Safety Science 167 (2023) 106275

Contents lists available at ScienceDirect

Safety Science

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

Applying System-Theoretic Process Analysis (STPA)-based methodology supported by Systems Engineering models to a UK rail project

Dapo Oginni [a], Fanny Camelia [b,*], Mikela Chatzimichailidou [c], Timothy L.J. Ferris [b]

[a] WSP, 8 First Street, Manchester M15 4RP, UK
[b] Cranfield University, Defence Academy of the United Kingdom, Shrivenham, SN6 8LA, UK
[c] Arup, 8 Fitzroy Street, London W1T 4BJ, UK

ARTICLE INFO

Keywords:
STPA
Safety risks
Hazards
Rail project
Traditional safety analysis methods

ABSTRACT

Systems safety in railways focuses on providing the necessary assurance that the railway system is operationally safe and meets all relevant regulatory requirements. Safety risks associated with changes in the UK railway are controlled through the Common Safety Method for Risk Evaluation and Assessment (CSM-RA). As part of the CSM-RA framework, various safety analysis methods such as Failure Modes and Effects Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and other traditional analysis methods conducted via expert brainstorming such as Hazard Identification (HAZID) workshops have been relied upon for many years in the UK rail industry; aiming to evaluate and mitigate all reasonably foreseeable hazards. This paper reports a comparison case study of the application of a novel System-Theoretic Process Analysis (STPA)-based methodology against the traditional approach for hazard analysis in UK rail projects. The proposed methodology uses Systems Engineering (SE) models in each of its steps. The application of the novel methodology demonstrates that it is suitable for hazard identification and analysis in complex rail systems. It shows that the approach goes beyond the capabilities of traditional methods, provides insights into the interaction among system components and captures hazards within the context of the whole. The SE models used in this study prove to be valuable not only for illustrating the System of Interest (SOI) visually, but also providing a high-level understanding of the system and a more detailed understanding of component interactions. They also improved the focus, in scope, effectiveness, and efficiency of the analysis.

1. Introduction

The UK rail industry continues to deliver technical, operational, and organisational changes to improve the performance and capacity of the UK's rail network. Systems safety in railways is concerned with providing the necessary assurance that the railway system is operationally safe and meets all relevant regulatory requirements. Safety risks associated with changes in the UK railway are controlled through the Common Safety Method for Risk Evaluation and Assessment (CSM-RA) (Office of Rail and Road, 2018). CSM-RA is an EU regulation utilised as best practice and standard within the UK. It provides a risk management framework that are to be adopted by programmes or projects undertaking a change to the mainline railway. The framework aim to identify all reasonably foreseeable hazards associated with the proposed change, and to eliminate or reduce associated hazards as low as reasonably practicable (Health and Safety Executive, 2022). The framework includes processes to demonstrate compliance through the provision of clear and comprehensive documentary evidence, including a list of hazards, safety measures, and requirements that are necessary to control the risks arising from the identified hazards.

As part of the CSM-RA framework, various safety analysis methods such as Failure Modes and Effects Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and other traditional analysis methods conducted via experts' brainstorming such as Hazard Identification (HAZID) workshops have been relied upon for many years in the UK rail industry; aiming to evaluate and mitigate all reasonably foreseeable hazards (Health and Safety Executive, 2022). However, with the introduction of digitalised solutions in railway systems to support safety–critical functions, the complexity and nature of these systems (i.e., cyber-physical systems), have changed. The increased complexity

* Corresponding author at: Centre for Systems, Simulation and Analysis, Cranfield University, Defence Academy of the United Kingdom, Shrivenham, SN6 8LA, UK.
E-mail addresses: dapo.oginni@wsp.com (D. Oginni), Fanny.Camelia@cranfield.ac.uk (F. Camelia), Mikela.Chatzimichailidou@arup.com (M. Chatzimichailidou), Timothy.Ferris@cranfield.ac.uk (T.L.J. Ferris).

https://doi.org/10.1016/j.ssci.2023.106275
Received 18 November 2022; Received in revised form 20 June 2023; Accepted 19 July 2023
Available online 7 August 2023
0925-7535/© 2023 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

includes changes to human roles within a system boundary. With automation, humans are now increasingly sharing control of systems, and human roles are shifting into positions of higher level decision-making, potentially generating new types of hazards and risks (Chatzimichailidou & Dunsford, 2019). For example, some basic functions of a train operation have changed; with more authority shifting from the human operator to machines, such as setting the train in motion, driving, and stopping train, operation in event of disruption, door closure, etc. The increased complexity of today's software-intensive railway systems can potentially introduce unknowns and undesirable system behaviours, creating new paths to losses or accidents (Rekabi, 2018).

Despite the generally accepted usefulness of traditional safety methods, as noted by practitioners, they may be limited in coping with today's complex systems. Therefore, it raises the question if these methods are the most effective or appropriate in capturing potentially new forms of hazards. The study reported in this paper is motivated by two main entrenched beliefs or assumptions underlying traditional safety methods.

First, well-established traditional safety methods such as FTA, ETA, FMECA, as well as Hazard and Operability Analysis (HAZOP), are based on the *chain of events theory*. That is, accidents are assumed to be caused by a chain of failure events, with each failure directly causing the next one in the chain, as described by accident models, such as Heinrich's Domino and the Swiss-cheese model. It, therefore, assumes that working backwards from a loss event or accident will identify the root cause. Thus, the emphasis is on system components failures and design errors. However, methods based on this approach are not able to capture the dynamics of complex systems that may include nonlinear interactions between their constituent components (Yousefi et al., 2019). The theory may also lead the analyst, i.e. System or Safety Engineer, to consider the underlying events of an accident subjectively (Leveson & Stephanopoulos, 2014).

Second, traditional safety methods employ the principle of *reductionism*; the principle assumes that the system of interest (SOI) can be separated into non-interacting components (Leveson 2011) and then assembled to a whole system with very little, if any, attention to interactions among components. The assumptions underlying the reductionist approach were reasonable in the past when systems were more mechanical and less complex, however, as systems have become increasingly complex over time, component interactions are on the increase, leading to unknown types of failure.

Leveson (2004) introduced a new accident causality model based on systems theory and systems approach to safety called Systems-Theoretic Accident Model and Processes (STAMP). STAMP is a model and a way of thinking about accidents beyond component failures that focus on interactions and controls in a system (Thomas, 2021). In STAMP, accidents are seen to occur not solely due to component failures but also due to dysfunctional interactions between the components within the system as a whole (Yousefi & Rodriguez Hernandez, 2019).

One of the most widely used STAMP-based methodology is the System-Theoretic Process Analysis (STPA). STPA is an iterative hazard analysis methodology that seeks to analyse the potential cause of accidents during design development so that safety risks can be eliminated or controlled (Leveson, 2011). Using STPA, it is assumed that every individual component's behaviour, including events and actions, cannot be understood without taking into account the components' roles and interactions within the overall system (Leveson, 2011). It recognises that there may be unsafe interactions between the components of an SOI with the system environment (Chatzimichailidou et al., 2015).

STPA has been found to be particularly beneficial when dealing with organisational and social factors, human decisions and software design errors (Leveson, 2011). It acknowledges that safety is an emergent property. Emergent properties arising from the interactions of components represent the fundamental concepts of this new way of thinking about accident causation and prevention (Hegde et al., 2019). It is also noteworthy that STPA defines and analyses a continuous control task to impose a set of constraints or requirements necessary to enforce or limit system behaviour rather than defining safety management as prevention of component failures (Yousefi & Rodriguez Hernandez, 2019). According to STPA, accidents often occur as a result of a violation of these constraints between system components (Leveson, 2018). Therefore, the goal of STPA is to control the behaviour of the components and the system, as a whole, to ensure that the safety constraints are enforced in the system under consideration.

Since its introduction, STPA has earned interest and recognition by academics and various industry sectors (Patriarca et al., 2022). It has been cited as an alternative to traditional approaches in dealing with complex systems (Silva, 2019). Recent areas of STPA application include security (Beaumont & Wolthusen, 2019), transport and storage (Samadi & Garbolino, 2018), automotive (Hegde et al., 2019), chemical (Yousefi & Rodriguez Hernandez, 2019), fish farming (Holen & Utne, 2018); other notable sectors include transportation, energy, construction, defence, healthcare, robotics, etc. (Bugalia et al., 2020; Chatzimichailidou & Dunsford, 2019; Jamot & Park, 2019; Patriarca et al., 2022).

Studies about the evaluations and comparisons of STPA to more traditional hazard analysis methods, such as FMECA, FTA, ETA, and HAZOP have been undertaken (Patriarca et al., 2022). An example of such an evaluation is the work by Fowler (2015) that compares STPA with traditional hazard analysis methods. Fowler (2015) concludes that STPA is the most comprehensive form of analysis amongst the other traditional methods. In addition to other comparisons undertaken, Leveson & Thomas (2018) observe that STPA appeared to be less costly in terms of time and resources compared to the traditional methods.

However, STPA application remains less prominent in industry, especially in the UK rail sector (Patriarca et al., 2022). Previous studies by Takata and Nakamura (2019) investigated a possible application of STPA method to an electronic interlocking system in railway, and (Hirao, 2020) evaluated a level crossing control system by using STPA. However, no significant research has been conducted to compare the STPA method to a traditional hazard analysis method within the context of a rail project. Therefore, the study reported in this paper presents a novel investigation into the effectiveness of applying an STPA-based methodology supported by Systems Engineering (SE) models to a rail project. The study compares this innovative STPA-based methodology, in terms of output and process, against the traditional approach to performing hazard analysis for safety assurance within the UK rail sector. It offers a novel perspective and contributes to the existing body of knowledge on hazard management and accident prevention within the rail context.

