Managing a System Safety Case in an Integrated Environment

Saeed Fararooy, rcm2 limited
Cheltonian House, Portsmouth Road
Esher, Surrey KT10 9AA, UK
+44 1372 468312
md@rcm2.co.uk

Keywords: Safety Cases, Hazard Log, Safety Requirements, Goal Structuring Notation, Traceability

ABSTRACT

This paper presents the challenges for development and maintenance of the safety case for electrical, electronic and programmable electronic systems (E/E/PES) used in safety-critical applications. A Remote Condition Monitoring (RCM) system is taken as a show case to demonstrate the elements of a safety case from concept, requirements and design through implementation, test, integration and transition to use. This reviews the techniques that may be used to manage safety issues at different phases of the project, namely:

a) Safety case data models such as Goal-Structuring Notation (GSN) to assist with the top-down planning of the safety goals, strategies, assumptions, models and context as well as arguments and evidence
b) Preliminary hazard analysis and the structure of a hazard log, its population and management
c) Compliance with safety regulations & standards
d) Full traceability and audit trail
e) Management information such as a summary safety risk classification matrix.

1 INDRODUCTION

When managing a complex system, at least one central shared database is indispensable for a team of developers and all other stakeholders. Safety is one important aspect of such a complex systems and is best addressed under the "fitness for purpose" paradigm. In other words: Is the system designed, developed, implemented, operated and maintained to be as safe as it needs to be? A recent study by the UK Health & Safety Executive (HSE) found that a greater volume of significant hazards were identified at the early conceptual and requirements phase of any project/product development. Yet, there is a knowledge gap between the safety engineering community and the systems engineering and requirements management world. The following problems with existing approaches based on status-quo were identified:

- Non-common processes – Parallel and disparate processes for managing safety as opposed to managing other system requirements;
- Re-inventing the wheel each time a new safety case project commences;
- Non-integrated approach – Generally many obstacles in unifying engineering and acceptance team efforts and insufficient integration within each team ('silo-working' leading to 'weakest-link' syndrome);
- Manual traceability – The most common IT tools for safety case production remain MS-Office (Word, Excel, …) resulting in difficulty of traceability between multitudes of separate generated documents;
- Lack of Control Tools – It was not possible to impose a credible technical management plan to monitor and review the safety case production process.

The approach promoted in this paper is one that attempts to overcome the above shortcomings. We have seen through dialogue with over 300-strong system safety and systems engineering community in the past year that the above problems are being recognised and several attempts are being made to bring an integrated approach to manage safety in synergy with other system features. In section 3, we introduce a case study of a novel distributed RCM system to demonstrate issues related to the development of a safety case. These include HAZard IDentification (HAZID, section 4), compliance with requirements in safety standards, regulations and best practice (section 5) and presentation of a structured case for safety with appropriate argumentation and supportive evidence (section 6). In section 7, we outline the features of an Integrated Safety Case Development Environment (ISCaDE), a commercial off-the-shelf software package, that we used to bring together all elements of the RCM system safety case. Benefits of the approach adopted and the integrated environment used are summarised in the conclusions.

2 RCM SYSTEMS

The Railwise RCM system under study here is a prototype distributed system based on fieldbus technology installed over existing safety-critical railway signalling equipment. It was developed as a collaborative industry-academia research programme at the University of Birmingham (UK).

The Railwise RCM system is designed specifically for the **purpose** of providing warning of incipient failures in safety-critical electro-mechanical systems such as signalling equipment (point machines, level-crossing). It allows the prediction of faults by input analogue and digital signals into knowledge of the state of the health of equipment being monitored. The system is intended to be used in the railway industry for remote condition and event monitoring. It has the following **functionality**:

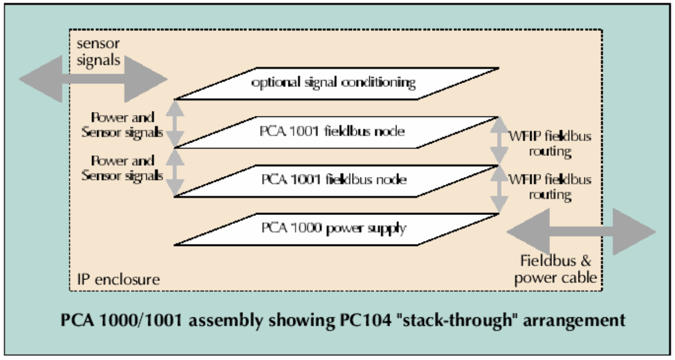
- Collects data from sensors attached to signalling asset (Equipment Being Monitored - EBM)
- Transmits data to a trackside PC (TSPC)
- Transmits data to Central Remote Monitoring PC (RCHSP)
- Stores data in a memory device
- Displays data using graphical interface (GUI)
- Analyses data, compares with normal mode and warns of abnormal deviations.

