SYSTEMATIC INTEGRATION OF HUMAN FACTORS IN THE SPECIFICATION OF REQUIREMENTS FOR NEW RAILWAY TECHNOLOGIES

Christian Wullems  
BIT (Hons) PhD GradDip Alnv MIEEE MACS  
CRC for Rail Innovation and CARRS-Q, Queensland University of Technology, Australia

Anjum Naweed  
BPsysch (Hons) MSc PhD MIEHF  
CRC for Rail Innovation and Appleton Institute for Behavioural Science, Central Queensland University, Australia

SUMMARY

Engineering design processes are necessary to attain the requisite standards of integrity for high-assurance safety-related systems. Additionally, human factors design initiatives can provide critical insights that parameterise their development. Unfortunately, the popular perception of human factors as a “forced marriage” between engineering and psychology often provokes views where the ‘human factor’ is perceived as a threat to systems design. Some popular performance-based standards for developing safety-related systems advocate identifying and managing human factors throughout the system lifecycle. However, they also have a tendency to fall short in their guidance on the application of human factors methods and tools, let alone how the outputs generated can be integrated in to various stages of the design process. This case study describes a project that converged engineering with human factors to develop a safety argument for new low-cost railway level crossing technology for system-wide implementation in Australia.

The paper enjoins the perspectives of a software engineer and cognitive psychologist and their involvement in the project over two years of collaborative work to develop a safety argument for low-cost level crossing technology. Safety and reliability requirements were informed by applying human factors analytical tools that supported the evaluation and quantification of human reliability where users interfaced with the technology. The project team was confronted with significant challenges in cross-disciplinary engagement, particularly with the complexities of dealing with incongruences in disciplinary language. They were also encouraged to think ‘outside the box’ as to how users of a system interpreted system states and behaviour. Importantly, some of these states, while considered safe within the boundary of the constituent systems that implemented safety-related functions, could actually lead the users to engage in deviant behaviour. Psychology explained how user compliance could be eroded to levels that effectively undermined levels of risk reduction afforded by systems. Linking the engineering and psychology disciplines intuitively, overall safety performance was improved by introducing technical requirements and making design decisions that minimized the system states and behaviours that led to user deviancy. As a commentary on the utility of transdisciplinary collaboration for technical specification, the processes used to bridge the two disciplines are conceptualised in a graphical model.

1. GENERAL INTRODUCTION

Engineering design processes are critical for attaining the requisite standards of integrity for high-assurance safety-related systems, but human factors-based design initiatives can also provide critical insights to parameterise their development. Unfortunately, the popular perception of the human factors discipline is that of a “forced marriage” for want of a better expression, between the disciplines of engineering and psychology. This perspective of human factors has a tendency to provoke views where the unpredictability of the human element is perceived as a vulnerability or threat to systems design. On balance, the view of the human factor as a limiting agent for systems design is not unfounded, but it is important to note that the ever-increasing complexity of systems drives these patterns, rendering human factors input in engineering design more important than ever before. In recent years, complexity theory has advocated a complex systems view of systems where complexity is gradually becoming the defining characteristic of technology [1, 2]. This theory describes how failures emerge opportunistically from the very systems put in place to prevent them, and explores the notion of normalisation of deviance. This is used to explain how compliance could actually give rise to hazards through deviant behaviours, and erode to a level that effectively reduces the risk reduction afforded by the system. Ironically, the perspective that the human element is a palpable threat to systems
design is ideological and a highly judgemental single-factor explanation for the causes of failure, undermining the sheer dynamism, complexity and opacity in the networking of systems interactions and processes in the technology of today [3]. To some extent, these views are reflected in a number of performance-based standards for developing safety-related systems. Most mention the importance of human factors as a thermometer to gauge human behaviour with respect to systems design, but fall short on the guidance. This will be a recurrent theme throughout this paper, largely because the complexity of systems is rivaled only by the under specification of how they may influence human performance. In practice, this under specification and practice of ‘silo thinking’ can create a lot of problems for human reliability in systems design.

One way to get over these issues is to recognise that the collaborative dynamic in systems design is inherently interconnected, and any disconnects in the design of system states and human factors impacts the facilitation in the process, and the integrity or usability of the system [4]. Generally speaking, facilitation literature lists a number of approaches that look beyond single disciplines to cross boundaries, ostensible or otherwise (e.g. multi-; cross-; trans-; inter-disciplinary) [5]. Integrating human factors systematically into systems design may transcend the boundaries of conventional disciplines and engender a greater understanding of different perspectives and interweave knowledge to anticipate problems and create solutions [5-7], building even more integrity for high-assurance safety-related systems.