2. Methods

This paper reports a comparison case study of the application of the proposed STPA-based methodology against the existing approach (i.e., traditional approach) for hazard analysis in UK rail projects. The proposed STPA methodology used SE models in each of its steps. The information on the traditional approach was collected via interviews of Subject Matter Experts (SMEs), individuals with rounded knowledge and experience of traditional approach in UK rail projects.

2.1. Case study

The case study is a Level Crossing and Signalling System upgrade project, herein referred to as LXSS. The LXSS system is a critical and complex system within in the rail network. However, understanding and predicting its behavior, operation and performance can be challenging due to the complex interface and interaction problems between multiple complex signalling systems.

The existing level crossing (LX) is currently Manually Controlled with Gates (MCG), assessed to be approaching the end of serviceable life. Therefore, the project aims to renew expired equipment; to improve LX

safety; and reduce operational expenditure. An option has been selected to renew it as Manually Controlled Crossing with Barriers and Obstacle Detection (MCB-OD). In addition, the LX renewal requires some signalling alterations of the signal box within the controlled area to facilitate the correct working of the MCB-OD level crossing.

The LXSS renewal case study reflects a real-world situation within the UK rail which is constrained by aging infrastructure. It provides a suitable context for assessing the effectiveness of STPA in identifying hazards, safety measures and preventing accidents in rail sector.

2.2. STPA-based methodology supported by Systems Engineering (SE) models

STPA is generally conducted based on four main steps as introduced by Leveson & Thomas (2018); summarised below:

- **Step 1**: define the purpose of the analysis by understanding the SOI and its environment, identifying losses, and identifying system hazards, as well as safety constraints.
- **Step 2**: model the 'control structure' to understand functional relationships, that is the system in its environment and the interaction between the SOI and its environment.
- **Step 3**: identify and mitigate the occurrence of Unsafe Control Actions (UCAs). This is a further analysis of the 'control structure' to discover what could go wrong in a particular context, with the aim of discovering new hazards.
- **Step 4**: identify the loss scenarios or causal factors of the UCAs identified in Step 3, considering the various elements of the 'control structure' against various scenarios.

However, the STPA methodology is not prescriptive, that is, it specifies the activities and results to be achieved, but not the tools or models to be used. Therefore, in this study, the STPA steps are supported by analysis models generally used in the SE process, including the context diagram, the use-case diagram, and the activity diagram (SEBoK Editorial Board, 2022). To illustrate, Leveson & Thomas (2018) suggested that Step 1 consists of identifying stakeholder and stakeholder's loss, and system boundary and system level hazards, without specifying how they could be identified. In this study, pig diagrams and rich pictures are used to identify stakeholder and their losses, while a context diagram was used to identify system boundary and system level hazards. The SE models represent the system under consideration and its contexts and enabled its exploration and analysis.

The STPA are incorporated with SE models to ensure an overall understanding of the system, improve the effectiveness and efficiency of the STPA methodology in identifying losses, hazards, safety constraints, UCAs, and loss scenarios.

Fig. 1 shows the methodology conducted for this study. The original four steps of STPA are illustrated within a light grey box, while the extended STPA methodology supported by SE models is illustrated in the dark grey box. The diagram also shows the approach taken to understand the traditional approach through the SME interviews, followed by a comparison of the proposed STPA approach and the traditional approach.

2.3. Define the purpose of analysis

This first STPA step was conducted by developing and iterating between a pig diagram, a rich picture, and a context diagram to present the

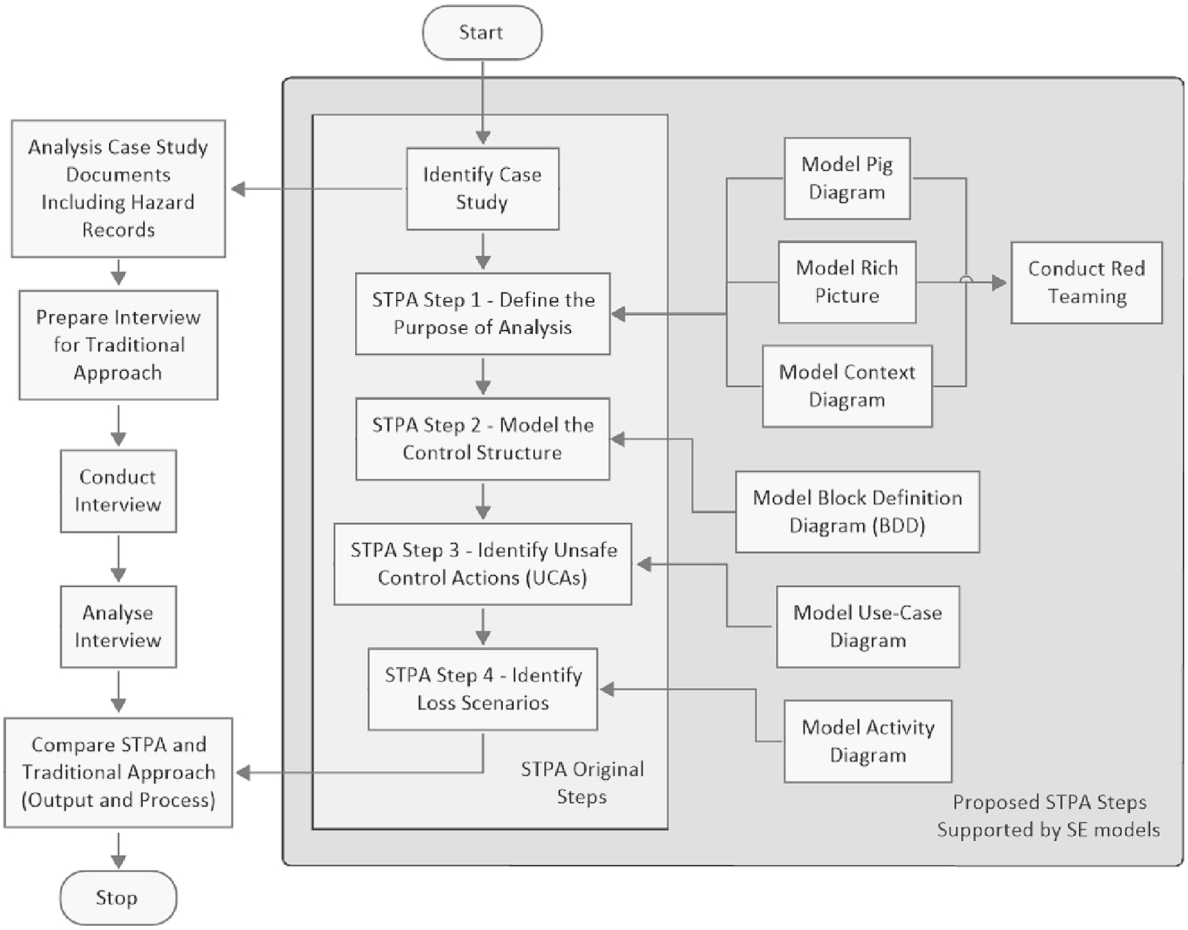

Fig. 1. Research methodology.

contextual situation in relation to the SOI (Government Office for & Science, 2022; SEBoK Editorial Board, 2022). A pig diagram is a model to explore how the SOI is seen by its stakeholders. A rich picture depicts any stakeholders, processes, and issues of significance to the problem situation within the SOI and their interactions. These two models described the stakeholders in relation to the LXSS upgrade project and supported the identification of their values and losses (i.e., their 'stake' in the SOI and any loss that's unacceptable to the stakeholder). In addition, a context diagram was developed to model the relationship between the SOI, its boundary, and its wider environment. This diagram supports the identification of system hazards based on interface points.

The pig diagram, rich picture, and context diagram models were validated through a red-teaming (RT) approach which is suitable for SE related research outcome validation (Ferris et al., 2022). The research applied the RT method by inviting RT members comprising two SMEs with considerable expertise and experience in the case study area, to provide feedback and validate the models developed for the first step of STPA.

2.4. Model the control structure

The control structures within the SOI were identified and modelled using a Block Definition Diagram (BDD) to illustrate a high-level and hierarchy structure view of the SOI. BDD was utilised to identify the input (i.e., control actions or command) imposed by the controller and the output (i.e., feedback) received from the controlled process. Analysis of the hierarchy structure, and interactions through the BDD supported further hazard identification in Step 3 (section 2.5).

2.5. Identify Unsafe Control Actions (UCAs)

UCAs are inappropriate interactions between components that can lead to hazards (Hirao, 2020). Leveson & Thomas (2018) suggested four ways a control action/command can be unsafe which can lead to hazardous scenarios:

1. 'not providing causes hazards' – when the control commands required for safety are not given;
2. 'providing causes hazards' – when unsafe commands are given;
3. 'too early' or 'too late' – potentially safe commands are given but provided too early or too late;
4. 'stopped too soon' or 'applied too long' – the control command stopped too soon or is applied too long.

Identification of the UCAs was supported by the development of use-case diagrams to explore control structures, high-level function, and their interactions, for additional source of hazard identification.

2.6. Identify loss scenarios (causal factors)

This is the final step of STPA with a more rigorous approach to understand or explain why and how the UCAs identified in previous step may occur by analysing the elements that form the control structure, i.e., control actions, feedback, controller, controlled process. At this stage, an activity diagram was developed to further analyse and understand the behaviours within the control structure, to identify the possible causal factors, thus identifying new hazards that need to be prevented.

2.7. Traditional methods: SME interview

To allow a comparison of the proposed STPA-based methodology supported by SE models, with the traditional methods, this study sought to collect qualitative data to understand existing approach for hazard identification and analysis in UK railway projects. Interviews were conducted with six SMEs consisting of a mixture of technical directors (2), principal managers (2) and associate managers (2). Two out of the six SMEs interviewed were directly involved with the case study. The selected SMEs have extensive knowledge and experience of safety assurance including the application of traditional hazard analysis approaches in the rail industry. The raw data collated from the interview process was analysed using thematic analysis to discover thoughts, experiences, or behaviours among participants regarding the traditional approach.