The Railwise system has a **distributed architecture** at four levels:

1. Physical layer: sensors and Fieldbus nodes
2. Data Link layer: defines the methods used to transmit and receive digital data, WorldFIP PC card
3. Transport layer: manages the flow control of data,employs WorldFIP protocol
4. Presentation layer: presents graphical information

Railwise employs WorldFIP Fieldbus distributed data acquisition technology. The network consists of track side elements (Fieldbus nodes and sensors, track side PC), server PC (RCMSP), data communication (modems), data presentation and analysis.

Figure 1 – A Typical Fieldbus Node Architecture

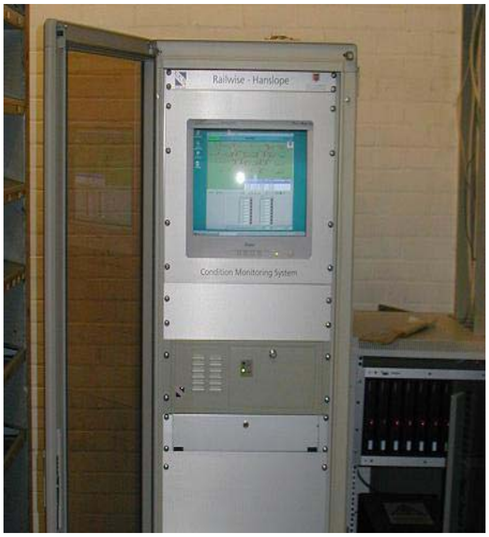


PCA 1000/1001 assembly showing PC104 "stack-through" arrangement

Fieldbus nodes - The transducers are connected to the Fieldbus network using WorldFIP communication protocol (specified in IEC-61158). Two different types of nodes have been designed – the digital node and the analogue node. The digital node acquires digital data from spare relay contacts and digital output signals from external monitoring equipment. Each analogue node is designed to provide an independent isolated power supply to two transducers and transmit the transducers output across the Fieldbus network to the PC. The analogue nodes are situated locally to the sensors (<500 m).

Trackside PC (TSPC): An on-site PC is used to control the network and process the data acquired. It should be housed in a floor standing lockable cabinet to provide security. The PC is required to transmit and receive data using a telephone modem. Industrial PC uses RAID technology for data backup. (see Figure 2 – TSPC).

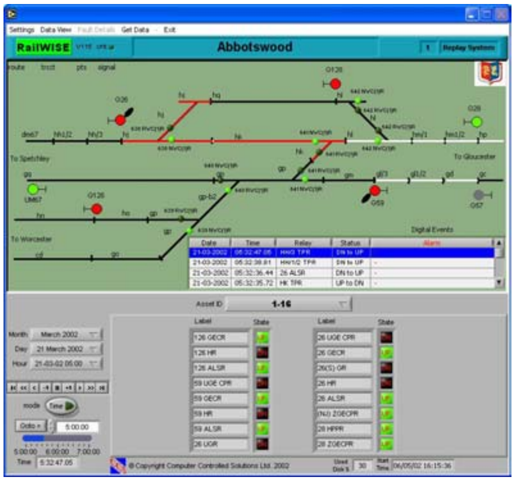
Figure 2 – Railwise RCM Track-side PC



Server PC (RCMSP): RCMSP connected to TSPC using ADSL, ISDN or plain old telephone system. It can be used as auto backup, alarm or data controller. The Server PC allows the publication of information on the Internet via an XML interface.

Data Presentation and Analysis. RailWISE provides the user with a mimic layout of the selected junction assets with the ability to dial up the site PC to retrieve data. Once the data has been downloaded to the system, the data files can be selected and analysed using CD player style controls to play/rewind events or to single step through the data. There are also options to edit the configuration file, view/print digital lists, export configuration files and view live analogue data.

