Practical Early-Lifecycle Application of Human Factors Assessment

Simon Connelly, Andrew Hussey, Holger Becht
Ansaldo STS Australia
11 Viola Place, Eagle Farm 4009, QLD
simon.connelly@ansaldo-sts.com.au
andrew.hussey@ansaldo-sts.com.au
holger.becht@ansaldo-sts.com.au

Abstract

Human Reliability Analysis (HRA) is often seen as a time consuming task, which requires significant expertise. This may lead to a reduced focus on the human in the loop, and a failure to consider both where human error and recovery may impact on system safety performance.

Through the use of a case study involving a Positive Train Control (PTC) driver interface, this paper aims to examine whether early system architecture phase task analysis can produce meaningful results with little time overhead or human factors expertise. The approach which has been used was to conduct a task analysis on a system sequence diagram, identifying the high order goals and the individual driver tasks, including alternate paths. Once this task analysis was completed, a tailored FMECA was conducted to identify human failure modes which may lead to system hazards and to thereby limit the scope of the subsequent HRA. The criticality analysis was performed via a HEART analysis to estimate error likelihoods, and which also identified risk factors in the HMI design and operating environment.

The outcomes of the case study were design requirements on the resulting driver interface, in addition to operating procedures, and training requirements. It is argued that the approach presented allows for an analysis to be conducted early in a system design lifecycle at low cost and with limited expertise, which adds to the overall safety argument for the end product.

Keywords: Human Reliability Analysis, HEART, Human Factors

1 Introduction

This paper provides a method for analysing and assessing safety-related human-machine interfaces. The method provided extends on the existing methods currently used for such assessment. Four key contributions and advances over current learning within the domain of analysis and assessment of safety-related human-machine interfaces are argued. These contributions/advances are summarised as follows:

1. Analysis is conducted early in the development lifecycle, before significant effort has been expended on developing the HMI, so that the development work can be guided from the outset by the analysis;
2. The method requires minimal human-factors expertise and can be performed by engineers with minimal (re)training. This is not to say that later more detailed expert analyses would not be conducted, but such small-footprint analysis means that it can be done as part of the normal safety engineering process and before time has been expended developing options that later may turn out to be unsuitable in terms of overall risk;
3. The method utilises and combines well understood safety-analysis techniques with HMI-analysis methods, meaning that safety engineers are extending and building on their existing knowledge; and
4. The method uses a quantified analysis to make comparative assessments of risk, to guide overall development direction. The intent is not to make a formal/precise assessment of quantified error likelihood, but to enable different design options to be compared within a broad risk framework.

The remainder of the paper is structured as follows:

1. Section 2.1 provides an overview of the literature concerned with HMI analysis techniques applied in the paper.
2. Section 2.2 discusses methods for assessing the risk of human error.
3. Section 3 discusses the analysis method used in this paper, which combines elements of both existing HMI-analysis techniques, as well as commonly used safety-engineering methods.
4. Section 4 gives an overview of the Case Study used in the paper, as well as the significant outcomes of the analysis, in terms of the specific HMI under analysis.
5. Section 5 summarises and concludes the paper, linking the contributions/advances listed above with the method and outcomes discussed in Sections 3 and 4.

2 Literature Survey

2.1 Analysing Operator Error

Operators are an integral part of any interactive system, working with safety-critical machines via operator

interfaces to achieve task goals. The safety argument for an interactive system should provide confidence that hazardous operator error rates have been minimised by analysis of operator characteristics (e.g., skill level and training) and the characteristics of the workplace of which the operator is a part (e.g., noise levels, lighting and the task itself).

Hussey & Atchison [Hussey00] presents a generic method for operator safety case preparation. Per Hussey & Atchison, there are four key steps to analysing hazards arising from operator error:

1. Task analysis;
2. Human error analysis;
3. Error reduction measures; and
4. Residual risk quantification.

2.1.1 Task Analysis

Tasks are goal-directed activities to transform some given initial state into a goal state. A task can be decomposed into sub-tasks unless the task is itself composed only of elementary actions.