2.8. Comparison of STPA-based methodology and traditional approach

This study compares the STPA-based methodology incorporating SE models and the traditional approach in two ways. First, it evaluates both methods in terms of their output, i.e., the list of hazards produced by the STPA-based methodology with the list of hazards generated using the traditional approach, considering completeness and comprehensiveness. Second, it compares the processes of the two approaches, in terms of their effectiveness; time and resources required for each method; as well as their ability to perform system-level analysis.

3. Results

3.1. STPA-based methodology supported by Systems Engineering (SE) models

This section is organised to present the research results in accordance with the structure of the STPA-based technique discussed in Section 2.2 and Fig. 1, including the purpose of the analysis; control structure; Unsafe Control Actions (UCAs) and loss scenarios.

3.2. Purpose of the analysis

The pig diagram (Fig. 2) and the rich picture (Fig. 3) allow the identification of stakeholders, stakeholder values, and stakeholder losses. Both the pig diagram and the rich picture have evolved from their initial versions based on feedback from the RT members. The final version of the models was agreed by the RT members with no further comments.

Some examples of stakeholder and their values are provided in Table 1.

The list of stakeholders and their values was analysed and summarised to define a list of stakeholder losses, i.e., losses that are unacceptable and need to be avoided to achieve the stakeholder's values/goals. A summary of losses is given in Table 2.

A context diagram (Fig. 4) was created to identify the components of the system, the environment, and describe the boundary to support the generation of hazards. It captures the interface relationships, constraints, and influences as related to the case study. The diagram has also been evolved from the original version based on feedback of the RT members.

The context diagram demonstrates that the SOI has relationships with the Wider SOI (WSOI) that includes elements that are required for the operation of the SOI. It also shows that the 'environment' in which the SOI will operate and survive can directly influence the SOI and the 'wider environment' that has influence on the 'environment'. The context diagram enables the generation of the list of hazards with each hazard linked or traced back to a corresponding loss (Table 2). Some examples of identified hazards, their associated interfaces and components, and their associated losses are provided in Table 3.

3.3. Control structure

The control structure model was created using the SysML Block Definition Diagram (BDD) (Fig. 5) syntaxes including 'composition', 'aggregation' and 'association', to identify the elements of the SOI and their interactions based on the elements identified in the context diagram. The composition and aggregation syntaxes help to identify the

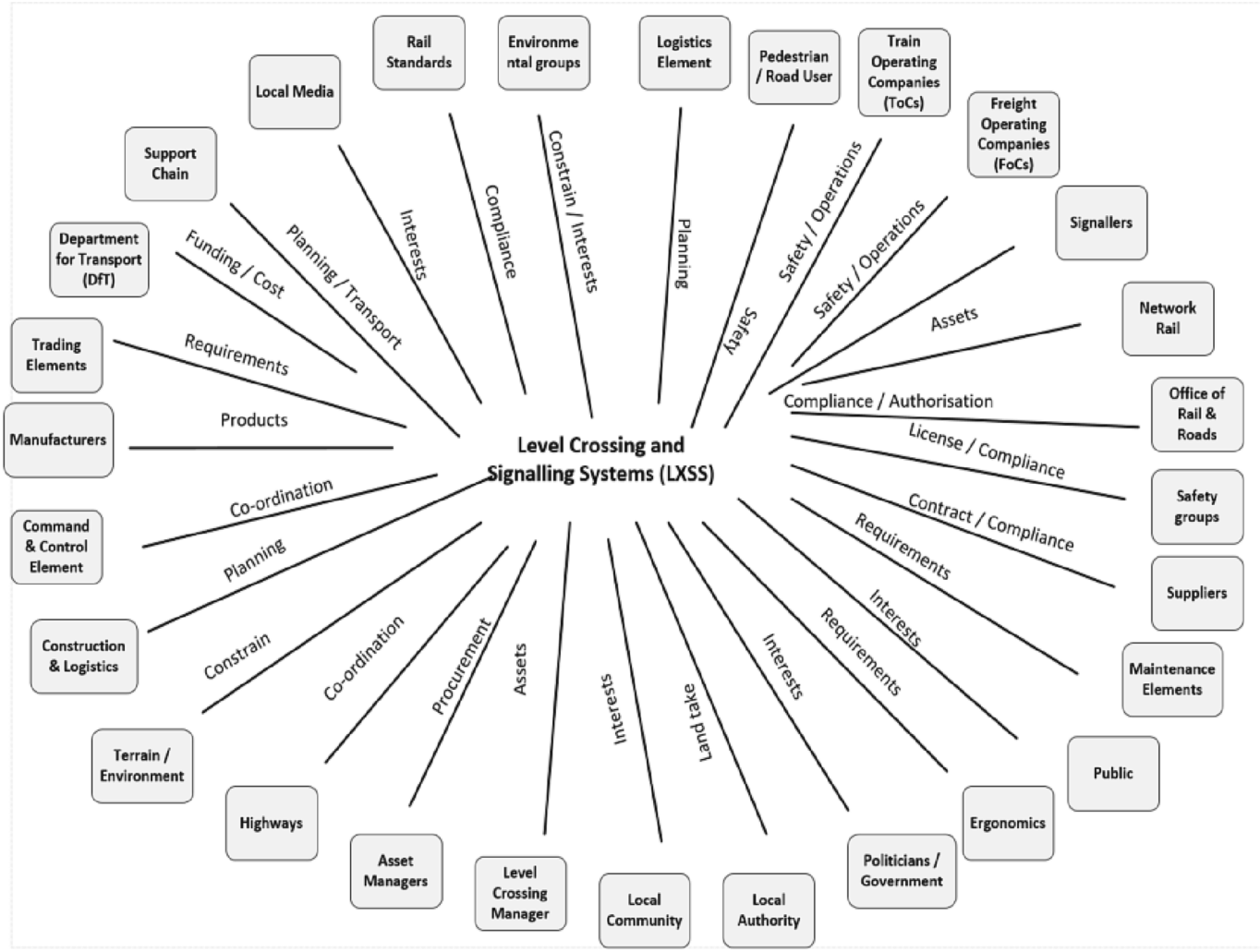

Fig. 2. Pig diagram.

hierarchy that exists within the SOI. The association syntax illustrates the cross-element interaction and communication between the elements within the SOI, which can be used to illustrate the controller's inputs (i.e., control actions/commands) and the outputs (i.e., feedback) received from the controlled process. For example, in the interaction of 'level crossing (LX) control' (controller) and the 'obstacle detection' (controlled process), the 'control action' is to check if the crossing is clear of obstacles; and the 'feedback' from the obstacle detection module is to provide information with a status or confirmation. It is noteworthy that although BDDs are usually utilised for representing physical architectures, in this study, they were developed to represent the control structures, to identify the hierarchy of control from a higher level, or controllers, to a lower level, or controlled process, with the higher-level having control over those lower to it. For example, the 'conflict control' can act as a controller by sending control actions to the 'level crossing (LX) control' and monitor for feedback (Fig. 5).

Multiple control loops can be identified within the SOI in Fig. 5; however, this study focused only on two of the control loops. These two control loops, namely LX Control/Barriers and LX Control/Obstacle Detection control loops are illustrated in Fig. 6. Analysis of these loops enabled further identification of hazards.

3.4. Unsafe control actions (UCAs)

To further understand the selected control loops (the LX Control/Barriers and the LX Control/Obstacle Detection), the behavioural views of the operational context of these loops were presented in the form of use-case diagrams including one as shown in Fig. 7.

The high-level functions shown in the use-case diagrams were analysed to generate a list of UCAs that describe the inappropriate interactions between components which may lead to accidents. Based on these use-case diagrams, the list of UCAs was populated against the four guidance scenarios or contexts described in Section 3.2 An example of UCA and its associated safety measures is given in Table 4.

3.5. Loss scenarios

The activity diagrams such as one shown in Fig. 8 were created to further investigate the UCAs to discover the causal factors of each UCA. To determine what could cause a UCA to occur, factors to consider include input into the controller from a higher-level controller. In such scenario, the controller under investigation will become the controlled process in another control loop. Another factor to consider is the information from other control loops or external systems supplied into the controlled process.