Figure 3 – A Typical Railwise GUI Front-end



Date	Time	Relay	Status	Alarm
21-03-2002	05:32:47.05	HH/3 TPR	DN to UP	
21-03-2002	05:32:38.81	HH/1/2 TPR	DN to UP	-
21-03-2002	05:32:36.44	26 ALSR	DN to UP	-
21-03-2002	05:32:35.72	HK TPR	UP to DN	-

Month: March 2002
Day: 21 March 2002
Hour: 21-03-02 05:00

Label	State	Label	State
126 GECR	UP	26 UGE CPR	DN
126 HR	DN	26 GECR	UP
126 ALSR	UP	26(S) GR	DN
59 UGE CPR	DN	26 HR	DN
59 GECR	UP	26 ALSR	UP
59 HR	DN	(NJ) ZGECPR	UP
59 ALSR	UP	28 HPPR	UP
26 UGR	DN	28 ZGECPR	UP

5:00:00 6:00:00 7:00:00
Time 5:32:47.05
Used Disk % 30
Start Time 06/05/02 16:15:36

RailWISE System Boundary - The RailWISE System consists of appropriate transducers, Fieldbus nodes and network power supply, network cables, TSPC and RCMSP. The transducer signal is converted into appropriate data to be transmitted to the WorldFIP PC card using the WorldFIP interface. A PCA1001 Fieldbus node circuit board is used to convert data. A PCA1000 Fieldbus power supply interface board is designed to convert voltage into a form that can be used to supply the system. RailWISE is a non-intrusive overlay system and will receive data through previously approved transducers and external monitoring systems.

3 SYSTEM HAZID

The purpose of the HAZID workshop was to identify hazards related to the Railwise (RCM) for a typical application on London Underground Limited (LUL) infrastructure. The objective was to ensure that there was sufficient evidence in support of Railwise (RCM) safety argument that system-level hazards are identified, eliminated mitigated or controlled to an As Low As Reasonably Practicable (ALARP) level.

3.1 Hazard Analysis Process

The hazard identification process as defined in the Yellow Book [1] and EN50126 [2] was used. The step adopted here identifies:

- Each hazard and its cause (causal factor/precursor).
- Hazard consequences (hazardous events).
- Any existing controls over the hazard.
- Scenario that best describes the hazard.
- The impact of the hazard to the overall risk.
- Mitigation/barriers (additional potential controls) over the hazard and its likely consequences.

Harmful consequences of hazard (incidents and accidents, also known as 'hazardous events') were grouped as follows: train collisions; train derailment; collision with an object on the line; Passenger injury/loss and/or worker injury/loss.

3.2 Hazard Analysis Guidewords.

The following guidewords were used to prompt the identification of hazards during the HAZID brainstorming sessions:

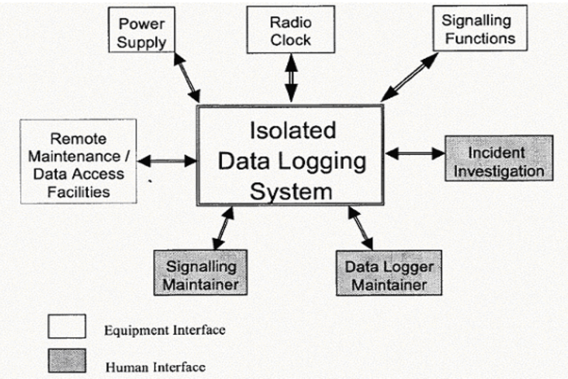
A) Life-cycle issues: An activity checklist was used for each lifecycle phase:

- Design (FMECA, EMC Tests)
- Installation (cabling)
- Test & Commissioning
- Operation (Manuals, Strategy, Training)
- Maintenance (Manuals, Strategy, Training)
- Decommissioning and Disposal

B) Interfaces (e.g. with Signalling or other assets): Example factors/guidewords used:

- Sensors – Equipment Being Monitored
- Sensors – Trackside PC
- Trackside PC – Server PC
- Signalling Centre – RTC LAN
- Data Centre - RCMSP
- Alarm Centre – RCMSP
- RCMSP – TSPC Comms

Figure 4 - RCM System External Interfaces



3. 3 HAZID Session Stakeholders.