"Knowledge Analysis of Tasks" (KAT) [Johnson 92] is a form of Cognitive Task Analysis (CTA) and divides a task analysis into four main parts:

1. goals;
2. task procedures;
3. actions and objects; and
4. summary.

CTA and similar techniques are well established, e.g., Carroll and Rosson have used scenarios as design representations [Carroll90].

Task models enable identification of requirements and analysis of designs for new requirements and user training needs [Johnson90]. Task models examine the knowledge or competence required to operate a system [Hoppe90].

For the purpose of safety-critical systems, the task analysis may describe procedures for normal operation of the system, maintenance procedures and also procedures for emergency situations [Redmill97]. The description of procedures for normal operation and maintenance should include any recovery steps by which errors of the user are detected and corrected to avoid an accident [Kirwan92]. Task Analysis may be conducted within the context of an overall Cognitive Work Analysis (CWA) [Vicente99]. The CWA informs the task analysis process and provides a functional model of the workplace within which tasks will be performed.

In this paper, to maintain the simplicity of the method that is presented, only the basic task analysis techniques, such as KAT, are considered. More advanced workplace models could be constructed to further inform both the task and human error analysis. However the extension of the methods in this paper to consider such workplace models is outside the scope of this paper.

2.1.2 Human Error Analysis

HAZOP Studies (e.g., [Std00-58]) and FMEA (e.g., [StdIEC-1025]) are the predominant techniques for analysing human error based on a task analysis as the model of the system. HAZOP Studies have been used by e.g., [Chudleigh93], [Kirwan94] and [Leathley97]). Because it is possible to categorise human error types and mechanisms, FMEA is the basis of many current methods for human error analysis including HEART (Human Error Assessment and Reduction Technique) [Williams86] and THERP (Technique for Human Error Rate Prediction) [Swain83]. THERP has been further developed and specialized for the nuclear plant industry via the SPAR-H method [Byers00].

HEART and THERP are both "first-generation" HRA methods. First generation techniques use a simple pattern-matching of the error situation with related error identification and quantification whereas second generation techniques are more theory based in their assessment and quantification of errors. One of the more widely used second-generation techniques is CREAM [Hollnagel98]. CREAM uses performance criteria (both positive and negative) in combination with a model of cognitive demand to determine overall error probabilities.

Only unintentional errors are considered in this paper. Categories of error include omissions, substitutions and repetitions (the latter two are commission errors) [Senders91]. Example error categories documented by Redmill [Redmill97] include: Action or check made too early or too late; Right action or check on wrong object; Wrong information obtained.

Reason and Embrey [Reason86] and Whalley [Whalley88] have summarised the common causes of human error:

- Failure to consider special circumstances;
- Short cut invoked;
- Stereotype takeover;
- Need for information not prompted;
- Misinterpretation of display;
- Assumption by operator;
- Forget isolated act;
- Mistake among alternatives;
- Place losing error;
- Other slip of memory;
- Motor variability; and
- Topographic or spatial orientation inadequate.

Norman's [Norman90a] model of human-machine interaction is referred to as the "execution-valuation" model (also refined by Rasmussen [Rasmussen83] in his "step-ladder" model of decision making from automatic activation and execution through to conscious interpretation and evaluation). Norman categorises errors into two types; slips and mistakes. The same distinction has also been made by Reason [Reason90]. Slips are concerned with automatic behaviour at the physical execution level. Mistakes are the result of conscious deliberation; a "wrong" procedure is formulated. Errors arise when decision makers take short-cuts in the decision process, e.g., using rule-based routines when knowledge-based decision is demanded by the novelty of a situation [Reason86]

2.1.3 Error reduction

The strategies to address operator errors have been summarised by Kirwan [Kirwan90]:

1. Prevention by hardware or software changes: automation of tasks and use of interlock devices and behavioural "forcing functions" to prevent error. Norman [Norman90a] calls features that prevent slips or mistakes "forcing functions" because they force a user to choose a safe sequence of actions. Whilst automation of functions is necessary for tasks that exceed an operator's physical capabilities [Mill92], the automation must not leave residual tasks that are outside the operator's capacity (e.g. during emergency situations) [Bainbridge87].
2. Enhanced error recovery: provide feedback, checking procedures, supervision and automatic monitoring of performance.
3. Reduce errors at source: improve procedures, training and interface design.

2.2 Risk Assessment

2.2.1 Qualitative Assessment

Error Producing Conditions (EPCs) are associated with characteristics of the operator interface, the individual, human cognition generally and the organisation [Rasmussen82]. Redmill [Redmill97] has produced a categorised list of EPCs including: Task demands and characteristics; Instructions and procedures; Environment; Displays and controls; Stresses; Individual capabilities; Social and cultural influences.

2.2.2 Quantitative Assessment

Human reliability quantification techniques aim to quantify the Human Error Probability (HEP) which is defined as: number of errors per number of opportunities for error. EPCs similar to those given by Redmill [Redmill97] appear as a factor in most of the available estimation methods, e.g., HEART, THERP [Kirwan90].

HEART uses a combination of generic task categories, coupled with nominal human unreliability assessments (HRAs) (as performance ranges), as well as EPCs that are used to refine those nominal HRAs to generate an assessed nominal likelihood of failure or Human Error Probability. HEART requires that the assessor judge the effect of each EPC (in terms of assessed proportion of possible effect, APE, between 0 and 1).

More recently, the Rail Safety and Standards Board (RSSB) issued a rail-specific HRA method based on HEART, which incorporated a rail-specific taxonomy of human error [RSSB04]. The RSSB-HRA method is oriented however toward existing rail technologies, whereas the example case study application considered in this paper is novel in its approach to railway operations. For this reason, we chose to use HEART rather than RSSB-HRA for our case study.

Truly accurate methods for predicting human error rates are yet to emerge. While databases of error likelihoods are relatively straightforward to apply, they can only give rough estimates of the likely error rate for any particular circumstance. Expert judgment may take account of particular circumstances better, but is likely to exhibit significant variation, and the effort required to apply methods involving expert judgment is likely to be much greater.

3 Methodology

3.1 Analysis Process

The analysis takes as an input the functional requirements and an understanding of the HMI design (an early prototype or design proposal is sufficient). User Goals are identified based on the functional requirements. A separate set of goals should be generated for each user group and system function.

For each goal we identify the tasks to be completed to achieve the goal, including alternate paths based on choice points (e.g. confirm correct vs. reject incorrect input) – a system architecture specification is generally useful for this step, however it isn't necessarily required, merely an understanding of the interaction sequences between the system and the user which are required to achieve the goal.

Once the task analysis is complete for all goals, conduct a modified FMECA on the output, analysing each step as a separate "component". Guidewords or SME advice may be used to determine the valid failure modes for each task step. To enable this analysis the "standard" FMECA process has been tailored as shown in Table 1. The event tree for the task analysis can be represented directly in the FMECA table to enable the task analysis and safety analysis to be combined.

3.2 Intent

The method discussed in this paper provides four key advantages over existing approaches to HMI-analysis of safety-related systems. The advantages are discussed in the following subsections.

3.2.1 Early lifecycle analysis

The method used in this paper enables engineers to conduct an early lifecycle analysis with reduced need for expert HF input, and provide early design advice on the suitability of a proposed HMI design. By conducting such analyses early in the product lifecycle it is possible to achieve customer / end-user buy-in of safety related interface designs, and also to determine where specific workflows may need to be enforced to achieve system level safety requirements.

Identification of critical tasks may also enable efficiencies to be designed into the workflows with limited impact on safety performance.

