Innovation vs Safety:
Hazard Analysis Techniques to Avoid Premature Commitment during the Early Stage Development of National Critical Infrastructures

Chris W. Johnson,

School of Computing Science, University of Glasgow, Glasgow, UK, G12 8RZ.

Keywords: Reliability, Availability, Maintainability and Safety, RAMS, Rail Safety, Safety-Management.

Abstract

Preliminary hazards analysis techniques help to identify safety concerns during the early stages of development. However, they often rely on scoping studies and functional decompositions that can be hard to sustain without premature commitment to particular software architectures. For example, small alterations to the high-level design of a critical infrastructure force radical change in the underlying hazard analysis. This creates tensions – safety managers can become "enemies of innovation" if they oppose modifications that create additional work redoing the hazard analysis. Equally, it can be hard for safety managers to control project costs if alterations to the underlying architecture force continual changes in the safety assessments. These tensions are compounded because many hazard analysis techniques have their roots in the 1960s when issues of scale, modularity and reuse were arguably less of a concern than they are today. These arguments are illustrated by the EATS project on Advanced Testing and Smart Train Positioning System for the next generation European Train Control System. This integrates a range of wireless infrastructures with input from Satellite Based Augmentation Systems to reduce reliance on trackside infrastructures. However, the dynamic, multidisciplinary nature of the work has created a need for continuous feedback on potential safety concerns as lab and bench studies continue to innovate with novel software architectures and prototype implementations. We present a number of approaches that can be used to balance the need for design commitment to support safety assessments and the flexibility required in early stage development of critical national infrastructures.

Introduction

There is a concern across European and North American railways to support increased levels of traffic without compromising safety. Very different accidents, especially the Lac-Mégantic derailment in Canada and the Santiago de Compostela derailment in Spain, have reinforced the importance of work in this area, even though rail transport remains extremely safe [1]. In the United States, concerns about capacity and safety have led to a series of research and development projects associated with Positive Train Control (PTC). PTC integrates data and voice communications to reduce the likelihood of accidents including collisions and derailments, as well as increasing protection for trackside workers. The underlying technologies for PTC include digital data link communications as well as satellite positioning systems. In particular, National Differential GPS (NDGPS) uses a network of ground-based reference stations to improve the accuracy of conventional GPS signals. The differences between the satellite signals and the known location of the receivers can be measured to compute corrections or pseudo-ranges. These corrections are then broadcast so that end users can update their position estimates from raw GPS. This reduces accuracy errors from tens of meters to tens of centimeters. The underlying PTC technologies support a wide range of innovative in-cab displays using digitized maps to continually update the position of other traffic, including maintenance crews and equipment. By collating this information, it is possible to improve safety and improve capacity through innovative scheduling techniques

In Europe, similar attention has focused on the development and delivery of the European Train Control System (ETCS). This uses slightly different infrastructure to the North American PTC proposals; however, the aims and objectives are comparable. To ease deployment, a number of different levels have been defined for ETCS, these support different concepts of operation and are summarized in the following list:

- ETCS Level 1 is a cab signaling system that can be superimposed on existing signaling infrastructures. Trackside (balise) radio beacons are deployed at fixed intervals. These detect signal aspects and transmit them as a 'movement authority' to any vehicle passing over that section of track. On-board systems monitor the signals and use them to calculate maximum speed/braking requirements.

- ETCS Level 2 relies on digital radio communications to implement train protection with advanced displays for the driver to remove/reduce the need for track side signaling. A Radio Block Centre

(RBC) uses radio signals to monitor the location of trains at regular intervals. Movement authority is transmitted continuously via GSM-R, which resembles the more conventional cellular GSM infrastructure for mobile telephones, together with balises acting as positioning beacons. On-board sensors help to locate the vehicle between balises by integrating data from braking and propulsion systems.

- ETCS Level 3 provides dynamic spacing between vehicles using radio signals. The RBC can detect when a train has left a track location and can, therefore, grant movement authority to any following train up to that point. There is, therefore, no notion of track sections being locked and released. Separation must preserve absolute braking distances between vehicles, taking into account terrain features, meteorological conditions, legacy rolling stock etc. Data from balise, from on-board systems and potentially from Global Navigation Satellite Systems (GNSS) similar to NDGPS is integrated and monitored to assess the integrity of the positioning information and of the supporting on-board systems. In ETCS, the enabling GNSS technology often includes the use of EGNOS – instead of ground based local broadcasts to update GPS pseudoranges, a geostationary satelite system is used.

Only ETCS levels one and two have seen sustained deployment in an operational context. The barriers to full implementation of ETCS level three are addressed in the remainder of this paper. For now it is sufficient to observe that the migration from ETCS level 2 to level 3 will significantly increase railway efficiency. However, it also places Reliability, Availability, Maintainability and Safety (RAMS) demands on GNSS infrastructures, which cannot be overcome using enhanced EGNOS or GPS in isolation.