The following competencies provided an input into the hazard analysis process:

- Supplier Representatives - Those with experience of system design, development and installation
- Safety Approval experts - Those from the infrastructure owner/operator/maintainer, with experience of the approval process for non-safety-critical RCM equipment
- Safety and Risk Management Consultants - rcm2 limited acting also as facilitators

3.4 Safety Risk Matrix.

Each hazard was assessed for its probability of occurrence and severity of its consequences. This allowed the identification of the risk the hazard contributed to the overall risk of the installation and operation of the system. The assessment was carried out by assigning each hazard with a probability and severity rating as detailed in the Tables 1, which in turn determined the overall risk rating.

Table 1 Probability that the hazard will occur

Category	Rating	Description
Frequent	6	Continually experienced.
Probable	5	Several times, Often.
Occasional	4	Several times but not often
Remote	3	Sometimes during lifecycle.
Improbable	2	Unlikely to occur but possible though exceptional.
Incredible	1	Extremely unlikely or Never.

It is often common practice for participants at HAZID session to agree a range of values to which each of these probabilities refer to. For example, "incredible" may refer to a potential accident or harmful incident once in 100 years and "improbable" once in a decade. Generally you may draw on analogy between a new hazard, a similar one, and ask the question that in the past say 10 years how many such incidents have occurred and therefore try to guesstimate the probability of the occurrence of the new hazard in the future.

Table 2 Severity - The level of impact the hazard will have

Severity Level	Rating	Consequence	Consequence to service
Catastrophic	4	Fatalities and/or major damage to the environment	Political (nation-wide or industry-wide)
Critical	3	A fatality and/or severe injury and/or environmental damage	Loss of a major system
Marginal	2	Minor injury and/or significant threat to the environment	Severe system damage
Minor	1	Possible minor injury	Minor system damage

The Overall Risk Rating (ORR) is a summation of the probability and severity ratings and determines the risk level of the hazard. The summation is based on the fact that each of the severity and probability ratings represent an order of magnitude increase from its predecessor, hence addition rather than multiplication of values based on logarithmic scales. An ORR of 4 or less is acceptable, in which case no action is required and between 5 and 7 the risk is tolerable and above 7 it is intolerable. In the last two cases actions have to be taken to try to reduce the risk to be as low as the (ALARP).

For Railwise RCM system case study, typical hazards included:

- Electrical shock to the technician from high voltage sources
- Electro-magnetic interference (EMI) issues
- RCM signals interfering with safety-critical signals as a result of bare cables, or RCM faults transferring incorrect potentials to safety-critical signaling circuitry.

Table 3 Risk Assessment

Occurrence	Risk Levels			
Frequent	7 lerable	8 Int	9	10 tolerable
Probable	6 Tolerable	7 To	8 Intolerable	9 Intolerable
Occasional	5 Tolerable	6 To	7 Tolerable	8 Intolerable
Remote	4 Acceptable	5 To	6 Tolerable	7 Tolerable
Improbable	3 Acceptable	4 Acceptable	Tolerable	erable
Incredible	2 Acceptable	3 able	4 Acceptable	5 Tolerable
Severity ->	**Negligible**	**Marginal**	**Critical**	**Catastrophic**

4 SAFETY REQUIREMENTS

A range of generic safety regulations and specific safety requirements apply to any novel electrical, electronic or programmable electronic system (EEPES). It is often a very time consuming exercise for any safety engineer to have to go through all existing regulations and standards in order to identify the ones that are applicable to the project in hand and to ensure that a complete, correct, clear, concise and consistent set of requirements are derived for the EEPES under study. A typical generic standard applicable to RCM case study is IEC61508 [3], and a specific industry standard is RT/ES/11304 [4]. In Section 7, we show how ISCaDE was used to facilitate this task as well as to allow potential changes/updates of standards to be traced and their impacts reviewed during the product life-cycle. It must also be noted that during the HAZID, specific new requirements may be derived to eliminate, mitigate or control newly identified hazards. It may also be useful to have a short-hand list of the most relevant safety requirements pertinent to the EEPES under study at the HAZID session in order to prompt the participants not to miss the obvious hazards that the requirements are designed to manage.