Using UCA-1 (see Table 4) as an example, the following causal factors have been identified:

- Controller: LX Control receives incorrect information/input from another controller such as the train detection. Train detection failure showing that the train is occupied when there is no train (mimicking

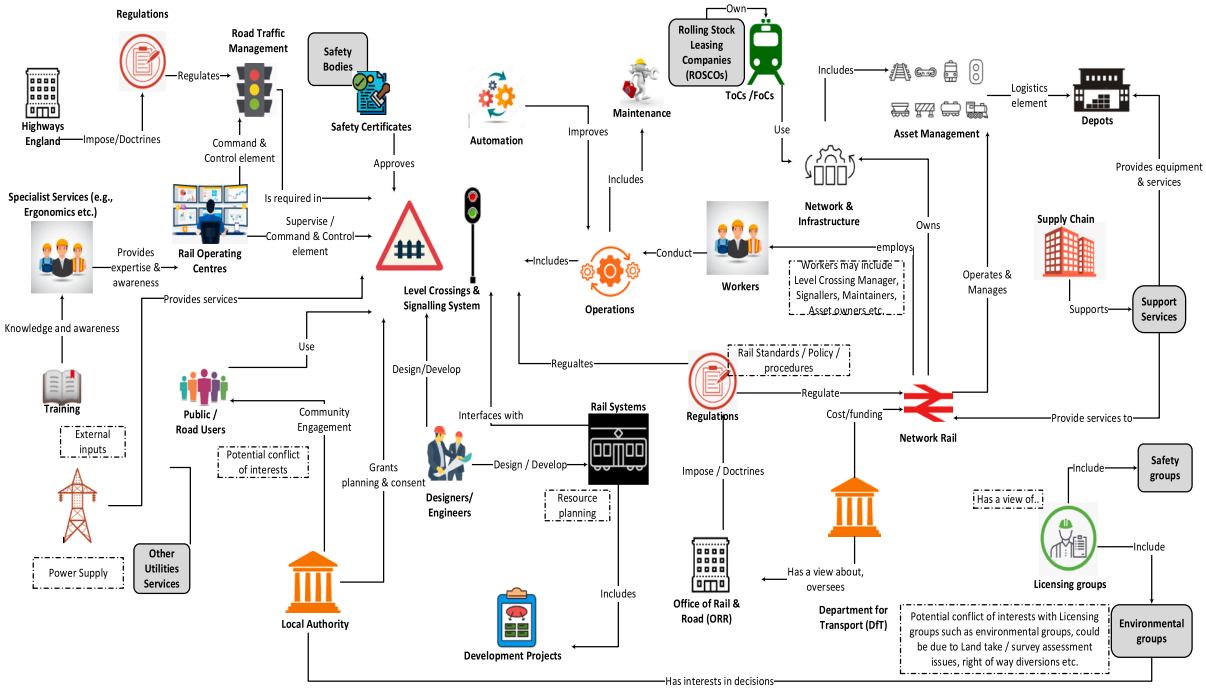

Fig. 3. Rich picture.

Table 1
Example of stakeholders and their values.

Stakeholder	Values / stakes in the SOI
Pedestrians / Road User	• Cross the LX safely Reduced road congestion Minimal waiting time at LX stops
Train Operating Companies (ToCs)	• Reduced disruption Run more services / increased capacity
Local Authority	• Reduced road congestion Increased road user and pedestrian safety Avoid disruption during construction and general aesthetics
Manufacturers	• Develop high quality assets in the least expensive way possible Manging growth and innovation
Public / Local Community	• Reduced road congestion Increased road user and pedestrian safety Avoid disruption during construction and general aesthetics

Table 2
Summary of losses.

Loss ID	Description
L1	Train collision with object (road users – pedestrians or vehicles) / death / loss of life / serious injury
L2	Negative impact to reputation
L3	Damage to railway asset(s)
L4	Damage to nonrailway asset(s) e.g., road traffic
L5	Negative environmental impact
L6	Inability to complete mission / operational delay / performance issues
L7	Loss of user experience/satisfaction / inability to perform duties/ responsibilities

the striking of the train). The system will think there is a train there when there is no valid train.

- Controlled process: Failure of the drive circuits (motor control of the barrier) causing the barrier to not send feedback / information. to the LX control.
- Control Actions: The Command to 'Authorise & Deploy Barriers to fall' is not applied to the barrier control, but barrier control responds as if the command had been received.
- Feedback: The (physical) microswitches in barriers might have failed; cable from the barrier to LX could be broken or high resistance – poor connection, poor signal transfer of the signal is poor as a result.

Based on the causal factors, the following safety constraints have therefore been generated from UCA-1:

- C-1a: LX Control must not provide 'deploy barriers to fall' action when a train is not approaching.
- C-1b: LX Control must not provide 'deploy barriers to fall' action when a train has gone through the LX.

3.6. Interview results: Traditional approach

Table 5 provides a description of interviewees in terms of their roles, experience, area of specialty, and sectors they worked in.

Based on a thematic analysis, some key themes emerged from the interview, namely, processes, benefits, and challenges.

3.7. Processes

In general, all interviewees perceived that the safety analysis process is systematic and well formulated over the years within the UK rail industry. Albeit non-prescriptive, the process seems to be conducted in a similar way. Approaches vary depending on the facilitator's experience and personal preference, but the process is consistent as 100% of the interviewees' description of the process aligned.

There are no written statements on how to conduct HAZID workshops, but most of the interviewees describe the approach in a fairly similar way. In a typical HAZID workshop, the design team presents the design, and the workshop participants discuss the design and raise hazards. The workshop is normally preceded by an initial desktop analysis of a list of generic hazards, design documents, operational

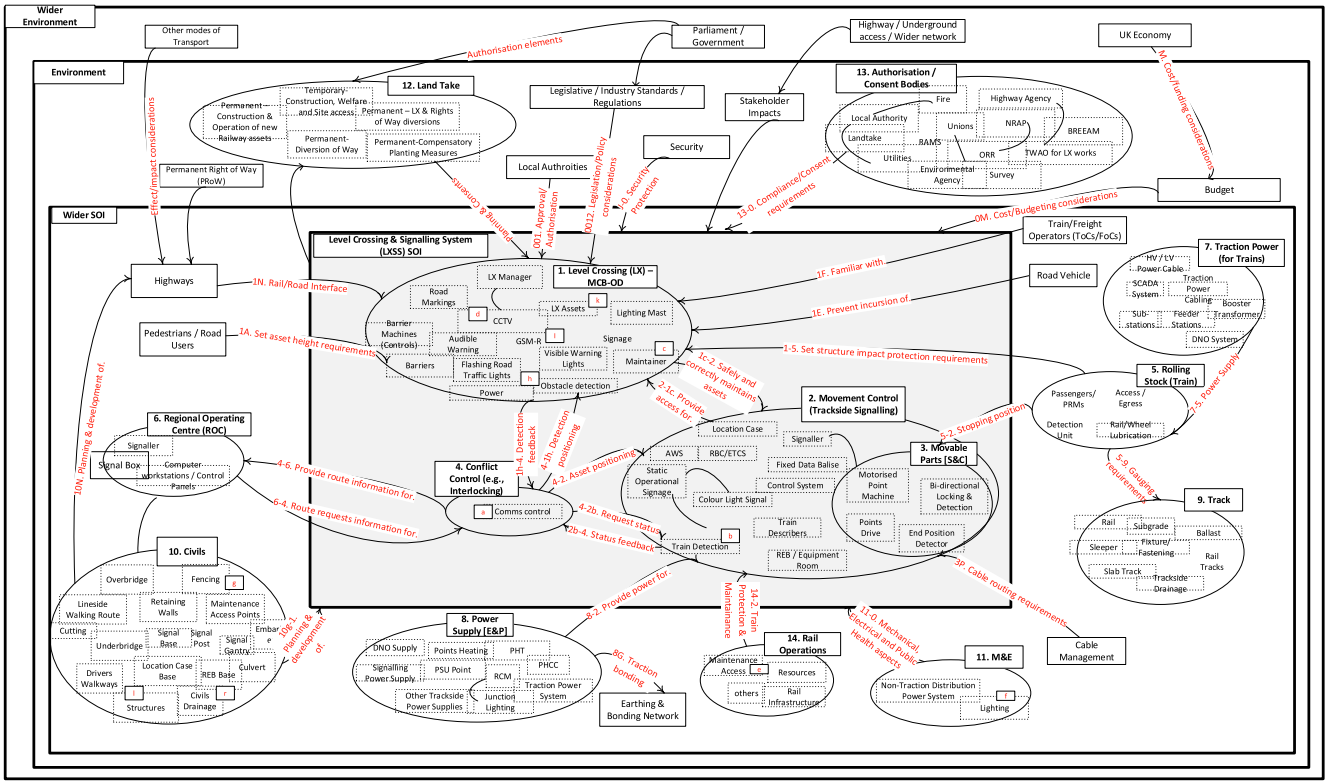

Fig. 4. Context diagram.

Table 3
Example of Hazards and the Associated Interfaces, System Elements and Losses.

Hazard ID	Interface Reference	Element A	Element B	Interface/ Function	Hazards	Associated Loses
H-1	4–6.	Conflict Control	ROC	Information displayed on the screen to show the routes are set, the position of the trains, and the aspects of the signals.	The information displayed on the screen is incorrect / does not correctly display which routes are set, the position of trains, and the aspects of signals.Incorrect train stopping position(s)	L6, L7
H-2	6–4.	ROC	Conflict Control	Route requests information to show what routes are set, the position of trains and the aspects of signals.	The requested information did not get to the Conflict control	L6, L7
H-3	6–1.	ROC (CCTV)	LX Control	Provide adequate coverage of the LX location.	The CCTV control room (in the ROC) does not have sufficient capacity to complete coverage of the new LX.	L6, L7
H-4	4a-2	Comms control	Trackside Signalling	Set asset positioning requirements	Ineffective comms asset positioning	L6
H-5	1A	Level Crossing (LX)	Pedestrian / Road Users	Set LX Barrier and LX structure/column positioning and set asset height requirements	Insufficient passenger/route user headroom from LX barrier and suspended assets	L1, L2, L3, L4

scenarios, a review of the system under evaluation, or hazard record from similar projects. The outcome of the workshop is a set or list of hazards which is shared with the participants for review and comments.

The interviewees also indicated that more rigorous and intensive desk-based techniques, such as HAZOP, FTA, FMECA, etc. can be used to tease out new hazards.

3.8. Benefits

Most of the interviewees did not explain in detail the benefits of the traditional approach as they did with the challenges (3.9), but there is a shared view that the traditional methods have brought design disciplines under the same set of rules, allowing for a systemic approach. Normally, there is familiarity of the approach with everyone involved in the design team. If done correctly, the approach provides a clear process on how to identify hazards, including specific steps to address the hazards. such as considering the categorisation of hazards (e.g., significant, or not significant) within the HAZID workshops. In addition, the traditional approach allows a project to prioritise crucial hazards early.