Reliability, Availability, Maintainability and Safety (RAMS) Concerns in the Rail Industry

Not only are there similarities between the proposed use of GNSS across European and North American railways, there have also been similar problems in moving from high-level design through detailed development to full deployment. Most of the technologies within PTC were successfully demonstrated more than a decade ago; however, wireless versions of the Incremental Train Control System still suffer from reliability concerns. In consequence, the Federal Railroad Agency have prioritized the deployment of PRC as the Rail Safety Improvement Act of 2008 sets a deadline of December, 2015, for implementation of positive train control (PTC) technology across the U.S. rail network. There have also been significant delays in putting ETCS level one and two equipment into service. One of the reasons for this is that there can be difficult for manufacturers and operators to correctly interpret the existing ETCS specifications that govern the development of these systems. Small differences can lead to significant costs when integrating level one and two equipment. There is, therefore, a concern to provide simulation and prototyping environments that can be used to identify potential problems prior to deployment.

This paper focuses on work within the ETCS Advanced Testing and Smart Train Positioning System (EATS) project. EATS started in October 2012 with two related aims. Firstly, it will provide a model of the complete on-board European Railway Train Management System behavior to reduce the interpretation differences that have delayed the deployment of level one and two infrastructures. Secondly, it is developing a laboratory of tools that can be used to model the dynamic behavior of wireless interfaces, including GNSS systems. Together will lead to reduced laboratory and field-testing certification process time and cost. In particular, the intention is that the ERTMS model and laboratory tools will increase confidence in the safety and reliability arguments that must support any deployment and which are crucial to increase the speed of ETCS deployment [2, 3].

In order to validate the application of the model and the lab tools, the EATS project has focused on a set of problems that are common both to ETCS and to the North American plans for PTC. These problems relate to the integration of positioning data from a number of sources including GNSS, GSM-R and Universal Mobile Telecommunications System (UMTS) with a novel Smart Train Positioning System. UMTS is a third generation mobile cellular system for networks based on GSM. This integrated approach has been a requirement in Europe given that previous projects have shown EGNOS alone cannot meet the integrity requirements (SIL4) for ETCS train signaling [4, 5]. At the heart of any integrated approach is the need to ensure the Reliability, Availability, Maintainability and Safety (RAMS) of designs supported by the ERTMS model and ETCS laboratory studies.

There have been an increasing number of studies that apply RAMS techniques to the railway industry [6, 7, 8]. The key focus of RAMS studies is to look at the interactions that exist between reliability, availability, maintainability and safety. This integrated perspective is particularly important for rail operations when, for example, safety can typically

be assured by halting the trains but only at the cost of availability. Alternatively, pressure to increase availability through reduced maintenance cycles may reduce reliability and also undermine safety. RAMS studies provide infrastructure managers with the metrics to assess the impact of investment decisions over particular periods of time. Models help to determine whether changes in the resources allocated to achieve particular reliability or safety targets will have significant knock-on effects for other operating parameters.

A host of standards and regulatory documents provide the background for the RAMS requirements in rail applications. In Europe, they come under the auspices of CENELEC including, but not limited to the: EN 50126; Railway applications, The specification and demonstration of Reliability, Availability, Maintainability and Safety (September 1999); EN 50128; Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems (March 2001); EN 50129; Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling (February 2003); EN 50159-1; Railway applications - Communications, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems (March 2001); EN 50159-2; Railway applications - Communications, signalling and processing systems - Part 2: Safety-related communication in open transmission systems (March 2001). For instance, EN 50126 defines RAMS in terms of long-term system characteristics as follows:

- **Reliability:** the probability that an item can perform a required function under given conditions for a given time interval.
- **Availability:** the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.
- **Maintainability:** the probability that a given active maintenance action, for an item under given conditions of use, can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.
- **Safety:** the state of technical system freedom from unacceptable risk of harm.

In the United States, ANSI encouraged harmonization through the development of IEC standards that parallel the European CENELEC requirements. Hence, EN50126 has a counter-part IEC 62278 dealing with railway RAMS requirements while the software requirements in EN50128 are mirrored in IEC 622279. In addition to these generic RAMS requirements, there are also specific objectives for both ETCS and PTC projects. For EATS, these requirements were based on the European UNISIG (Union of Signaling Industry) requirements. UNISIG is an industry body, including Alstom, Ansaldo, Bombardier, Invensys, Siemens and Thales, working together to define interoperability requirements so that ETCS applications can be used across member states. The UNISIG[1] Subset 091 states the RAMS requirements for ETCS Levels 1 and 2:

> "Any specific implementation and application will need its own hazard identification and safety analysis process to be undertaken in accordance with the applicable European standards and this process will be supplemented and supported by the generic safety requirements defined herein. The requirements in this document being the minimum to ensure Technical Interoperability".

The Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 are stated in terms of Tolerable Hazard Rates (THRs). The THR refers to the equipment installed on a single train and in the ETCS equipped area visited by the train during a reference journey or mission. UNISIG Subset 091 defines the key objective for the ETCS reference architecture as the ability to provide the Driver with information to allow her/him to drive the train safely and to enforce respect of this information (4.2.1.6). This leads to the top-level or core hazard as: Exceeding the safe speed / distance as advised to ETCS (4.2.1.8). The maximum allowed rate of occurrence for the core hazard is defined by the Railways and approved by National Safety Authorities as:

$$THR(ECTS) = 2.0*10\text{-}9 / hour / train$$

The THR refers to the ETCS reference architecture and deliberately excludes failures due to operators including drivers, signalers and maintenance staff. It also excludes the influence of operational rules. Associated with the Tolerable Hazard Rate is a list of adverse events identified from a functional analysis. The aim is to show that any implementation would mitigate the probability or consequences of these adverse events to ensure that the overall THR is respected. The overall tolerable hazard rate also drives risk apportionment for onboard and

[1] UNISIG/Industry Consortium for ERTMS Specifications, Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, Subset 091, May 2009. http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-091.aspx

trackside equipment as well as the non-trusted transmissions systems used to exchange data between these two sub-systems. Each accounts for one third of the total ETCS THR for the one-hour 'representative' journey.

Fault trees were then developed for level 1 & 2 ETCS to map out the failures that might undermine the THR for any failure to 'provide the driver with information to drive the train safely and to enforce respect of this information'. Each gate in the tree was then included within a Failure Modes and Effects Analysis (FMEA). This enabled the propagation of failures from a base event through the fault tree. This informs more detailed engineering assessments. For instance, the THR(On-Board) is defined to be 33% of the THR(ETCS). One possible set of hazards that might undermine this reliability requirement centers on the use of incorrect data, for instance during configuration or installation of equipment; incorrect data entered by the Driver; incorrect information at the train interface etc. UNISIG Subset 088, part 3 mitigates these hazards by requiring that "The creation of engineering data and its loading into the on-board must achieve a quality level commensurate with a SIL 4 system. This is interpreted as meaning that the process for the obtaining of the raw data through to its loading into ETCS must be analyzed to identify possible threats to the correctness of the data and putting in place actions which minimize the scope for error", similarly "The Data Preparation and Installation Engineering must be considered as a part of the design of a specific ETCS application. Therefore, it will be managed with quality procedures commensurate with the SIL 4 allocation to the technical system". This illustrates the aspirational nature of the UNISIG requirements. IEC EN 61508 rates SIL 4 as equating to a probability of failure per operating hour in continuous operations as between 10-8 and 10-9, from 10-4 to 10-5 for probability of failure to perform a safety function on demand. There are very few SIL 4 systems in commercial operation and certainly this level of reliability is hard to achieve in existing signaling infrastructures/information systems.

Balancing Innovation and Standards in Grail and Grail 2

Previous sections have described how the UNISIG industry body developed detailed interoperability requirements for the next generation of European train control systems, consistent with the requirements in existing CENELEC standards. However, their focus was primarily on supporting the medium term development of the ETCS level 1 cab signaling system based on trackside (balise) radio beacons and level 2 digital radio communications with reduced trackside signaling through the use of Radio Block Centres. In contrast, a number of research projects have considered the RAMS requirements for the longer term development of ETCS level 3, based on dynamic spacing using the GNSS architectures common to PTC projects. In particular, the GRAIL project focused on Galileo Localization for ETCS. GRAIL fused conventional on-board and trackside information sources with GNSS satellite data for enhanced odometry [9].

The RAMS analysis within the GRAIL project was intended to identify and mitigate the hazards associated with the novel integration of GNSS data into existing architectures. Integration raised significant concenrs for any RAMS analysis. Although the introiduction of satellite positioning systems created opportunities for reduced maintenance sosts, through the removal of expensive trackside balisses or Radio Control Block infrastructures, it also raised a host of concerns about reliability, availability and safety. For example, it can be difficult to ensure sufficient, reliability sateillite readings in urban environments where multipath effects occur as signals bounce of built objects before reaching a vehicle. There are particular concerns for satellite signal availability inside stations when the bandwidth limitations of alternate GSM-R infrastructures may compound GNSS concerns.

During the GRAIL RAMS analysis, HAZOPS was used to identify concerns for the use of GNSS daat in ETC applications, as well as particular concerns associated with Train Awakening; Train Integrity and Absolute Positioning. The HAZOPS project team reviewed the requirements specifications for these subsystem functions. The aim of the RAMS assessments for Enhanced Odometry within GRAIL was to:

- Identify hazard and operability considerations that may require the functional requirements to be modified or changed.
- Identify new requirements relating to the resolution of identified hazard and operability issues
- Identify, where appropriate areas for closer scrutiny using other hazard analysis techniques.
- In achieving the above objectives, provide assurance that a reasonable consideration for safety has been made and that suitable provision for safety can eventually be made, based on functional requirements, by a future designer of the system.

