decision is of interest because it has been studied from numerous perspectives including power-oriented and cultural approaches (Antonsen, 2009; Perrow, 1999; Vaughan, 1997). As reported in (Rogers, 1986a), the night before the Challengers' launch the O-ring problem was the subject of teleconferences between NASA and Morton Thiokol (the contractor responsible for the solid rocket booster). The engineers of Morton Thiokol expressed concerns that the combination of rubber O-rings and cold weather could threaten the safety of the mission, and recommended delaying the launch. Ultimately, under immense pressure to proceed with the launch, the engineers' warnings that the combination of rubber O-rings and cold weather could threaten the safety of the mission went unheeded. What is interesting is that in the testimony provided to the Rogers Commission, the Morton Thiokol's engineer who voiced the highest concern about launching in cold weather stated: 'I was not even asked to participate in giving any input to the final decision charts. (...) I did not agree with some of the statements that were being made to support the decision. I was never asked nor polled, and it was clearly a management decision from that point' (Rogers, 1986a, p. 228). Based on this extract, power-oriented theorists have argued that the argument of the Morton Thiokol's engineer was sidelined in the concluding phases of the decision making process (Antonsen, 2009) and that this illustrates how the opinion of the less powerful can disappear when real decisions are made (Antonsen, 2009). Still, theorists supporting a cultural perspective on safety (Vaughan, 1997) have argued that engineers at NASA and Morton Thiokol were immersed into a 'technical culture' centred around positivist rationality. Within this culture, decisions were based on evidence emerging from rigorous quantitative analysis and testing rather than hunches and intuition. Hence, these theorists suggest that the engineers' warnings went unheeded because of a lack of credible supporting evidence. Regardless of which theory better accounts for the sequence of events that happened that day, a system such as IBIS can help bring strong rationale and evidence to the attention of decision makers. It is expected that the accountability that comes from its use has the potential to make arguments persistent and coherently structured, decision-making processes more participatory and to redistribute power and control (Buckingham Shum, 1997). In essence, it can make the arguments underpinning key decisions more explicit and transparent which can support decisions made during the development as well as support the decision making processes during in-service diagnoses of complex engineered systems.

6.3. Towards richer causation knowledge bases

A key strategy to support engineering work is to develop and exploit knowledge bases. In particular, we refer to the knowledge typically documented by engineers through design methods and in technical reports. This research has shown that causation knowledge can be enriched with two important pieces of information. The first is the rationale for why the events in a causal chain occurred and led to specific effects. The second is information linking failure modes, useful and harmful functions, and product structure. For example, the FAD method has captured the relationship between erosion as a failure mode for the seals in the joint, the behaviour of the seals under specific environmental conditions, and the configuration of the seals and the joint. This work can be seen as aligning to the efforts (Stone et al., 2005a, 2005b) to create representations linking functional and failure mode information. However, while in the above research the knowledge was manually extracted from technical reports and presented through a matrix-based approach, this research has proposed a representation for live documentation during failure investigations.

7. Limitations and further work

The main limitation of this work is related to the data used to populate the IBIS and FAD structures. Publicly available technical reports typically cover only the line or lines of investigation that led to the main root causes. Hence, they do not allow mapping the alternatives that an investigation team may have considered while carrying out the work. In addition, reports do not permit mapping the tasks that an investigation team may have identified, justified to management and executed to collect necessary evidence. To gather this type of information there is a need to carry out studies, which involve participation in real investigations.

Various lines of future work are possible to extend this research. The IBIS-based method for root cause analysis was applied to study accident causation but, in line with our argument in Section 6, it could be applied to understand problems that emerge during design and development. In addition, our application of the FAD method was confined to developing understanding of the joint behaviour. However, the FAD method lends itself well to hierarchical modelling (i.e., modelling at different levels of the product breakdown structure of a system) and therefore could be used to model what happened to the Space Shuttle Challenger beyond the aft field joint to show how the problem propagated. It would also be interesting to explore application of the FAD method to model the communication which led to the decision to launch the Space Shuttle Challenger.