5 SAFETY CASE ARGUMENTATION

The maintenance of a hazard log, risk assessment and compliance with safety requirements are now the cornerstones of any system safety management standard for safety-critical industries [e.g. 5]. These, however, are not sufficient for addressing the central claim that the system is safe for its intended mission, and most Standards now require the production of a System Safety Case. The *Safety Case* shall contain a structured argument demonstrating that the evidence contained therein is sufficient to show that the system is safe. A safety case is often a larger requirement and implies a set of arguments and evidence to support a central claim and a structured set of (associated) sub-claims. A safety case, therefore, consists of;

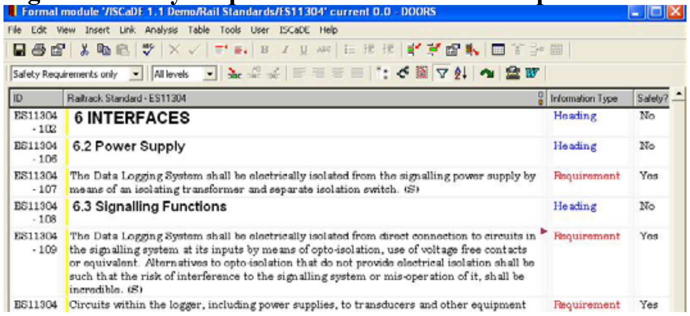
- Goals/Claims – An explicit set of objectives (goals/claims) about the system, whether an undertaking, project or product. These are safety requirements that are adequate and shall be met in a given context (application/environment) based on well-defined validation criteria,
- Evidence – Supporting processes and documents such as risk modelling, hazard identification, risk reduction measures, quality and safety management system and audit reports,
- Arguments – A set of arguments that link the evidence to the goals (claims), together with any underlying assumptions and judgements.

Various graphical notations have been proposed to support the development and presentation of system safety cases. These notations are readily used at the early safety case planning phase to identify focus areas needing attention in terms of argumentation and evidence gathering. They are alternatively used at the safety audit and approval phases by independent assessors to find their way logically through a myriad of documents pertaining to a particular system safety case. Safety case notations are discussed in Section 6.5 below.

6. INTEGRATED DATABASE ENVIRONMENT

ISCaDE is a networked software environment that uses the DOORS (Dynamic Object-Oriented Requirement System) database as its platform.. It combines the features of a multi-user, multi-access, object-oriented database and graphical presentation capabilities in an integrated environment that marries different safety case development techniques: GSN with Hazard Log and traceability to safety requirements/standards compliance.

Figure 5. Safety Requirements/Standards Compliance



Formal module '/ISCaDE 1.1 Demo/Rail Standards/ES11304' current 0.0 - DOORS

File Edit View Insert Link Analysis Table Tools User ISCaDE Help

Safety Requirements only | All levels

ID	Railtrack Standard - ES11304	Information Type	Safety?
ES11304 - 102	6 INTERFACES	Heading	No
ES11304 - 106	6.2 Power Supply	Heading	No
ES11304 - 107	The Data Logging System shall be electrically isolated from the signalling power supply by means of an isolating transformer and separate isolation switch. (S)	Requirement	Yes
ES11304 - 108	6.3 Signalling Functions	Heading	No
ES11304 - 109	The Data Logging System shall be electrically isolated from direct connection to circuits in the signalling system at its inputs by means of opto-isolation, use of voltage free contacts or equivalent. Alternatives to opto-isolation that do not provide electrical isolation shall be such that the risk of interference to the signalling system or mis-operation of it, shall be incredible. (S)	Requirement	Yes
ES11304	Circuits within the logger, including power supplies, to transducers and other equipment	Requirement	Yes

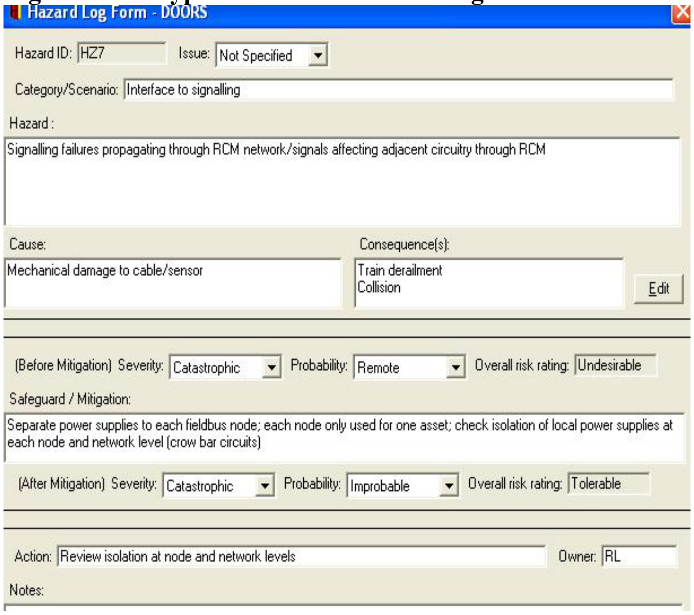
6.1 Safety Standards & Safety Requirements Capture.