The meeting participants were provided with a functional description of the subsystem; any changes to these descriptions were noted and agreed upon prior to the hazard analysis. The key functional components included enhanced odometry function self-test; request status of the user terminal enhanced odometry function by the ETCS; odometry macro-function; provide data at periodic intervals; provide status data; provide standstill data; provide speed data data; provide speed confidence interval data; provide direction data. The GRAIL HAZOPs analysis was also guided by a range of simplifying assumptions, for instance that the ETCS odometry macro-function is that required by the current ETCS SRS and that the User Terminal enhanced odometry function is an additional sub-system. Attributes were identified to clarify aspects of the main functions; these attributes included signals, data, integrity issues, and operational environment and test requirements. The HAZOPs analysis then proceeded in the usual fashion by applying a number of guidewords – such as no; less; more; error; early; late etc. For each combination of guideword and attribute for each function the team tried to identify the cause of an associated hazard/operability deviation; the potential consequences; any existing mitigations including engineering safeguards and controls and other measures to eliminate the occurrence of the hazard or to mitigate the consequences. The team also identified combinations where they felt there was no conceivable hazard. This process led to the compilation of a hazard log that was extended by less structured brainstorming to ensure adequate coverage of potential risks. The HAZOPS study generated a number of action sheets for the relevant project managers. They had to explain the action taken or provide a reason why no action was taken. These action sheets identified control activities that either affected sub-system specifications or the design process or an operational procedure – this last category should be used with care; given the problems of ensuring the consistent implementation across member states. These options are not mutually exclusive.

The Grail 2 project extended the previous focus by taking the enhanced odometry functions investigated in Grail from a proof of concept to the point close to commercial exploitation [10]. The safety requirements identified in the previous project resulted in an assumption that a systematic failure in the enhanced odometry leading to fatal consequences must have a probability of less than 10-8 per hour. However, it was recognised that the GRAIL GNSS User Terminal could not meet such a SIL-4 requirement and it was decided that the novel use of GNSS could not entirely replace conventional sensors; limiting the transition between ETCS levels 2 and 3. Instead, GRAIL 2 developed a revised architecture for sensor fusion in ETCS reaching SIL-2 reliability levels (with a THR between 10-6 and 10-7). In order to do this they developed a dual processor architecture with voting elements and a fail-safe philosophy that incorporated Receiver Autonomous Integrity Monitoring and protection levels to raise alarms when satellite signals might fail to meet accuracy and confidence limits [11]. This created new concerns for RAMS analysis; by increasing safety through the use of a default fail-safe philosophy there can be concerns to ensure the overall availability of ETCS implementations.

RAMS and Safety as a Barrier to Innovation

A functional decomposition scoped the HAZOPS study that drove the GRAIL RAMS analysis; meeting participants were provided with a functional description of the subsystem and any changes were agreed upon prior to the hazard analysis. It was initially decided to adopt a similar approach within the EATS project. Recall that our aim was to build upon the integrated GNSS approach used in GRAIL for ETCS level-3 implementation. The use of a functional decomposition to support the reliability, availability, maintainability and safety assessments has been recommended by similar studies. For example, Patra's has recently studied the interactions between maintenance cost, reliability and safety in rail applications [6]. He argues that

> "A thorough understanding of the technical description of the system is necessary to perform RAMS analysis of the system. In the case of railway infrastructure, there are three different systems, namely the track system, the signaling and communication system, and the power system. These systems have a combined effect on the degradation of the infrastructure. Each system is subjected to degradation due to various internal and external factors. All these aspects need to be considered to estimate the RAMS of the infrastructure, which makes the calculation more complex… To estimate the RAMS figures at the infrastructure level, one must evaluate the RAMS characteristics at the sub-system and component level. In general, the reliability and maintainability parameters are estimated both on the component level and on the system level, whereas the availability and safety parameters are estimated only on the system level. In order to achieve the required performance of the infrastructure, the failure modes should be identified and classified".

Patra's summary helps to identify some of the practical consequences in applying RAMS techniques in exploratory research and development projects, similar to GRAIL and EATS. While it may be possible to perform calculations on the system-level safety of near-term infrastructure changes, for instance based on ETCS

level1 and 2, this is far more difficult in longer-term initiatives. For instance, many questions remain to be answered about the environment in which EATS applications will be running in terms of the track-side architecture. One of the motivations for ETCS level 3 has been to reduce the trackside costs. However, it seems likely to be many years before most rail infrastructure companies would be willing to remove all existing trackside systems, including balises. From this it follows that we may have to repeat the calculations many times based on different environmental assumptions. It is for this reason that the RAMS analysis in GRAIL and GRAIL-2 were intended to be indicative – they illustrate how such an analysis might be performed but many parameters would have to be revised with the detailed characteristics of particular implementations. ETCS level-3 RAMS computations are further complicated in the context of the EATS project because a primary aim was the development of a laboratory that could be used to explore different integration techniques and architectures. This led to a tension between the RAMS objectives based on the functional decomposition necessary to conduct a preliminary hazard analysis and the wider aims of EATS to support multi-disciplinary studies in GNSS-ETCS integration.