8. Conclusions

The increasing complexity of engineered systems makes it difficult to identify all the possible failure modes during design leading to numerous in-service adverse events. Improving the efficacy of current tools for root cause analysis was identified as an important issue both to support investigation teams and to create rich legacy data from which teams can learn. This research has proposed the concept of using both the IBIS and FAD methods to support an enhanced approach to the root cause analysis of complex engineered systems. Specifically, the approach allows tracing enriched event chains, and understanding what system components failed, how the system components interacted and how and why redesign solutions will prevent accident reoccurrence. The research contributes to root cause analysis and engineering design at four levels.

The IBIS method was shown to enable the capture of justified cause–effect trees. In particular, a multilevel cause–effect chain was enriched with argument-based design rationale and therefore its ability to explain a complex series of events augmented. This is a characteristic that sets it apart from traditional methods for root cause analysis.

Although functional reasoning has been applied in failure prevention, e.g., FMEA, this research has proposed a first-of-its-kind application of functional modelling in failure analysis. FAD-style functional modelling, capturing intricate aspects of the events leading to the failure of a complex system, was argued to support reasoning to understand failure causation. The method has

potential to be applied both with traditional and systemic methods for root cause analysis and addresses the need for more sophisticated models of causality based on systems thinking and system theory (Leveson, 2011).

The IBIS method was also shown to be a flexible tool as in addition to supporting root cause analysis, it was used to capture and justify redesign decisions and more importantly to trace them to the initiating problems in a way that validates their effectiveness.

Finally, the research has introduced a software tool, known as designVUE, to produce information models based on the IBIS and FAD methods, and integrate them using various forms of hyperlinks in a way that support root cause analyses.

Acknowledgments

The authors acknowledge the support of the United Kingdom Engineering and Physical Sciences Research Council (EPSRC) through the Impact Acceleration, Pathways to Impact Award (EP/K503733/1), and the National Aeronautics and Space Administration (NASA) Aviation Safety Program (System-wide Safety Assurance: Human Systems Solutions project element). The data underlying this research are publicly available and can be accessed as indicated in Table 1, section 4.2.

References

Antonsen, S., 2009. Safety culture and the issue of power. Safety Sci. 47 (2), 183–191.

Aurisicchio, M., Bracewell, R., Armstrong, G., 2012. The function analysis diagram. In: ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Amer Soc Mechanical Engineers, pp. 849–861.

Aurisicchio, M., Bracewell, RH., 2013a. Capturing an integrated design information space with a diagram-based approach. J. Eng. Des. 24 (6), 397–428.

Aurisicchio, M., Bracewell, R.H., 2013b. The function analysis diagram: intended benefits and co-existence with other functional models. Artif. Intell. Eng. Des., Anal. Manuf. 27 (3), 249–257 (Special Issue on Functional Descriptions in Engineering).

Baroni, P., Romano, M., Toni, F., Aurisicchio, M., Bertanza, G., 2013. An argumentation-based approach for automatic evaluation of design debates. CLIMA XIV, LNAI 8143, 340–356.

Bracewell, R., Wallace, K., Moss, M., Knott, D., 2009. Capturing design rationale. Computer-Aided Des. 41 (3), 173–186.

Buckingham Shum, S.J., 1997. Negotiating the construction and reconstruction of organisational memories. J. Universal Comput. Sci. 3 (8), 889–928.

Buckingham Shum, S.J., Selvin, A.M., Sierhuis, M., Conklin, J., Haley, C.B., Nuseibeh, B., 2006. Hypermedia support for argumentation-based rationale: 15 years on from gIBIS and QOC. In: Dutoit, A.H., McCall, R., Mistrik, I., Paech, B. (Eds.), Rationale Management in Software Engineering. Springer, pp. 111–132.

Devoino, I.G., Koshevoy, O.E., Litvin, S.S., Tsourikov, V., 1997. Computer Based System for Imagining and Analysing an Engineering Object System and Indicating Values of Specific Design Changes, United States Patent 6056428, filed 1997.

desginVUE, 2015. design Visual Understanding Environment <http://www3.imperial.ac.uk/designengineering/tools/designvue> (accessed: 26 November 2015).