1.1. Aims and Objectives

In this paper, we describe the case study of a project that converged engineering with human factors to develop a safety argument for new low-cost railway level crossing technology for system-wide implementation in Australia. The aim of this paper is to illustrate the importance of systematic integration of human factors in the specification of requirements for new level crossing technologies in the Australian rail context. The objectives that were used to meet this aim are as follows:

- Provide a tangible example of a rail research project where reciprocity in the engineering and human factors processes converged to strengthen and endorse the safety argument,
- Discuss the effect of human factors on safety in relation to level crossing warning device failure modes,
- Illustrate personal accounts of how trans-disciplinary learning and collaboration took root in the project team (i.e. the authors), who were originally educated very traditionally in the engineering and psychology disciplines, and
- Conceptualise the processes through which knowledge was shared.

2. HUMAN FACTOR “MATTERS”

Although the science of human factors has now become recognised as a discipline in its own right, imbued with the capabilities to expound causation for some of the more euphemistic classifications of failure (e.g. “Controlled Flight into Terrain”), its tension with systems engineering can still be observed in some popular performance-based standards for developing safety-related systems. While these advocate the identification and management of human factors considerations throughout the system lifecycle, they also have a tendency to fall short in their guidance of how human factors methods and tools should be applied, let alone how the outputs generated can be integrated into various stages of the design process.

For example, the CENELEC standard EN50126-1 Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) [8] states:

“Humans shall be considered as possessing the ability to contribute to the RAMS of a railway system. To achieve this aim, the manner in which human factors can influence railway RAMS should be identified and managed throughout the entire lifecycle. The analysis should include the potential impact of human factors of railway RAMS within the design and development phases of the system.” (pp. 16)

This excerpt highlights the requirements for human factors as an important part of the entire lifecycle, but the standard falls short in providing guidance and/or tools to point the reader to further literature. As a result, engineers or designers aiming to meet these requirements will interpret this as they see fit, breeding inconsistencies, nuances, and assumptions to create yet further disconnects [9].

In determining appropriate safety requirements for systems such as a level crossing warning device (i.e. a hazard control for system hazard: collision between road and rail vehicle), a risk analysis is conducted to identify the hazards at the hazard control’s boundary. Appropriate tolerable hazard rates (THR) are then allocated to these hazards. THR at this level should ensure that the hazard control is effective in reducing risk to a tolerable level for system hazards (i.e. residual risk meets THR defined for system hazard: collision between road and rail vehicle).

System designers and developers use THR to determine appropriate levels of safety integrity,
failure rates, etc., through an apportionment process, for constituent systems that implement functions defined in the safety requirements of the hazard control.

At this level, the challenge is to allocate THR{s that take into consideration human performance at all interfaces to the system, ensuring the hazard control reduces risk to a level that meets THR{s for system hazards. This is particularly pertinent for degraded modes of operation, where changes to function allocation during failures and degraded modes of operation can result in additional hazards.

For example, if the system is no longer able to perform safety-related functions due to a failure, functions that were otherwise entirely provided by the system are now entirely or partially allocated to humans (often unexpectedly for users of level crossings). Human reliability can significantly influence effectiveness of the hazard control, especially in cases where humans are part of detection and mitigation functions of some failure conditions. Human reliability in this context can affect the persistence of such failures and therefore exposure to a potentially dangerous condition for users of the level crossing.

Further complicating matters, intermittent or prolonged exposure of system users to degraded modes of operation can also affect the user's performance and response to the system, both short-term and long-term. Degradation of human performance gives rise to additional hazards, therefore requiring targets or upper bounds to the frequency with which degraded modes of operation occur.

In determining appropriate THR{s and reliability targets, tools facilitating the quantification of human reliability are necessary, allowing human performance considerations to be integrated into quantitative risk assessment. It is this intimate inter-working of both engineering and psychology disciplines that are needed to achieve the design of systems optimised for human performance.

Researchers advocate collaborative work between different disciplines as a way of overcoming these sorts of issues whilst energising the process of systems design and cultivating insight through mutual endeavour (e.g. reliability testing). This has the effect of not only finding common ground, but also weaving knowledge and methods in ways that transcend conventional boundaries. The next section will outline the scene and background of the case study.