In many projects, these issues are addressed by conducting the RAMS analysis at a relatively high-level of abstraction. This was used in the GRAIL project – the HAZOPS looked at an abstract set of functions that could be implemented by across different architectures. However, team members still had to agree on the functional decomposition before the study could begin. For EATS, this was more problematic given the dual aims of supporting laboratory development and the creation of an ETCS Reference Model. The project team included specialists in GNSS applications, in antenna array development, in rail operations. Each brought different skills and perspectives leading to a range of alternate ideas about the functional decomposition and detailed design of the EATS Smart Train Positioning System. A key concern, therefore, was to encourage flexibility and avoid ***premature commitment*** to particular software architectures. This creates tensions – safety managers can become "enemies of innovation" if they oppose modifications that create additional work redoing the hazard analysis [12]. Equally, it can be hard for safety managers to control project costs if alterations to the underlying architecture force continual changes in the safety assessments. For example, small alterations to the high-level design of a critical infrastructure force radical change in the underlying hazard analysis. At the same time, the other team members were continually asking questions about aspects of RAMS through each successive design. The dynamic, multidisciplinary nature of the work created a need for continuous feedback on potential safety concerns as lab and bench studies continue to innovate with novel software architectures and prototype implementations.

These creative tension between multidisciplinary engineering teams and the project safety-group were compounded because many hazard analysis techniques have their roots in the 1960s when issues of scale, modularity and reuse were arguably less of a concern than they are today. One consequence is that there are no existing refinement techniques that might otherwise help to re-use elements of an initial high-level HAZOPS during a more sustained RAMS analysis of a detailed design.

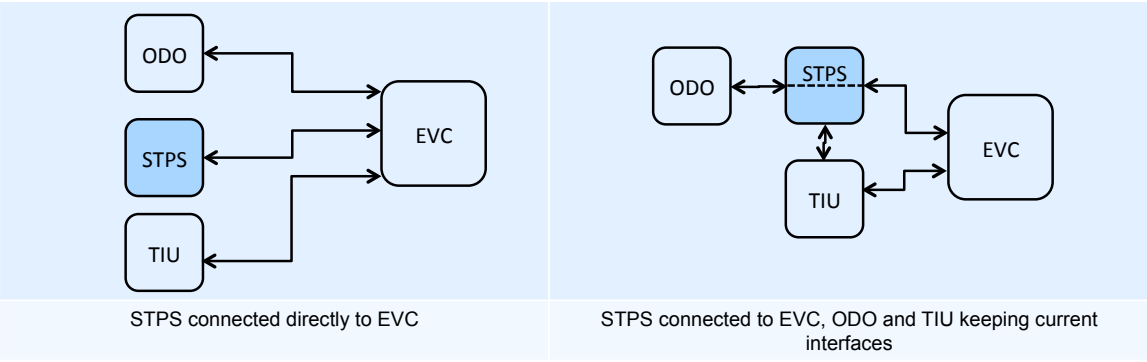

Fig 1. Working Through the High-Level Architecture for the Smart Train Positioning System

Figure 1 provides a specific example of the issues faces during the initial reliability, availability, maintainability and safety analysis of the EATS project. They both illustrate architectures for the integration of the Smart Train Positioning System with the EVC (the European Vital Computer is the at the heart of the on-board data processing), the ODO (this is the odometry function at the heart of the GRAIL and GRAIL-2 projects) and the TIU (the Train Interface Unit controls the train's onboard functions via interfaces with the braking systems, train control and engine control applications and with cab status information). The image on the left illustrates an initial proposal in which the STPS is developed as a separate module from other major components in the ETCS

on-board systems. In terms of any RAMS analysis, this has significant benefits because existing work on the ODO and TIU need not be updated providing it can be shown that there are no side effects created by the interaction between the EVC and the STPS. However, this approach loses many of the benefits that might be obtained from ETCS level 3 implementations. For instance, the EVC might pass ODO data to the STPS as a means of implementing Receiver Autonomous Integrity Monitoring (RAIMS). The odometry information might be compared with GNSS and GSM-R signals to determine potential discrepancies. From a RAMS perspective, this could undermine modularity by creating hidden inter-dependencies between the ODO and the STPS RAIMS – reliability might be affected by the ways in which discrepancies are resolved.