Dien, Y., Dechy, N., Guillaume, E., 2012. Accident investigation: from searching direct causes to finding in-depth causes – problem of analysis or/and of analyst? Safety Sci. 50 (6), 1398–1407.

Doggett, A.M., 2004. A statistical comparison of three root cause analysis tools. J. Indust. Technol. 20 (2), 1–9.

Doggett, A.M., 2005. Root cause analysis: a framework for tool selection. The Quality Manage. J. 12 (4), 34–35.

Dunar, A.J., Waring, S.P., 1999. Power to Explore: A History of Marshall Space Flight Center 1960–1990. NASA, NASA History Office, Office of Policy and Plans, Washington DC.

El Ariss, O., Xu, D., Wong, W.E., 2011. Integrating safety analysis with functional modeling. IEEE Trans. Syst., Man, Cybernet., Part A 41 (4), 610–624.

Eng, N., Aurisicchio, M., Bracewell, R., Armstrong, G., 2012. Mapping for design decision support in industry. In: ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Amer. Soc. Mechanical Engineers, pp. 579–590.

Ferry, TS., 1988. Modern Accident Investigation and Analysis. John Wiley & Sons.

Galley, M., Griffith, A., 2014. Lessons from Space Program Disasters, ThinkReliability webinar <https://attendee.gotowebinar.com/recording/4472145161407662091> (accessed: 18 November 2016).

Gano, DL., 2007. Apollo Root Cause Analysis – A New Way of Thinking, Third ed. Apollonian Publications LLC.

Hari, A., Weiss, M.P., 1999. CFMA – an effective FMEA tool for analysis and selection of the concept for a new product. In: Proceedings of the 1999 ASME Design Engineering Technical Conference, Design Theory and Methodology Conference, DETC99/DTM-8756, Las Vegas, NV.

Hooey, B.L., Aurisicchio, M., Bracewell, R., Foyle, D.C., 2014. Evidence-based error analysis: supporting the design of error tolerant systems. In: 16th International Conference, HCI International 2014, Heraklion, Crete, Greece, June 22–27, 2014, Proceedings, Part III, vol. 8512 of Lecture Notes in Computer Science. Springer, pp. 401–412.

Ishikawa, K., 1982. Guide to Quality Control, second ed. Asian Productivity Organization, Tokyo.

Johnson, C., 2001. A case study in the integration of accident reports and constructive design documents. Reliab. Eng. Syst. Safety 71 (3), 311–326.

Katsakiori, P., Sakellaropoulos, G., Manatakis, E., 2009. Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. Safety Sci. 47 (7), 1007–1015.

Kelly, T.P., McDermid, J.A., 2001. A systematic approach to safety case maintenance. Reliab. Eng. Syst. Safety 71 (3), 271–284.

King, D., 2010. Aircraft Accident Report No: 1/2010 (EW/C2008/01/01) <https://assets.digital.cabinet-office.gov.uk/media/5422f3dbe5274a1314000495/1-2010_G-YMMM.pdf> (accessed: 30 October, 2015).

Kmenta, S., Fitch, P., Ishii, K., 1999. Advanced failure modes and effects analysis of complex processes. In: Proceedings of the 1999 ASME Design Engineering Technical Conference, Design for Manufacturing Conference, DETC99/DFM-8939, Las Vegas, NV.

Kum, S., Sahin, B., 2015. A root cause analysis for Arctic Marine accidents from 1993 to 2011. Safety Sci. 74, 206–220.

Kunz, W., Rittel, H.W.J., 1970. Issues as Elements of Information Systems. Center for Planning and Development Research, Berkeley, USA.

Leveson, N., 2004. A new accident model for engineering safer systems. Safety Sci. 42 (4), 237–270.

Leveson, N., 2011. Applying system thinking to analyse and learn from events. Safety Sci. 49 (1), 55–64.

Livingston, A.D., Jackson, G., Priestley, K., 2001. Root causes analysis: Literature review. Contract Research Report 325/2001 Prepared by WS Atkins Consultants Ltd for the Health and Safety Executive. HSE Books, 62.