3. DEVELOPING A SAFETY ARGUMENT FOR LOW COST LEVEL CROSSINGS

The Cooperative Research Centre for Rail Innovation (Rail CRC), an Australian government research initiative, has funded several projects aiming to develop and trial a safety argument for adopting low-cost level crossing warning devices (LCLCWDs) in Australia. These devices are intended for deployment at low-exposure sites with passive controls (i.e. single track, low road and rail traffic volumes). Figure 1 illustrates an example of such a site.

![Figure 1 – Example of a low-exposure level crossing with passive controls.](image)

The LCLCWD project is comprised of engineers and cognitive psychologists (amongst other team members). This mix of expertise cultivated ‘out-of-the-box’ thinking in the way the safety argument was developed, not just from a systems view, but also from the perspective of policy and practice. Although both perspectives agreed fundamentally on the need for a risk-based system-wide approach to upgrade low-exposure level crossings, the manner in which they approached it was very own-discipline oriented. This was reflected in the existence of a scoping project that sought to develop an interventions framework for level crossing upgrades [10]. At the same time, the Rail CRC developed a proposal for LCLCWDs. The reduced cost would allow railways to update a greater number of level crossings across the network, and in doing so, provide an earlier and much larger safety benefit compared with an incremental upgrade based on existing type-approved technology. This was the point at which both projects collided and cross-disciplinary collaboration commenced (between the authors). In essence, the larger more technically robust project with pragmatic applications absorbed the principles of the higher-level and people-centred scoping project.

3.1. Low Cost Level Crossing Warning Devices

The design of LCLCWDs is characterised by the use of innovative technologies aimed at significantly reducing lifecycle costs [11, 12]. An example of costs of level crossings that can be reduced through the application of innovative approaches and technologies include:
• Installation and civil works such as trenching, cable runs, under road/under track bores and track improvement work (e.g. ballast cleaning, head bonding, etc.),
• Provision of mains power,
• Re-commissioning of seasonal lines, and
• Preventative and corrective maintenance.

A significant component of the cost of conventional level crossing warning devices is associated with the required levels of safety integrity. Thus, the higher the level of integrity, the more demanding the development processes, which are reflected in relative development costs. For example, wireless technology and solar power may reduce the costs associated with trenching, under-road bores and provision of mains power, particularly as these activities comprise as much as 50% of the total cost of a level crossing installation. However, this can result in increased system complexity due to the need to power each component independently with solar power, increasing the cost of meeting the warning safety function’s tolerable hazard rate. Inevitably there is also a trade-off between safety integrity and reliability in achieving safety targets. Safe failure modes as a result of reliability issues are anecdotally known to lead to additional hazards, however determining appropriate and acceptable levels of reliability to avoid giving rise to these additional hazards is a key issue that need to be addressed.

3.2. Approaching Levels of Safety Integrity and Risk

Many railways require that all signalling technology be developed to the highest level of safety integrity (i.e. SIL4). However in most cases, this is as a result of the lack of a safety argument supporting lower levels of integrity for low-exposure level crossings. The Rail CRC project is partway through the development of an argument to support a risk-based approach for the adoption of low-cost level crossings, such that the level of safety integrity required for the safety function: warn level crossing user of approaching train, would need to be at least commensurate to magnitude of risk reduction required to meet the tolerable hazard rate (THR) for the system-hazard: collision between road and rail vehicle.

As such, for level crossings with lower risk (e.g. lower-exposure level crossing with passive controls), the magnitude of risk reduction required to meet the respective THR would be less than that required for a level crossing with higher risk (e.g. high exposure urban crossing). In order to support the argument, a comprehensive safety justification was developed and was comprised of the following elements:

• System definition,
• An assessment of baseline risk and the risk from LCLCWDs,
• Risk acceptance criteria (definition of tolerability of risk and tolerable hazard rates),
• A cost benefit analysis, and
• An assessment of legal duty (reduction of risk so far as is reasonably practicable), and whether the acceptance criteria were met.