The image on the right of Figure 1 illustrates an alternate proposal addressing further concerns over the initial EATS STPS architecture. In the first proposal on the left, there was an assumption that the ETCS EVC could be extended with an interface to the proposed EATS Smart Train Positioning System. This creates additional complexity because any changes to the EVC involve multi-party agreement and formal adoption into the UNISIG ERTMS baseline. This is a non-trivial process given the millions of euros that have been invested across member states by, for instance, companies that have produced infrastructure components that are compliant with the existing baselines. The alternate proposal on the right of Figure 1 offers the advantage that the STPS can be integrated into the existing ODO interface, with an additional interface to the TIU. This reduces the complexity of synthesizing additional EATS functionality into existing ERTMS on-board components. However, it introduces major new challenges for the RAMS assessment. For instance, in the original proposal the EVC had unchanged access to ODO data; helping to modularize the impact of the STPS integration. Although the revised architecture on the right simplifies the EVC interface it creates a requirement to develop a RAMS analysis for both the STPS and also for the existing ODO functions. For example, we must ensure that any routing of ODO data via the STPS does not invalidate the hard real-time operability constraints for EVC functionality. The interface between the ODO and the STPS creates a range of hazards in which STPS faults delay all position information from reaching the EVC. The meta-level point here is not to analyze the costs and benefits of particular architectures for the STPS but to point out the huge impact that architectural decisions will have upon the RAMS analysis in safety-related infrastructures.

Partial Solutions: Incremental RAMS and the Need to Avoid Premature Commitment

In the early stages of the EATS project, we conducted HAZOPS training sessions with the multi-disciplinary teams to replicate the approach used in the GRAIL project. However, we soon felt that we were trying to impose agreement about the functional decomposition in a manner that ran against the ethos of a project to encourage flexible innovation through the development of an ETCS laboratory and reference model. The following sections present a number of approaches that helped us in this task.

1. *Avoid Premature Commitment.* The purpose of the project was not to deliver a detailed RAMS analysis but to support the delivery of tools that would reduce costs in the later design and certification of ETCS level 3 implementations. We, therefore, had to balance our need, as safety professionals, for design commitment to support RAMS assessments against the flexibility required in the early stages a critical infrastructure development project.

2. *Blend Stakeholder Meetings and Pairwise Focus Groups.* Most preliminary hazard analysis techniques suggest that initial meetings should bring together as many of the various stakeholders as possible. Although this was useful in the initial phases of the project, we could not rely on team meetings to support the exploratory hazard analysis in the EATS project. One reason for this was the difficulty and expense of bringing together multi-party teams of experts working in high-demand areas of engineering. A further problem was that these large team meetings tended to focus on architectural development even though they had been scheduled to support the RAMS analysis – this is not a criticism of the management skills of the RAMS team but a natural consequence of trying to apply techniques like HAZOPS at a premature stage in the development process. We, therefore, supplemented these large group meetings with pair-wise focus groups and workshops where RAMS specialists met with the technical domain experts to focus on the generic hazards that they identified for their area of concern. We recognized that this will provide few insights into the interactions that are a key concern of complex systems, but the intention was to develop the foundations for the RAMS analysis and then consider these more complex failure modes once we had sufficient details about the underlying system architectures.

3. *Identify a Generic Hazard Set.* It is possible to identify a set of hazards that arise for complex systems, irrespective of the detailed functional decomposition that might guide the development of a more detailed design. Many of these are well understood within the different technical domains that contribute to projects such as EATS, and it is critical that these are identified and documented at an early stage in development so that they are not forgotten in more conventional HAZOPS studies where the focus is often more on the interactions between components in novel infrastructures. As a specific example, an initial meeting with the GNSS application group identified hazards associated with the uploading of ephemeris data for the satellite array to be used by on-board systems, further concerns focused on incorrect models being used for atmospheric errors. There were concerns about ionospheric scintillation, about the impact of hardware clock errors etc. The key point is that these generic concerns can be identified at an early stage in development even before there is general consensus on the development architecture or the detailed functional decomposition required by existing hazard analysis techniques. It is also possible to identify interactions between these generic hazards, even at an early stage in design. Figure 2 illustrates a whiteboard attempt to map out some of these interactions during initial meetings between the RAMS team and the GNSS application group.