Lundberg, J., Rollenhagen, C., Hollnagel, E., 2009. What-you-look-for-is-what-you-find the consequences of underlying accident models in eight accident investigation manuals. Safety Sci. 47 (10), 1297–1311.

Marais, K., Dulac, N., Leveson, N., 2004. Beyond normal accidents and high reliability organisations: the need for an alternative approach to safety in complex systems. In: ESD Symposium. MIT, Cambridge, MA.

Marashi, E., Davis, J.P., 2006. An argumentation based method for managing complex issues in design of infrastructural systems. Reliab. Eng. Syst. Safety 91 (12), 1535–1545.

NASA Engineering and Safety Center, 2011. National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation, Appendix B, Technical Report.

Otto, K., Wood, K., 2001. Product Design: Techniques in Reverse Engineering and New Product Development. Prentice Hall.

Pahl, G., Beitz, W., Feldhusen, J., Grote, K.H., 2007. Engineering Design: A Systematic Approach. Springer.

Perrow, C., 1999. Normal Accidents: Living with High Risk Technologies. Princeton University Press.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Safety Sci. 27 (2/3), 183–213.

Reason, J., 1990. The contribution of latent human failures to the breakdown of complex systems. Philos. Trans. R. Soc. Lon. Ser. B, Biol. Sci. 327 (1241), 475–484.

Research Excellence Framework, 2014. United Kingdom Research Excellence Framework Impact Case Study 14057 <http://impact.ref.ac.uk/casestudies2/refservice.svc/GetCaseStudyPDF/14057> (accessed: 26 November 2015).

Rochlin, G.I., La Porte, T.R., Roberts, K.H., 1987. The Self-Designing High Reliability Organization. Naval War College Review, Autumn.

Rogers, W.P., 1986a. Report of the Presidential Commission on the Space Shuttle Challenger Accident <http://history.nasa.gov/rogersrep/genindex.htm> (accessed: 23 May 2014).

Rogers, W.P., 1986b. Actions to Implement the Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident <http://history.nasa.gov/rogersrep/genindex.htm> (accessed: 23 May 2014).

Rogers, W.P., 1987. Implementation of the Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident <http://history.nasa.gov/rogersrep/genindex.htm> (accessed: 23 May 2014).

Salmon, P.M., Cornelissen, M., Trotter, M.J., 2012. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. Safety Sci. 50 (4), 1158–1170.

Saleh, J.H., Marais, K.B., Bakolas, E., Cowlagi, R.V., 2010. Highlights from the literature on accident causation and system safety: review of major ideas, recent contributions, and challenges. Reliab. Eng. Syst. Safety 95 (11), 1105–1116.

Stamatis, D.H., 1995. Failure Mode and Effect Analysis, FMEA from Theory to Execution. ASQ Quality Press, Milwaukee, USA.

Stone, R., Tumer, I.Y., Van Wie, M., 2005a. The function failure design method. J. Mech. Des. 127 (3), 397–407.

Stone, R., Tumer, I.Y., Stock, M.E., 2005b. Linking product functionality to historic failures to improve failure analysis in design. Res. Eng. Des. 16 (1–2), 96–108.

Svedung, I., Rasmussen, J., 2002. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. Safety Sci. 40, 397–417.

ThinkReliability, 2014. Cause Mapping <http://www.thinkreliability.com/> (accessed: 30 Jan 2014).

ThinkReliability, 2015. Challenger Cause Map <http://www.thinkreliability.com/graphics/CauseMaps/CM-Challenger.pdf> (accessed: 16 Nov 2015).

Underwood, P., Waterson, P., 2013. Systemic accident analysis: examining the gap between research and practice. Acc. Anal. Prevent. 55, 154–164.

Underwood, P., Waterson, P., Braithwaite, G., 2016. 'Accident investigation in the wild' – a small scale, field-based evaluation of the STAMP method for accident analysis. Safety Sci. 82, 129–143.

Vaughan, D., 1997. The trickle-down effect: policy decisions, risky work, and the Challenger tragedy. California Manage. Rev. 39 (2), 80–102.

Weick, K.E., 1987. Organizational culture as a source of high reliability. California Manage. Rev. 29 (2), 112–127.