One of the challenges in developing a safety argument for new technologies was the definition of quantitative safety targets (THRs) for hazards of the system that would result in dangerous failure and therefore loss of the safety function. In the case of LCLCWDs, these would be hazards of the warning system that would result in loss of the train approach warning (wrong-side failure), such that no warning or inadequate or discontinuous warning would be provided to road users. The tolerable hazard rate (THR) for the warning function of a LCLCWD was informed by evaluating the baseline level crossing risk, the expected risk reduction as a result of installing active protection, and the additional risk contributed from a LCLCWD as a result of having a lower level of safety integrity for the warning function (see Figure 2).

![Figure 2 – Risk model to determine magnitude of risk reduction for LCLCWDs](image_url)

Specifying requirements for railway technologies, including the quantitative safety targets (THRs), allows suppliers to apportion these to constituent subsystems that implement the safety function (e.g. control system, train or track occupancy detection, etc.). As stated earlier, although standards for application of RAMS in railway applications [11, 12] prescribe the consideration of human factors throughout the safety lifecycle, there is little to no actual guidance on how to
practically integrate human factors analysis in the specification of quantitative targets that are needed by engineers to implement such systems. In many cases, system design, behaviour and failure modes can influence human performance at the interfaces between humans and the safety system.

The specification of technical requirements often tends to focus on hazards within the system boundaries, giving little to no consideration to design and behaviours of the system can lead users to become over-reliant, disregard or mistrust the system, potentially resulting in other hazards or a degraded level of performance that affects the overall magnitude of risk reduction that had been estimated for installation of the safety technology. If these aspects of the human-system interface are not adequately considered, residual risk estimates may in fact underestimate risk, and potentially not meet tolerable hazard rates for system hazards. Thus, there is a general need to understand how system failure modes and behaviour can influence human performance or even give rise to other hazards that can affect the safety of the overall system – ergo, human factors. The next section examines two top-level hazards identified in the preliminary safety argument for LCLCWDs and discusses the challenges that were faced in specifying tolerable hazard rates from a holistic assessment of risk including both technical and human factors performance.

4. ASSESSING RISK OF LCLCWDs

The assessment of risk conducted in the preliminary safety argument identified two top-level hazards for LCLCWDs:

- Hazard 1: Level crossing warning device does not provide adequate warning to road users of a rail vehicle while approaching or traversing the level crossing; and
- Hazard 2: Level crossing warning device leads road users to engage in risk-taking behaviour.

One of the key elements of the risk assessment process is to link hazards to fatalities. In this case, it was relatively straightforward for Hazard 1, where a risk model was developed to estimate the likelihood of a failure of the warning function (i.e. wrong-side failure) resulting in a fatality. Using level crossing survey data of road and rail vehicle volumes and an estimate of fatalities per collision from historical crash data, the hazard rate was linked to fatalities, albeit with some underlying assumptions based around persistence of failure.

In the preliminary modelling, the assumption was that failure of the warning function would be detected and reported to the train controller, therefore limiting the exposure of the failure to the traversal of a single rail vehicle. This may well be the case for some railways, however, the performance of the humans that would be fundamentally involved in the process of detecting and reporting the failure was not considered. Detection of failure is further complicated by the myriad of monitoring systems and procedures used in different jurisdictions.

For example, if no remote monitoring function is provided, detection of the failure becomes the responsibility of the train or maintenance crew. Healthy state indications or sidelights can indicate to the train driver whether the warning system is operating correctly. In this case, persistence of the failure is related to the reliability of the train driver detecting and reporting the failure, a probability that potentially diminishes for each subsequent train driver failing to detect and/or report the failure. This is supported by ergonomics profiles of the ways of working of train drivers, and analyses of the environmental events, disturbances and errors are observed, detected and diagnosed when managing the environment during train driving [13].

Alternatively, if a remote monitoring capability is provided, it is assumed that only a proportion of failures (e.g. discontinuous or late warning) will be detected by the monitoring system. Failures that compromise the safety function and that fall within the diagnostic coverage of the warning system should result in the system entering a more restrictive “safe” failure state. Undetected failure of the level crossing could be detected by correlating actual train movements with expected train movements. As the persistence of failure determines the exposure of the risk to road users, the model is sensitive to this assumption and therefore requires sensitivity analysis across the different monitoring technologies and procedures used in various jurisdictions.

4.1. Level Crossings and Error Producing Conditions

Level crossings are fundamentally complex and dynamic socio-technical systems, where degraded modes of operation involve numerous procedures. Based on draft Australian rules and procedures (ANRP), the following is an example scenario illustrating the complexity and impact of human reliability of a series of procedures on the level of exposure to road users of the failure.