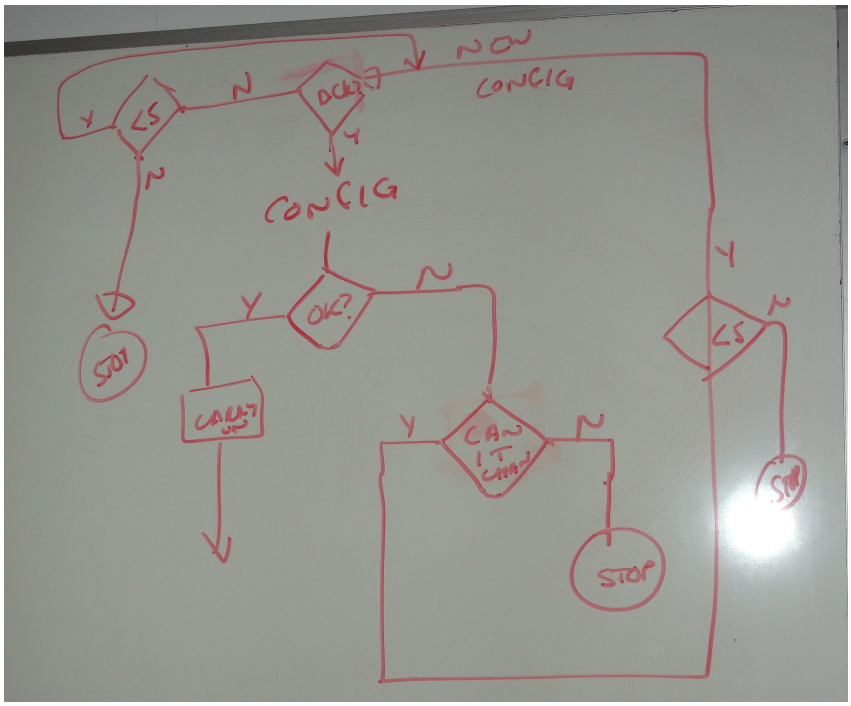

Fig. 2 – Working Through the Functional Relationships in EATS

4. *Achieve Consensus Over Islands of Commitment.* As the development discussions progressed, it became clear that there were significant areas of agreement at key interfaces in the overall systems architecture. For instance, it was possible to identify the functions likely to be needed within the train integrity components before it was possible to identify a similar level of detail in the Smart Train Position System location data fusion. This enable the RAMS team to work on 'islands of commitment' but with the understanding that some of the initial safety work might have to be repeated as a consequence of decisions still to be made at other interfaces within the overall systems architecture. These areas of consensus were identified during the group meetings that built upon the pairwise discussions, mentioned in previous sections.

5. *Using RAMS Assessments for Project Management.* The 'islands of commitment' amenable to RAMS analysis will grow over time as the project develops. Functional decompositions and generic hazard lists can be combined from the pairwise studies during larger multi-party meetings. HAZOPS and other techniques must be used to consider system level interactions. In consequence, the output of RAMS analysis can be used to measure progress towards project deliverables. They provided KPIs to assess the maturity of different areas within the overall EATS architecture.

Previous paragraphs have described an incremental approach to RAMS analysis in complex, innovative infrastructure projects. A number of caveats can be raised – interactions between different functional areas can force RAMS teams to rework an initial analysis. This may be necessary when further development reveals, for instance, that one team cannot meet their initial reliability targets. An alternative to our piecemeal approach would be to conserve RAMS resources until all areas were at a sufficient level of maturity. This approach could not be applied within the ETCS for two reasons. Firstly, the project was time-limited and there is a danger that delays in any one area of the project would have left insufficient resources to complete the final Reliability, Availability, Maintainability and Safety assessments. The second concern is that it becomes harder and harder to address RAMS concerns, the later they are identified in the development process.

Conclusions

There is a growing consensus that we need to ensure 'safety is engineered into a design' from the earliest stages. However, Europe and North America have created a number of revolutionary projects including European Train Control System (ETCS) and Positive Train Control (PTC) in the rail industry but also NextGen and SESAR in aviation. In many of these projects, it is particularly difficult to apply existing Reliability, Availability, Maintenance and Safety (RAMS) analysis techniques that typically require an agreed, stable functional decomposition before any detailed insights can be obtained. These scoping studies are hard to sustain without premature commitment to particular software architectures. For example, small alterations to the high-level design of a critical infrastructure force radical change in the underlying hazard analysis. This creates tensions – safety managers can become "enemies of innovation" if they oppose modifications that create additional work redoing the hazard analysis. Equally, it can be hard for safety managers to control project costs if alterations to the underlying architecture force continual changes in the safety assessments. These tensions are compounded because many hazard analysis techniques have their roots in the 1960s when issues of scale, modularity and reuse were arguably less of a concern than they are today.

Our experience on the EATS project on Advanced Testing and Smart Train Positioning System for the next generation European Train Control System has been used to illustrate these arguments. The EATS project integrates a range of wireless infrastructures with input from Satellite Based Augmentation Systems to reduce reliance on trackside infrastructures and is comparable to the US PTC program. However, the dynamic, multidisciplinary nature of the work has created a need for continuous feedback on potential safety concerns as lab and bench studies continue to innovate with novel software architectures and prototype implementations.

In the early stages of the EATS project, we conducted conventional HAZOPS training sessions with our multi-disciplinary teams. These provided limited benefits and the RAMS sessions began to focus on a broad range of design issues that were only partly related to Reliability, Availability, Maintenance and Safety concerns. The RAMS team were also concerned that we were constraining valuable development discussions. Forcing agreement about the functional decomposition ran against the ethos of a project to encourage flexible innovation through the development of an ETCS laboratory and reference model. In consequence, we were forced to innovate. This paper identified a number of approaches that helped to avoid premature commitment too early in the development cycle of complex, safety-related infrastructure projects.