3.9. Challenges

About 60% of the interviewees believe that the safety analysis process needs to be modified. Despite the belief of some interviewees that the existing process was adequate, a combination of methods or an integration of new methods would be very useful, particularly if efficiency can be gained or the hazard identification process simplified or even improved. Some interviewees noted the importance of integrating system models to support hazard analysis. A context diagram, for example, in some cases has been used to identify hazards, as hazards most often appear at interface points.

The interviewees believe that different people understand or see hazards differently. Therefore, people or organisations do hazard analysis differently or may have different points of view. For example, an

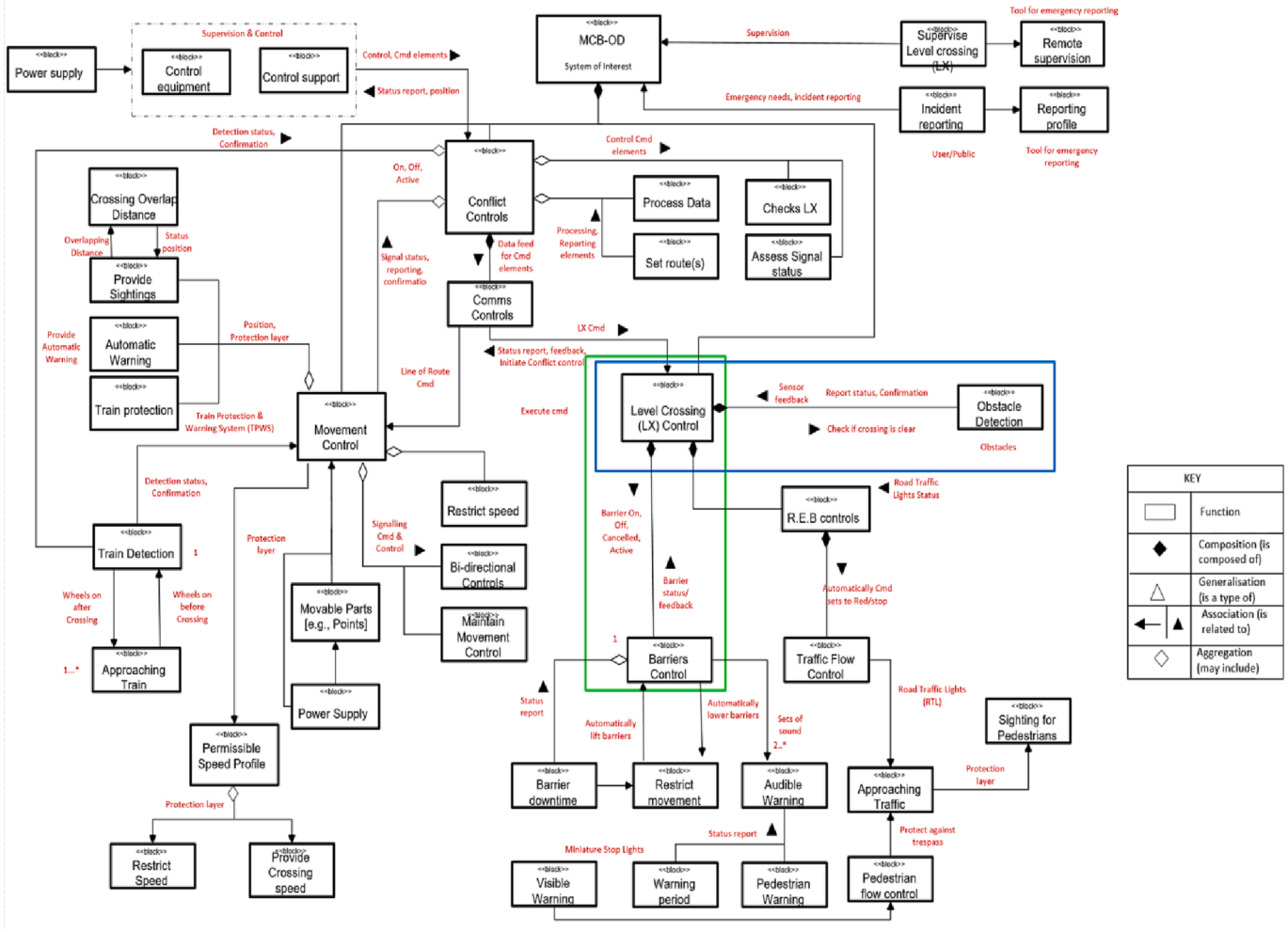

Fig. 5. Block definition diagram.

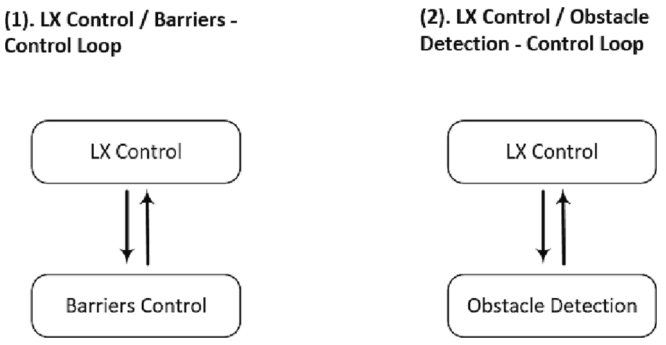

Fig. 6. Focused loops in the study.

organisation may view that all hazards are equal so that it does not perform hazard categorisation by filtering them and distributing proportionate effort, while other organisation may perform hazard ranking and classification.

It should also be noted that the traditional approach to hazard analysis risks becoming a tick-box exercise rather than a consideration of good safety management. Safety analysis is not usually considered at the beginning of the design stage. Sometimes a project may undertake hazard analysis at the end of a design stage as an additional deliverable after a design option has been selected. The hazard analysis process is not seen as fundamental to the progression of the project.

Other identified key challenges include:

- Lack of knowledge of the system under consideration amongst the workshop participants that can lead into inaccurate information.
- About 80% of the participants identified that the skill of the person performing the hazard analysis is vital.
- Challenge in ensuring the participation of the appropriate individuals in the workshop such as asset managers, maintenance owners, and other relevant stakeholders.
- The hazard analysis process can be 'patchwork', as in, it is based on the scope of the change only.
- It is possible for some project managers to complete the hazard analysis on their own because of familiarity or to save costs, the generated hazards may be inaccurate as a result.
- A single voice or a group of voices can dominate the HAZID workshops, resulting in limited participation across the entire project team.
- The repetitive nature of the workshop process may cause participants to 'switch off'. It can be challenging to vary the workshop so that the right outputs are delivered without becoming monotonous.
- Engineers often assume that they do not need to record what they have already designed as they do not see the need for doing so.

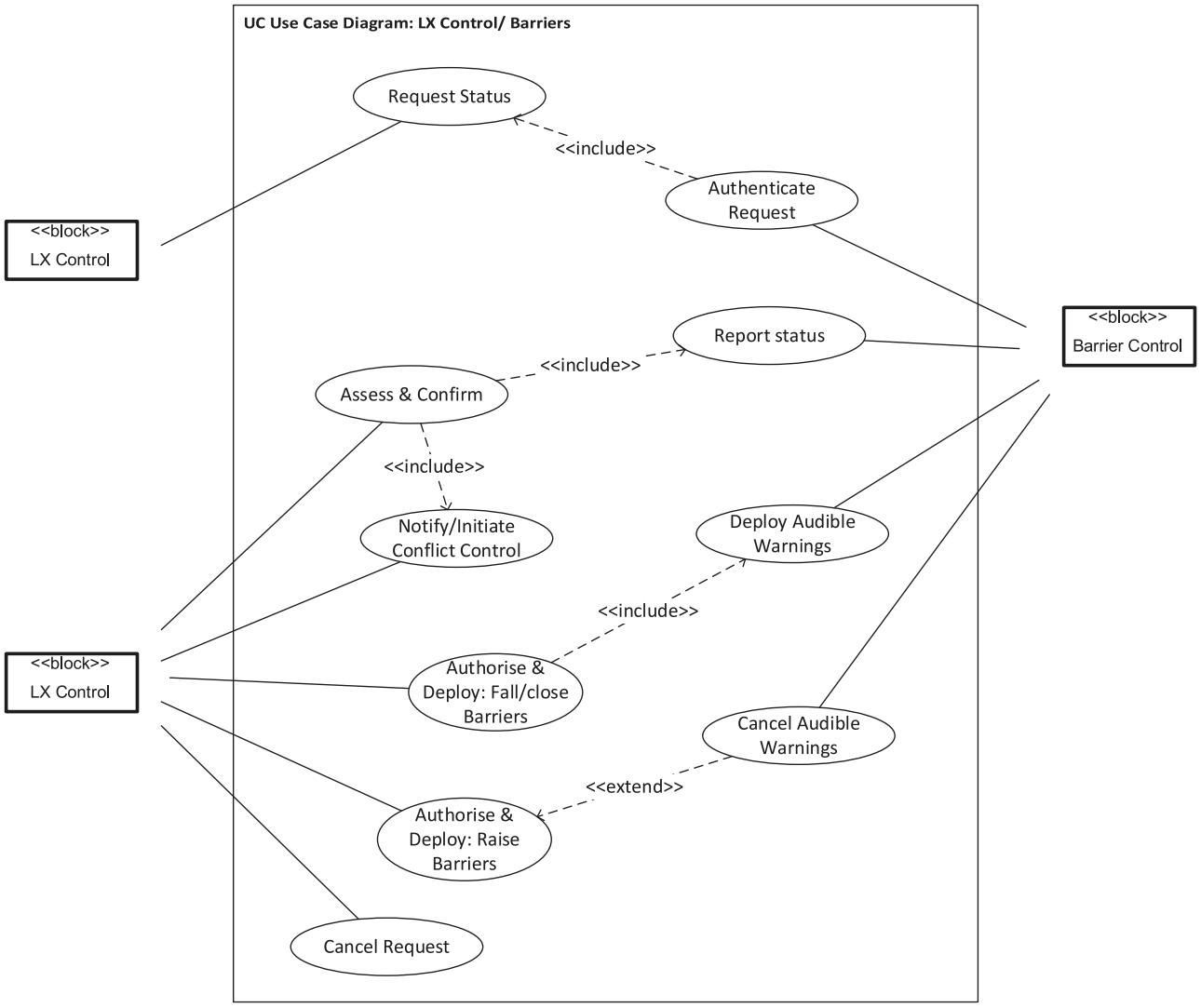

Fig. 7. Use-case diagram.