A common challenge to the development of product safety case is to identify the applicable safety standards and legislation and to develop new safety requirements that should drive the design and other phases of the product development. This may be an iterative process and needs to be managed throughout the product's lifecycle. ISCaDE provides an 'Initialise Standard' functionality and allows the whole standard to be imported but only relevant clauses marked as safety requirements and saved as a view for future traceability purposes. A structured word document is therefore turned into a database table and additional attributes such as validation and verification criteria and tests may be assigned to each safety requirement (Fig. 5).

6.2 The Hazard Log and Hazard Log Form.

ISCaDE allows a configurable hazard log with an easy to use data entry form. Each hazard is given a unique identifier and as a DOORS 'Object' has properties that include cause, scenarios leading to consequences (accidents and incidents), probability and severity of accidents and the overall risk rating, mitigation and controls, the state of each hazard, actions recorded and the actionees (Fig. 6).

Figure 6 – A Typical ISCaDE Hazard Log Form



Hazard Log Form - DOORS

Hazard ID: HZ7 Issue: Not Specified

Category/Scenario: Interface to signalling

Hazard: Signalling failures propagating through RCM network/signals affecting adjacent circuitry through RCM

Cause: Mechanical damage to cable/sensor

Consequence(s): Train derailment
Collision

(Before Mitigation) Severity: Catastrophic Probability: Remote Overall risk rating: Undesirable

Safeguard / Mitigation: Separate power supplies to each fieldbus node; each node only used for one asset; check isolation of local power supplies at each node and network level (crow bar circuits)

(After Mitigation) Severity: Catastrophic Probability: Improbable Overall risk rating: Tolerable

Action: Review isolation at node and network levels Owner: RL

Notes:

6.3 Hazards/Safety Requirements Gap Analysis.

The ability to provide many to many traceability links between hazards and safety requirements is an advantageous feature of the ISCaDE environment. This allows identification of gaps, on the one hand development of new requirements that control/mitigate hazards and on the other ensuring that all hazards that existing standards imply are identified and managed.

6.4 Safety Risk classification Matrix.

It is often important for engineers to monitor progress with safety and hazard management at the system level in order to present it to management. ISCaDE produces a system safety risk classification martrix automatically from the snap-shot information stored in the system hazard log (similar to Table 3).

6.5 Safety Case Notations.

ISCaDE allows automatic production of safety case diagrams from a safety case notation structures such as:

a) **Goal-Structuring Notation** (GSN) is a graphical approach to presenting the structure of a safety argument.

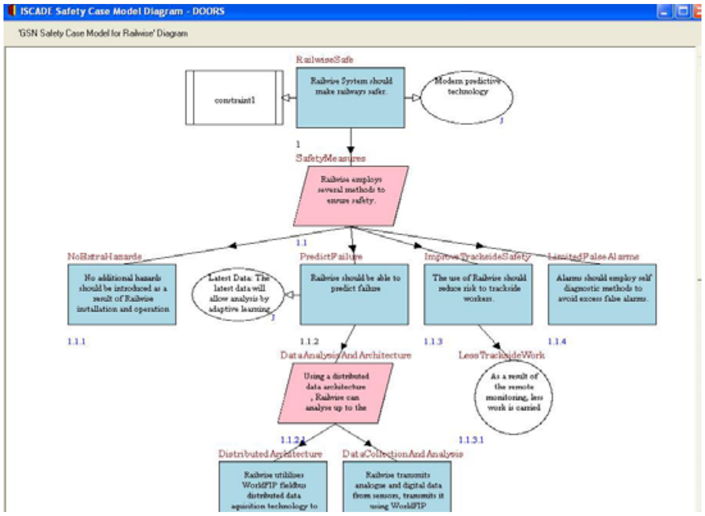
Goal hierarchies consist of: *Goals* – a requirement, target or constraint to be met by the system; *Strategies* – rules to be invoked in the solution of goals; *Context*; *Models*; *Justification*; *Assumption* and *Solutions* – evidence, analysis, design review and audit report.

b) Adelard Safety Case Development Manual (ASCAD) is a total safety case development strategy. It is based on Evidence-Argument-Claim structure: *Claims* about the properties of the system; *Evidence* used as basis for the safety argument; and *Argument* that links the evidence to the claims via a series of inference rules.

c) Weighted Factor Analysis (WeFA) is a graphical presentation of drivers and inhibitors to a top safety goal or objective. Each driver/inhibitor is in turn a sub-goal with a different positive/negative contribution to the higher level goal, represented by a weighting factor.