- The level crossing failure is detected either via remote monitoring or reports of failure from the train crew. Network control officers must become aware of the failure, for example via a human-machine...
interface communications from train crew of the level crossing failure.

- Network control officers must warn rail traffic crews if a level crossing with active controls is faulty or potentially faulty. This is likely to happen using radio communications.
- Rail traffic crews are required to approach faulty level crossing at a speed allowing them to stop short of the level crossing.
- The rail vehicle can only proceed if safe to do so.

Error producing conditions can severely impact the performance of humans performing tasks of the above procedures. An example of error producing conditions includes:

- Alarm flooding in the control room, where network officers are inundated with multiple failure warnings. For example, environmental influences such as lightning strikes may cause multiple equipment failures contemporaneously. False alarms can also contribute to network control officers disregarding legitimate warnings.
- The train could be a significant distance from the faulty level crossing requiring the use of the driver’s long-term memory. The train driver could simply forget to approach the faulty level crossing at a speed allowing them to stop.
- Verbal communication used to communicate complex information, where there can be reliability issues in miscommunication of information such as level crossing locations.

In order to quantify the reliability of these procedures for use in the sensitivity analysis, the Railway Action Reliability Assessment tool \([8, 14-16]\) will be used. Although in its infancy, this tool that has been developed for the rail industry for the quantification of human error, allowing it to be considered as part of a larger risk assessment. The process involves performing a task analysis of the relevant procedures, selection of the generic task type from the tool, identification, selection and review of error producing conditions (EPCs) including estimation of the EPC’s effect on the task and finally calculation of the human error probability using the formulas’ effect on the task and finally calculation of the human error probability using the formulas’ effect on the task and finally calculation of the human error probability using the formulas’ effect on the task and finally calculation of the human error probability using the formulas’ effect on the task and finally calculation of the human error probability using the formulas’ effect on the task and finally calculation of the human error probability using the formulas’ effect on the task and finally calculation of the human error probability using the formulas’ effect on the task.

Assessing risk for Hazard 2 is significantly more complicated to quantify than Hazard 1, as the performance range of road users (general public) is invariably large. Thus, there are several factors regarding the design of the road interface of level crossings that need to be taken into consideration when evaluating this hazard. Right-side failures have been identified as a major contributor to Hazard 1, but unlike the type of failure discussed in Hazard 1 (where risk is associated with the train approaching with no or insufficient warning), this failure type is detected by the warning system and results in the system entering a fail-safe state. From a technical “within system boundary” perspective, the fail-safe state is a more restrictive state that, in theory, prevents road traffic from entering the rail corridor. However, this is complicated rather spectacularly by the interface with humans, where design of the system can potentially lead humans to engage in extreme risk taking behaviour (figure 3).

**Figure 3 – Not all safe failure states outside warning device system boundary are safe**
In Australia, the RX5 flashing light assembly [17], consisting of a pair of alternatively flashing red lights, indicates the approach of a train and signals to road users that they must not traverse the crossing. This is also the same indication for the “safe” failure state. A key issue with the design is that road users are not able to differentiate the train approach warning from the failure mode, leading to mode confusion.

According to the Queensland Road code (pp. 66) [18]:

“A driver must not enter a level crossing if—

(a) Warning lights (for example, twin red lights or rotating red lights) are operating or warning bells are ringing; or

(b) A gate, boom or barrier at the crossing is closed or is opening or closing; or

(c) …

Maximum penalty – 20 penalty units.”

However, it is not reasonable to assume level crossing users will wait indefinitely. A regular user of a failed level crossing may encounter the same level crossing several times in succession for prolonged failure or on occasion for intermittent failure. Frequent exposure to failure can condition level crossing users to lose confidence in warning, potentially affecting their performance at other level crossings. Error producing conditions such as expectations of when trains run (known schedules) can engender a mismatch between actual and perceived risk in the mental model of level crossing users, for when a warning is credible. Currently, all Australian level crossings must have a road user interface that complies with the standard AS1742.7 [18]. These issues therefore need to be taken into consideration for all level crossings, whether new LCLCWDs or existing technology.