4. Discussion

4.1. Comparison of outputs

A comparison of the initial list of hazards generated by the STPA-based method supported by SE models at Step 1, to those generated by the traditional approach, shows similarities in term of its completeness and comprehensiveness. Table 6 is an excerpt of hazards and their similarities.

The completeness comparison shows that STPA Step 1 alone can be used to produce a hazard list that may lead to accident that is similar to that produced by a typical traditional hazard analysis technique, with the hazard description. Nevertheless, as observed in Table 6, STPA significantly enhances the information richness in hazard descriptions, as STPA prompts the analyst to consider the context, complex interactions and dependencies as well as scenarios within which a system may demonstrate unsafe behaviour. Consequently, STPA expands the depth of hazard understanding and enables a more comprehensive approach to safety.

Steps 2 to 4 of STPA enables identification of unsolicited behaviours that may occur within the SOI; behaviours that were not accounted for by the traditional approach. For example, within the LX control/ Obstacle detection loop (Fig. 6), the 'requesting detection information' command when a train is not approaching or after the train has passed the LX, is identified as an UCA. This UCA may cause operational and performance issues. For example, it can result in a project team sending out a maintenance engineer without any apparent reason, which may subsequently result in the engineer or the system itself taking the wrong action based on the incorrect assumption that there is an obstacle on the LX. Although these behaviours do not necessarily guarantee that a hazard will occur, however, by understanding the behaviours to prevent, the project or design team can take these into consideration as part of their system development, proactively mitigating risks and enhancing system performance. Similar logic applies if the project team is using Commercial-Off-the-Shelf (COTS) products as part of their system design. The manufacturer of the COTS product will be well-informed, or the requirements will be better understood based on the STPA data.

Furthermore, the STPA supported by SE methodology used in this study enables a detailed evaluation of the system hazards including identifying non-obvious factors, which are often missed by traditional approaches. Traditional approaches typically focus on identification of primary and secondary causes, and often overlook trivial or nonobvious behaviours such as those caused by software and/or human errors. This is illustrated below by analysing an example of a hazard that may lead to train collision generated by both the traditional approach and the STPA-based methodology respectively.

A hazard and its causes generated by traditional approach:

Table 4
An example of UCA.

Source Controller	LX Control
UCA - Number	UCA-1
UCA - Type	*Provides* - When 'control commands' required for safety are not given
UCA - Action	Authorise & Deploy Barriers to Fall Command (i.e., close road traffic)
Context	When no train is approaching or after the train has gone past the LX
Associated safety hazard	• H05: Insufficient passenger, road users' headroom from LX barrier and suspended assets. • H13: Inadequate vehicle incursion prevention; Train collision with road vehicle on the LX. • H14: Does not prevent unauthorised access to track. • H18: Incorrect train detection positioning resulting in inability to signal trains or to control the LX. • H22: Does not interlock signals with the lifting barriers. The Comms between the conflict control to the lifting barriers is ineffective. • H34: Out of sequence detection leading to performance/ failure issues. • H35: Drop the barriers/or lift barriers, maybe out of sequence. • H36: Out of sequence train detection; Train detection is either occupy or clear. • H76: Incorrect train detection positioning resulting in inability to signal trains through the LX route; Operational delay.

- **Hazard:** Inadequate separation between trains;
- **Primary Cause:** Less restrictive aspect displayed instead of the'red' aspect.
- **Secondary Cause:** Interlocking failure: System error

A hazard and its causes generated by STPA-based methodology supported by SE models:

- **Hazard:** Inadequate vehicle incursion prevention; train collision with road vehicle in the LX
- **UCA:** The LX control 'authorise & deploy barriers to raise' command (i.e., open road traffic), when there is an approaching train.
- **Causal factors:** Failure of track circuits (train detection) to identify an approaching train. Unsafe input received by the LX control from train detection (another controller). Barrier control sensors (detectors) are malfunctioning, and barrier detector reporting as down rather than raised. Route setting failure by the signaller or Automatic Route Setting (ARS). False current running through the barrier detector measured by the road traffic lights due to halogen red lights failure. etc.

As shown by the example above, it can be concluded that in terms of comprehensiveness, the proposed STPA- supported by SE models methodology, capture more rigorous and detailed evaluation of the system hazard including non-obvious factors e.g., identifying what behaviours could directly or indirectly lead to the hazard. This exceeds the capability of traditional methods, which typically only address step 1 of STPA.

It may be argued using the example above that these are fail-safe products or that there are back-up elements to these systems and therefore would not lead to a hazard or something tragic. However, as shown by this research, STPA is a worst-case analysis method. It is ideally applied early in the design life cycle before fail-safe or back-up options are known and incorporated into the design. Once STPA has identified those behaviours needing to be prevented, requirements or design decisions are better informed to prevent those unsolicited behaviours. This innovative approach enables identification of behaviours that should be prevented and their causal factors. These are key to additional safety measures as well as requirements which are not observed in the traditional output.

4.2. Comparison of process

In terms of the effectiveness, as identified through the interview results (section 3.2), a typical HAZID workshop usually involves bringing together SMEs to brainstorm ideas of hazards. These workshops are often dictated or led by a generic list of hazards as a starting point; in some cases, there may be no new hazard to add beyond what is already captured in existing datasets. In addition, the 'brainstorming sessions' offered by these workshops often leads to experts (i.e., participants) with their own culminative biases in terms of what is plausible and probabilistic, while missing other important information.

On the other hand, the application of the STPA-based methodology enhanced by SE models, as demonstrated through this study, enables a systematic approach to generating and addressing a hazard list. This approach systematic approach provides a structured process with enhanced guidance and the thought process to facilitate the identification of control logic, which may be lacking in other approaches. It also helps to prevent omissions or errors due to a lack of competence or experience, thus, it does not necessarily require an experienced safety engineer to apply it and to achieve reliable and comprehensive results.

The SE models used during this research demonstrate their value in leveraging insights to a more effective and visual approach for implementing STPA. The combination of the pig diagram, rich picture, and context diagram provided a representation of the SOI, to effectively analyse the system and identify hazards. Further models, including BDD, use-case diagrams, and activity diagrams, illustrate the systems structure and control to capture more rigorous and detailed hazards beyond those of traditional approach from the context of the whole. These models facilitate the evaluation of interactions between system components. They allow the assessment of the interactions through different scenarios or contexts to generate unsafe behaviours and their causal factors. In other words, these SE models help the analyst to analyse the SOI in a more focused, and efficient way, which would otherwise have been challenging if using traditional approaches. In addition, these models represent the underlying structures, components and relationships of the system under considerations and communicated the system to a wider audience.

In terms of resource, admittedly, STPA can be laborious and time-consuming, especially when familiarity with the method has not been achieved in advance. Consequently, due to limited resources, this research only investigate two 'control loops' out of potentially multiple loops. However, in fact, most hazard analysis methods are laborious and time consuming. The repetitive nature of traditional approaches and the lengthy HAZID workshops, which in some cases may take days for hazard identification alone, give the impression of a monotonous and unintelligent mission, that sometimes could result in incorrect or incomplete output due to complacency, overconfidence, or disengagement from the process. STPA forces analysts to investigate each control loop within the control structure in a structured, deliberate and staged manner, which can help avoid loss of attention and, in turn, lead to better outputs. Furthermore, integrating the SE model to the STPA may require more effort and time, but on the other hand the models help to make the analysis more focused, in scope and make the process more effective and efficient. The experience from this study aligned with the previous work by Fowler (2015) that suggests that STPA is the most comprehensive hazard analysis method.

In addition, the traditional risk analysis approach only considers change from existing infrastructure, i.e., elements within the project scope, whilst ignoring the whole picture and potential impact on surrounding infrastructure or network. Consequently, hazards are not identified for elements that are outside project' scope; even if those hazards constitute non-compliance of the railway. Nevertheless, STPA enables consideration of influences not just within the project boundary or scope but also outside that boundary. In terms of system-level