Each of the above notations has its particular strengths. The WeFA model allows one to view the opportunities for improving safety the new product entails as well as the threats (managing hazards). ASCAD uses the terminology (evidence, argument) readily used by engineers in their safety case documentation. GSN, on the other hand, benefits from the ability to assign attributes such as Context, Justification and Assumptions to goals (claims) and strategy (arguments) and the 'solution' is where supportive 'evidence' of compliance or argumentation is phrased. Figure 7 shows an ISCaDE-generated GSN diagram for the Railwise system.

Figure 7 – ISCaDE GSN for Railwise


ISCADE Safety Case Model Diagram - DOORS
'GSN Safety Case Model for Railwise' Diagram
RailwiseSafe
Railwise System should make railways safer.
constraint1
Modern predictive technology
J
1
SafetyMeasures
Railwise employs several methods to ensure safety.
1.1
NoExtraHazards
No additional hazards should be introduced as a result of Railwise installation and operation
Latest Data: The latest data will allow analysis by adaptive learning
J
PredictFailure
Railwise should be able to predict failure
ImproveTracksideSafety
The use of Railwise should reduce risk to trackside workers.
LimitedFalseAlarms
Alarms should employ self diagnostic methods to avoid excess false alarms.
1.1.1
1.1.2
1.1.3
1.1.4
DataAnalysisAndArchitecture
Using a distributed data architecture , Railwise can analyse up to the
LessTracksideWork
As a result of the remote monitoring, less work is carried
1.1.2.1
1.1.3.1
DistributedArchitecture
Railwise utilises WorldFIP fieldbus distributed data aquisition technology to
DataCollectionAndAnalysis
Railwise transmits analogue and digital data from sensors, transmits it using WorldFIP

7. CONCLUSIONS

The overall approach advocated in this paper is to view the safety approval process as synergetic to, and in parallel with, the systems engineering and requirements management processes. In other words, the safety paradigm is an intrinsic element of the overarching problem: is the system 'fit for purpose'? And is the safety managed accordingly, i.e. do the safety requirements (that control/mitigate hazard), design features, implementation etc. meet the system mission? This approach was demonstrated for the RCM case study using Integrated Safety Case Development Environment (ISCaDE), a commercial-off-the-shelf (COTS) software package. ISCaDE extends the features of the DOORS requirements management database to cover the techniques and processes widely used for safety management. The benefits and challenges of using such an integrated environment may be summarised as follows:

- No duplication or missing effort as all project information including safety is managed within a single object-oriented database.
- Transparency of information to all team members within a secure multi-user multi-access environment.
- Graphical presentation of safety information automatically from the structured data for the benefit of all stakeholders including managers to monitor progress with technical aspects of the product/project.
- Automatic traceability and a full audit trail between all elements of a system safety case and the processes and techniques used in its development and maintenance.
- Encouraging and facilitating cooperative teamwork.
- Saving considerable time and money, ultimately leading to a safer and less expensive end-product.

8. REFERENCES

1. Railtrack Engineering Safety Management (Yellow Book). 2000. (Issue 3).
2. BS EN 50126 Railway applications, The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 1999.
3. IEC61508: Functional Safety of Electrical, Electronic and Programmable Electronic Safety-Related Systems (EEPES). 1998.
4. RT/ES/11304: Requirement for Data Logging Systems used to Monitor Signalling Installations. 2003. (Issue 1).
5. DEF STAN 00-56, Safety Management Requirements for Defence Systems, Part 1: Requirements, Final Draft. 2004. (Issue 3).

Biography

Dr Saeed Fararooy is the managing director of rcm2 limited, a small high-tech UK company offering system safety and reliability consultancy, training and systems/IT engineering/integration services to transportation/other safety-critical industries. He is an electronic control systems engineer with over 22 years experience in a range of industries from manufacturing and process to transportation.