4.2. Quantifying Reliability Targets

Given that failures which result in a so-called “safe state” can also give rise to hazards leading to the system-hazard: collision between road and rail vehicle, system reliability becomes an important albeit indirect safety-related consideration. Safety requirements therefore need to include appropriate reliability targets in addition to safety integrity targets, however quantification of these targets remains an issue if we cannot establish a link between “system leading road user to engage in risk-taking behaviour” and fatalities. However, this hazard had not been quantified in the preliminary safety argument, as there was no quantitative evidence available linking the hazard to fatalities. While there is anecdotal evidence on this relationship, quantifying it will require further research in providing a suitable base of evidence.

The approach being investigated involves using a failure mode effect and criticality analysis (FMECA) of the system to identify failure modes that revert the system to a “safe” failure state. Existing literature and simulation research are possible sources of data that can be used to inform the development of a model for road user reliability, taking into consideration the degradation in performance (loss of confidence in warning) from exposure to the failure and possible recovery in performance following restoration of the system. The model would need to consider the probability of the road user traversing the level crossing when the warning device is in a right-side failure state, the probability of the road vehicle colliding with a train taking into consideration environmental factors and sighting conditions at the crossing, and error producing conditions that affect the reliability of the perception of the warning and decision-making process (i.e. traversal when safe, looking for trains before crossing).

In our experience of developing this argument to

![Figure 4 – Graphical model illustrating the dynamic between the software engineering and cognitive psychology disciplines experienced in the case study.](image-url)
date, a robust understanding of human behaviour and psychology is fundamental for informing quantitative models. There is a clear need to bring together both disciplines to facilitate the specification and design of systems optimised for humans, rather than requiring humans to make procedures to deal with complex and misleading system states.

5. Conceptualising Collaboration in the Case Study

To reiterate an important point made at the start of this paper, the LCLCWD project was comprised of software engineers and cognitive psychologists (amongst other team members). These collaborative dynamics can be (1) multidisciplinary, (2) cross-disciplinary, (3) transdisciplinary, or (4) interdisciplinary. The latter is the apogee of collaboration, and involves combining two or more disciplines, fields of study, or professions, much like the discipline of human factors has with engineering and the study of human behaviour. Achieving this type of collaboration in systems design is difficult, particularly as the engineers or designers that would be following performance-based standards for the development or specification of safety-related systems are unlikely to have a human factors practitioner on their team. Additionally, not all projects would have the critical mass of expertise that would be required to foster these engagements. Thus, for the purpose of this case study and the audience at CORE 2014, we have conceptualised the collaboration in a simple graphical model, tailored specifically to the work that was conducted in the project.

Figure 4 provides a clear indication of the two disciplines using the foundations of transdisciplinarity [6]. The view of opposing and conflicting principles between engineering and psychology were originally apparent, but through the process of continued cross-disciplinary work and sharing of ideas, these views evolved and fundamentally transcended knowledge. In this way, the lack of specification in the standards was compensated with the guidance and initiatives that came out of the dynamic. Reading the graphical model from bottom to top, it refers to what is known (i.e. existing knowledge), what people are capable of (i.e. their capabilities), what they want to do (i.e. desired action), and lastly, how it is achieved (i.e. underlying motivation). The graph illustrates that coordination of a higher-level aim is needed to share knowledge and collaborate effectively, but more often than not an exchange of knowledge starts at an empirical level (at the bottom) and must travel from pragmatic and normative layers to the value level at the top. At the outset, key individuals in what became the project team rarely looked beyond their own knowledge and capabilities, and viewed the subject in in highly discipline-oriented terms. The continual sharing of knowledge and perspectives eventually converged with an understanding and appreciation of the underlying motivators – i.e. the values and philosophies upon which each discipline was based. Strikingly, these shared more similarities than they did differences.

6. CONCLUSION

This paper has described a case study for the development of a safety argument for new low-cost level crossing warning devices through an integrated approach to engineering and human factors. The authors’ have described the collaborative dynamic that emerged as a result of the project’s requirement to understand how human performance affected the safety of the larger socio-technical level crossing system, and how the technology could potentially influence human performance as a result of intermittent or prolonged exposure to failure modes that are deemed safe within the warning device’s system boundary, but potentially give rise to other hazards when considered in the larger socio-technical context.

The paper discussed the need to have an integrated approach to the specification of safety requirements, allowing human performance considerations to be integrated into quantitative risk assessment.

The paper concluded with a discussion on the conceptualization of the collaboration dynamic between the disciplines of engineering and psychology that has been and continues to be used to facilitate this on-going work.

REFERENCES