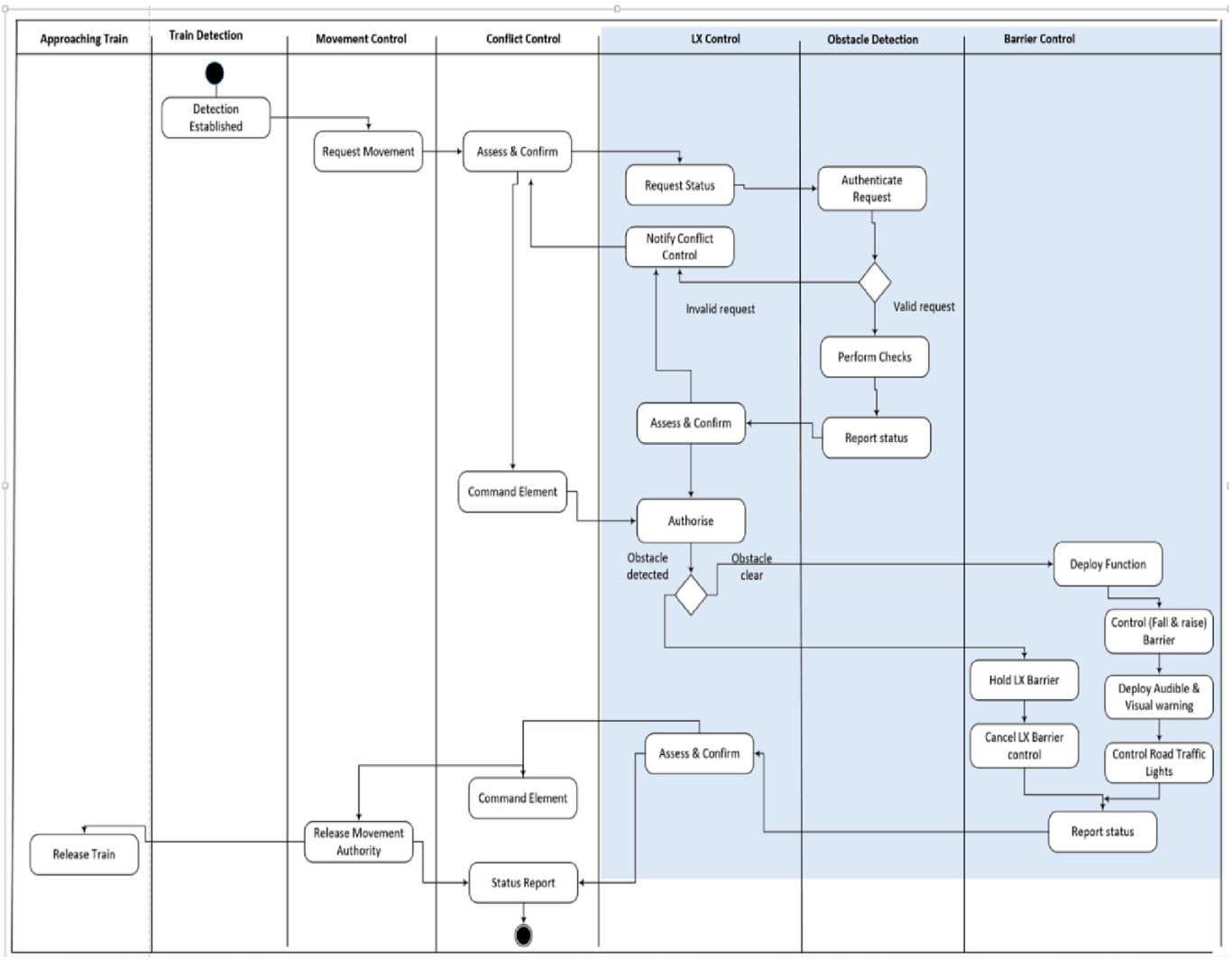

Fig. 8. Activity diagram.

Table 5
Interview participants.

Participants ID	Position/ Roles	Years of experience	Area of Specialty	Sectors worked in
Participant 1	Associate Safety Assurance	28	Safety Assurance	Rail, Telecommunication
Participant 2	Associate Safety Assurance	14	Safety Assurance	Rail & Nuclear
Participant 3	Associate Director Safety Assurance	22	Safety Assurance	Rail & Marine
Participant 4	Associate Director Safety Assurance	25	Signalling and Safety	Rail, Industrial automation.
Participant 5	Principal Safety Assurance	12	Safety Assurance	Rail, Defence
Participant 6	Principal Safety Assurance	9	Safety Assurance	Rail, Oil & Gas

Table 6
Comparison of hazards derived from STPA-based methods and traditional methods.

Traditional Methods Hazard Description	STPA Hazard Description
Train striking/ struck by object within kinematic envelope	Inadequate vehicle incursion prevention. Train collision with road vehicle on the LX.
Electrical Hazards	Traction return, disconnected, or high-resistance traction bonding can lead to safety issues.
Slips, trips and falls	Inadequate LX footprint/area illuminance levels for both normal and emergency situations. (This includes uniformity). Potential for slips, trips, and falls. Potential people-train incident at the LX.
Inadequate separation between trains	Inadequate controls in situations of reduced (gauge/passing) clearances. Potential for (train) collision. Potential for derailment.
Exposure to hazardous materials	Pedestrians, road users and / or maintenance workers are exposed to hazardous materials/ environments.
Incorrect Manual Handling	New assets introduced that are unfamiliar to maintenance/ and operational staff. Inappropriate maintenance. Manual handling issues.

analysis, the context diagram (Fig. 4) is instrumental in identifying the impacts of the SOI, inside or outside the SOI boundary, as well as the interactions of those elements which proved to be a source of hazards.

4.3. Systems Engineering (SE) models: Experience and lessons learnt

The decision to incorporate SE models such as rich pictures, pig diagram, context diagram, among others, prove to be beneficial. The rich pictures and the pig diagram effectively identify the relevant stakeholders, their influence and their loses on the SOI. The context diagram thoroughly explores the system, by identifying interfaces, system boundaries and interactions or relationships between system components, and examining what falls within and outside the system boundary. A combination of the rich pictures, the pig diagram and the context diagram provide a solid foundation for hazard identification. Furthermore, the BDDs help in identifying functions within the SOI by determining the relationships between these functions as well as the hierarchy among them. The Use Case diagrams are effective in identifying UCAs, while the activity diagrams provide insights into the causal factors of UCAs. These two SE models play a key role in identifying safety constraints.

One of the major constraints of traditional approach highlighted by approximately 80% of the interviewed participants (Section 3.2) is the human element, especially the skills of the individual undertaking the risk analysis. The research conducted in this study demonstrates that the structured approach facilitated by SE models offers improved efficiency in uncovering hazards, particularly when developed collaboratively. Therefore, there are opportunities for the traditional approach to integrate the use of SE models as an integral part of its current process.

Another challenge that was identified relates to the participation of the right individuals in the HAZID workshop. To address this challenge, the pig diagram (Fig. 2), which was used to understand stakeholders within a problem context, could be the best solution. The pig diagram enables to identify the relevant participants and their influence on the SOI. The research suggests that integrating this model into the workshop will help establish the appropriate individuals to ensure a more comprehensive and efficient workshop.

In addition, the existing traditional process can be ‘patchwork’ in terms of focusing only on the scope of the change such as change from an existing infrastructure. This approach often overlooks the broader impact on surrounding infrastructures or the network as a whole. Consequently, hazards are not identified for elements that are outside project’ scope, even if they constitute non-compliance with the railway regulations. Therefore, opportunities exist for rail projects to consider the influences not only within its boundary or scope but also those outside the boundary. As demonstrated though this research, there are elements that influence the SOI, inside and outside the SOI boundary where the interactions of those elements can potentially introduce hazards. The context diagram (Fig. 4), an SE model, play a important role in identifying those interactions and influences.

4.4. Contrast of philosophical position

In both methods, the system is studied to identify potential safety hazards. Identification of hazards enables action to address hazards. However, there is an important difference between the methods. The traditional method focuses on the identification of hazards that may arise from the failure of system components and/or their design errors. Thus, it is a failure prevention focused approach to safety. In contrast, the STPA method emphasises on imposing constraints to limit system behaviours. In addition to failure of system components, it recognises that failure could arise from systemic interaction of the components of the connected system. The cause of this outcome is the emergent effects that arise when a system is constructed from a set of components which must interact to produce the intended effect of the system. Thus, STPA may discover UCAs between system components without any system components having failed (Hirao, 2020). These UCAs and their causal factors are key to safety measures, which set the STPA apart from the traditional approaches.

Overall, the STPA process leads to generating a set of richer outputs that are not subject to any constraints, such as cost or time. STPA draws an ideal picture – from a safety viewpoint – of the system under consideration (Chatzimichailidou & Dokas, 2016), which designers can then manage and adapt in such a way so that it is financially sustainable, on track to be delivered on time and according to client and end-user needs, priorities, and requirements.

5. Conclusion

This study started with a belief that traditional safety analysis methods used in UK rail development projects can no longer cope with the increasing complexity of modern, complex, socio-technical systems (Dunsford & Chatzimichailidou, 2020). A systems-based approach is needed to confidently identify all reasonably foreseeable hazards, their corresponding safety measures, and requirements to prevent potential accidents.

It must be emphasised that STPA is not intended to replace traditional tools and techniques, but rather to shift our attention from hardware and reliability focussed techniques to more intangible factors such organisational, social factors, human decisions and software design errors. This is especially relevant for complex systems with latent or unknown relationships between its components that could have an impact on the safety of the system, as shown by the previous accidents (Dunsford & Chatzimichailidou, 2020).

The first contribution of this study is to introduce and implement the application of a novel STPA methodology incorporating SE models to a rail case study - the upgrade of a Level Crossing and Signalling System (LXSS) project. The proposed methodology was supported and enhanced by SE models including a pig diagram, a rich picture, a context diagram, block definition diagram, use-case diagrams, and an activity diagram. The experience and lesson learnt in this study has shown that the SE models used in this study prove to be valuable not only for illustrating the SOI visually, but also providing a high-level understanding of the system, and a more detailed understanding of component interactions. The proposed methodology improves the focus, scope, effectiveness, and efficiency of the analysis. Incorporating SE models into the STPA methodology ensures that the hazard analysis process is more efficient and effective. It is important to note that there is no one-size-fits-all approach when it comes to SE models. A combination of SE models could be employed to understand the context or explore a problem situation comprehensively.

The second contribution of this study is to compare the novel STPA-based methodology supported by SE models against the traditional approach that prevails in the UK rail sector in a case study. This study demonstrates that the proposed STPA methodology with SE models’ integration is suitable for hazard identification and analysis in complex rail systems. It also demonstrates that the approach goes beyond the capability of traditional methods. Analysis of safety–critical systems that utilise advanced technology and include human interactions will benefit from the consideration of components’ interaction. The STPA-based methodology enhanced by SE models provides insights into the interaction among system components and captures hazards within the context of the whole. They are able to assess the interactions of these components through various scenarios, contexts, or environment, generating a list of potentially unsafe behaviours along with their causal factors, which must be addressed.