We, therefore, had to balance our need, as safety professionals, for design commitment to support RAMS assessments against the flexibility required in the early stages a critical infrastructure development project. For instance, in order to make progress in the RAMS analysis during the early stages it was important to balance both project level stakeholder meetings and more focused pairwise discussions with domain experts. One reason for this was the difficulty and expense of bringing together multi-party teams of experts working in high-demand areas of engineering. A further problem was that large team meetings tended to focus on architectural development even though they had been scheduled to support the RAMS. We used the larger project meetings to discuss system-level RAMS issues at a high-level of abstraction. In contrast, the pairwise meetings were used to identify a generic hazard set for the key technical focus areas. Generic hazards arise for complex systems, irrespective of the detailed functional decomposition that might guide the development of a more detailed design. Many of these are well understood within the different technical domains that contribute to projects such as EATS, and it is critical that these are identified and documented at an early stage in development so that they are not forgotten in more conventional HAZOPS studies where the focus is often more on the interactions between components in novel infrastructures.

The RAMS team was concerned that the safety analysis should not be relegated to an afterthought in the development process. We, therefore, began to achieve consensus over 'islands of commitment'; areas of the

design that were stable enough to permit a more formal functional decomposition. By accepting such a piecemeal approach, we understood that some of the initial safety work might have to be repeated as a consequence of decisions still to be made at other interfaces within the overall systems architecture. Over time it was possible to merge the functional decompositions and generic hazard lists during larger stakeholder meetings to drive the more formal HAZOPs.

Acknowledgement

This work was funded as part of the EC EATS project: European Train Control System Advanced Testing and Smart Train Positioning System (FP7-TRANSPORT-314219). Thanks are due to the members of the project team; all errors in the paper remain those of the author. We also acknowledge Profs. Alan Dix, Michael Harrison and Colin Runciman who developed ideas on premature commitment in the design of interactive systems during the early 1990s.

References

1. C.W. Johnson, S. Reinartz and M. Rebentisch, Practical Insights for the Exchange of Lessons Learned in Accident Investigations across European Railways. In D. Swallom (ed.), Proceedings of the 32nd International Systems Safety Society, Louisville, USA 2013, International Systems Safety Society, Unionville, VA, USA, 2014, this volume.
2. S. Arrizabalaga, J. Mendizabal, S. Pinte, J.M. Sánchez, J.M. González, J. Bauer, M. Themistokleous, D. Lowe. Development of an advanced testing System and Smart Train Positioning System for ETCS applications. TRA2014 5th Conference. 14th-17th April. Paris
3. J. del Portillo, I. Adin, J. Mendizabal, D. Valderas, I. Ortego, G. Solas. Enhancing the rolling stock standards towards a harmonized electromagnetic environment. TRA2014 5th Conference. 14th-17th April. Paris
4. LOCOLOC (2004) System Preliminary Safety Case, VERSION 2.1, European Space Agency, Restricted Report, 2008.
5. A. Filip, J. Beugin, J. Marais & H. Mocek, Interpretation of the Galileo safety-of-life service by means of railway RAMS terminology. *Transactions on Transport Sciences* 1.2 (2008).
6. Ambika Prasad Patra, Maintenance Decision Support Models for Railway Infrastructure using RAMS & Low Cost Cycle Analyses, PhD thesis, RAMS, Division of Operation and Maintenance Engineering, Sweden, 2009.
7. Lyngby, Narve, Per Hokstad, and Jørn Vatn. RAMS management of railway tracks. Handbook Of Performability Engineering. Springer London, 2008. 1123-1145.
8. M.G. Park, RAMS management of railway systems, PhD Thesis, University of Birmingham, UK, 2014.
9. M. Thomas, The GRAIL (GNSS Introduction in then Rail Sector) Project, HAZOP for ETCS Applications: Enhanced Odometry, August 2007. GJU/05/2409/CTR/GRAIL.
10. E. Gonzáleza, C. Pradosa, V. Antón and B. Kennes, GRAIL-2: Enhanced Odometry based on GNSS, Transport Research Arena, 48:880-887, 2012.
11. L. Marradi, A. Galimberti, L. Foglia, A. Zin, C. Pecchioni, M. Doronzo, E. J. García-Consuegra and M. Lekchiri, GNSS for Enhanced Odometry: The GRAIL-2 results. 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, (NAVITEC), 2012.
12. C.W. Johnson, Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting, University of Glasgow Press, Glasgow, Scotland, October 2003.

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP,
School of Computing Science, Univ. of Glasgow, Glasgow, G12 8RZ, Scotland, UK.
Tel +44(141)3306053, Fax +44(141)3304913, Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor and Head of Computing Science at the University of Glasgow in Scotland. He leads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety and security-critical domains ranging from healthcare, to the military to aviation and rail.