The findings of this research must also be seen in light of some potential problems and limitations. The application of a novel STPA methodology which incorporates SE models into the STPA process requires a good understanding of SE methods. Unlike STPA, the proposed enriched methodology is not self-explanatory and may require guidance from an SE specialist to develop SE models. Therefore, additional time

and resources may be required for the development of SE models making the process more time consuming and laborious compared to STPA alone.

This study focuses on a case study with only two control loops due to time and resources constraints. When analysing larger systems, it is expected that the proposed methodology will generate a large number of visuals and results, which could present challenges in terms of comprehension, utilisation and practical implementation. Tools, such as cost-benefit analysis, can help practitioners prioritise solutions and filter out impractical information. Principles such as ALARP (Health and Safety Executive, 2022) can support decision making.

Nonetheless, future study can expand into the investigation of the entire control structure to strengthen the argument of the effectiveness of the proposed methodology (i.e., STPA and SE) against the traditional approach. The two loops considered in this study were primarily sensitive in identifying software errors, future studies may expand into more specific cases for comparison and experience, such as the observation of human errors, as noted in studies conducted by Lower et al. (2018) and Rong & Tian (2015). Future study can investigate a combination of STPA and a traditional method as part of a workshop-based approach, such as Faiella et al. (2018) who carried out a study combining safety management methods. In addition, this research work could be further expanded to include not only experts but early career professionals in the field on SA to understand their perspectives.

CRediT authorship contribution statement

Dapo Oginni: Writing – review & editing, Validation, Project administration, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Fanny Camelia:** Writing – original draft, Supervision, Methodology, Conceptualization. **Mikela Chatzimichailidou:** Writing – review & editing, Supervision. **Timothy L.J. Ferris:** Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgement

We gratefully acknowledge the assistance of the Systems Engineering Integration and Assurance team of WSP UK, who provided us with their time, space, and specialists to perform interviews and shared their expertise in Systems Engineering and System Safety within the rail sector.

References

Beaumont, P., Wolthusen, S., 2019. Micro-Grid Control Security Analysis: Analysis of Current and Emerging Vulnerabilities. In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (Eds.), Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies. Springer International Publishing, pp. 159–184. https://doi.org/10.1007/978-3-030-00024-0_9.

Bugalia, N., Maemura, Y., Ozawa, K., 2020. Organizational and institutional factors affecting high-speed rail safety in Japan. Saf. Sci. 128, 104762 https://doi.org/10.1016/j.ssci.2020.104762.

Chatzimichailidou, M., Dunsford, R., 2019. Providing for Safety in Rail Megaprojects. WSP Insights. https://www.wsp.com/en-GB/insights/providing-for-safety-in-rail-megaprojects.

Chatzimichailidou, M.M., Dokas, I.M., 2016. RiskSOAP: Introducing and applying a methodology of risk self-awareness in road tunnel safety. Accid. Anal. Prev. 90, 118–127.

Chatzimichailidou, M.M., Stanton, N.A., Dokas, I.M., 2015. The concept of risk situation awareness provision: Towards a new approach for assessing the DSA about the threats and vulnerabilities of complex socio-technical systems. Saf. Sci. 79, 126–138. https://doi.org/10.1016/j.ssci.2015.05.012.

Dunsford, R., Chatzimichailidou, M., 2020. Introducing a system theoretic framework for safety in the rail sector: supplementing CSM-RA with STPA. Saf. Reliab. 39 (1), 59–82. https://doi.org/10.1080/09617353.2019.1709289.

Faiella, G., Parand, A., Franklin, B.D., Chana, P., Cesarelli, M., Stanton, N.A., Sevdalis, N., 2018. Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach. Reliab. Eng. Syst. Saf. 169, 117–126. https://doi.org/10.1016/j.ress.2017.08.003.

Ferris, T.L.J., Camelia, F., Mattsson, T., Machado, R.C., 2022. Red-Teaming as a Research Validation Method for Systems Engineering Thesis Students. 32nd Annual INCOSE International Symposium, Detroit, MI, USA.

Fowler, K.R., 2015. Chapter 7—Analyses and Tradeoffs. In: Fowler, K.R., Silver, C.L. (Eds.), Developing and Managing Embedded Systems and Products. Newnes, pp. 189–234. https://doi.org/10.1016/B978-0-12-405879-8.00007-6.

Government Office for & Science, 2022. Systems thinking: An Introductory Toolkit for Civil Servants. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079384/GO-Science_Systems_Thinking_Toolkit_2022_v1.0.pdf.

Health and Safety Executive, 2022. ALARP 'at a glance'. https://www.hse.gov.uk/managing/theory/alarpglance.htm.

Hegde, R., Yako, S., Post, K., Nuesch, S., 2019. Systems theoretic process analysis for layers of system safety. INCOSE Int. Sympos. 29 (1), 895–909. https://doi.org/10.1002/j.2334-5837.2019.00642.x.

Hirao, Y., 2020. Techniques at the forefront of system safety and their application to railway signalling. International Technical Committee, Institution of Railway Signal Engineers (IRSE) News.

Holen, S.M., Utne, I.B., 2018. A Framework based on a systems approach to developing safety indicators in fish farming. Safety 4 (2), Article 2. https://doi.org/10.3390/safety4020019.

Jamot, D.G.C., Park, J.Y., 2019. System theory based hazard analysis for construction site safety: a case study from Cameroon. Saf. Sci. 118, 783–794. https://doi.org/10.1016/j.ssci.2019.06.007.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42 (4), 237–270. https://doi.org/10.1016/S0925-7535(03)00047-X.

Leveson, N., 2011. Engineering a Safer World: Systems Thinking Applied to Safety, 1st edn. The MIT Press, Massachusetts.

Leveson, N., 2018. Safety analysis in early concept development and requirements generation. INCOSE Int. Sympos. 28 (1), 441–455. https://doi.org/10.1002/j.2334-5837.2018.00492.x.

Leveson, N., Stephanopoulos, G., 2014. A system-theoretic, control-inspired view and approach to process safety. AIChE J 60 (1), 2–14. https://doi.org/10.1002/aic.14278.

Leveson, N., Thomas, J., 2018. STPA Handbook. 188.

Lower, M., Magott, J., Skorupski, J., 2018. A system-theoretic accident model and process with human factors analysis and classification system taxonomy. Saf. Sci. 110, 393–410. https://doi.org/10.1016/j.ssci.2018.04.015.

Office of Rail and Road, 2018. Common Safety Method for Risk Evaluation and Assessment'. Guidance on the application of Commission Regulation (EU) 402/2013.

Patriarca, R., Chatzimichailidou, M., Karanikas, N., Di Gravio, G., 2022. The past and present of system-theoretic accident model and processes (STAMP) and its associated techniques: a scoping review. Saf. Sci. 146, 105566 https://doi.org/10.1016/j.ssci.2021.105566.

Rekabi, M.M., 2018. Bayesian Safety Analysis of Railway systems with Driver errors. Norwegian University of Science and Technology [MSc thesis].

Rong, H., Tian, J., 2015. STAMP-Based HRA Considering Causality Within a Sociotechnical System: A Case of Minuteman III Missile Accident. Hum. Factors 57 (3), 375–396. https://doi.org/10.1177/0018720814551555.

Samadi, J., Garbolino, E., 2018. Systems Theory, System Dynamics and Their Contribution to CTSC Risk Management. In: Samadi, J., Garbolino, E. (Eds.), Future of CO2 Capture, Transport and Storage Projects: analysis Using a Systemic Risk Management Approach. Springer International Publishing, pp. 27–39. https://doi.org/10.1007/978-3-319-74850-4_2.

SEBoK Editorial Board, 2022. The Guide to the Systems Engineering Body of Knowledge (SEBoK) (v. 2.6). www.sebokwiki.org.

Silva, S.R.e., 2019. System Theoretic Process Analysis: A Literature Survey on the Approaches Used for Improving the Safety in Complex Systems. https://link.springer.com/chapter/10.1007/978-3-030-14850-8_7.

Takata, T., Nakamura, H., 2019. Safety Analysys Using STAMP/STPA for Electronic Interlockings. 8.

Thomas, J. (Director), 2021. Introduction to STPA: Anticipating & Preventing Loss Scenarios in Complex Systems [YouTube Video]. https://www.youtube.com/watch?v=2W-iqnPbhyc.

Yousefi, A., Rodriguez Hernandez, M., 2019. Using a system theory based method (STAMP) for hazard analysis in process industry. J. Loss Prev. Process Ind. 61, 305–324. https://doi.org/10.1016/j.jlp.2019.06.014.

Yousefi, A., Rodriguez Hernandez, M., Lopez Peña, V., 2019. Systemic accident analysis models: a comparison study between AcciMap, FRAM, and STAMP. Process Saf. Prog. 38 (2), e12002.

Cranfield University

CERES Research Repository **https://dspace.lib.cranfield.ac.uk/**

Cranfield Defence and Security Staff publications (CDS)

Applying System-Theoretic Process Analysis (STPA)-based methodology supported by Systems Engineering models to a UK rail project

Oginni, Dapo

2023-08-07

Attribution-NonCommercial 4.0 International

Oginni D, Camelia F, Chatzimichailidou M, Ferris TLJ. (2023) Applying System-Theoretic Process Analysis (STPA)-based methodology supported by Systems Engineering models to a UK rail project. Safety Science, Volume 167, November 2023, Article number 106275
https://doi.org/10.1016/j.ssci.2023.106275

Downloaded from CERES Research Repository, Cranfield University