3.2.2 Minimal human-factors expertise

As the conduct of FMECAs is well understood within the RAMS and Engineering communities, it is envisaged that a broad range of resources could apply this approach, without the need for detailed HF knowledge.

It is important to note that this isn't a full HEART analysis as such a full analysis would require much more time than is intended here, and significant support from skilled HF resources.

Column Title	Description
ID	Row identifier
Goal	Top level goal identified from analysis of functional requirements
Main Task	Step in the main task sequence
Alternate Path(s)	Possible alternate sequence steps broken off at each choice point. Can rejoin at the next main step or reference an earlier or later main sequence step
Failure mode(s)	Possible failure mode for this task, where a task has more than one valid failure mode, each should be examined. Failure modes may be based on SME advice, or guidewords
Local Effect	impact on the current task, including implications for future task steps (be they main or alternate)
System Hazard	Definition of any possible hazards the local failure effect may present
HEART task Category	HEART category selected for this task failure
Category nominal unreliability	The nominal human unreliability allocated to the selected Heart category
Error Producing Conditions	A summary of the applicable EPC(s) from the HEART table, and the Assessed Proportion of Effect (APE) for each.
HEP	Calculated based on the HEP for the task failure
External Triggers / Conditions	Defines what is required for hazard to become an accident, including pre-existing mitigations
Adjusted likelihood of hazard	Modified HEP taking into account the impact of the external triggers and conditions
Severity of accident	Severity of worst credible accident, calibrated to match the risk matrix or other technique, in use.
Risk	Calculated risk
Recommended mitigations	Mitigations to reduce risk where required, taking into account the hazard mitigation hierarchy. Noting that the focus of this analysis technique is to reduce either the category of the Task, Or to remove EPCs / reduce their APE.
Post-mitigation Likelihood	Likelihood following implementation of mitigations
Post-mitigation Severity	Severity following mitigation
Post-mitigation Risk	Calculated Risk, once all mitigations implemented
Comments	Any further comments which relate to this failure mode.

Table 1: Analysis structure

3.2.3 Well-understood techniques

The approach focuses on conducting an early breakdown of User Tasks, based on Functional requirements of the system, and performing a FMECA style analysis on failures of each user task. This FMECA is calibrated based on a very quick HEART based analysis (guided directly by the tables). The intention is to remove subjectivity in the analysis, by using a structured calibration such as HEART it allows the team conducting the analysis to compare like with like.

3.2.4 Comparative assessment

The analysis is not intended to form a quantitative risk analysis, rather it allows for a comparative assessment of the different HMI hazards presented in the proposed system.

As the analysis is comparative in nature, it is argued that it is less prone to individual risk rating criteria. As long as the engineer conducting the analysis applies the HEART method consistently, it does not matter if they have a more or less risk averse strategy.

This will enable the system designers to either eliminate hazards, or develop the system in such a way to reduce these hazards SFAIRP. The key outcomes will be the critical functions, and the magnitude of achieved risk reduction from the selected mitigation strategies.

4 Case Study

To demonstrate an application of the methodology a case study is provided in this section. The selected case study examines a proposed design for a Positive Train Control (PTC) Driver Machine Interface (DMI). No specific technology is referenced, as the purpose is to examine the interface only, rather than compare different PTC solutions.

4.1 PTC Screen

The proposed PTC under examination provides supervision of a train against defined allowed speeds (both temporary and permanent) and defined Limits of Authority (LoA) within a rail network. To enable this supervision the PTC needs to be configured with the network geography to be covered and the specific configuration of each train to be supervised.

Two separate interfaces are provided to support the configuration and operation of each installed PTC. To configure the track database, and generic information about the network and train types a Maintenance interface is provided, which is portable and shared between the fleet. Each locomotive is also fitted with a DMI which allows for driving advice to be provided to the driver, and to seek configuration specific to a given train, or driver confirmations.

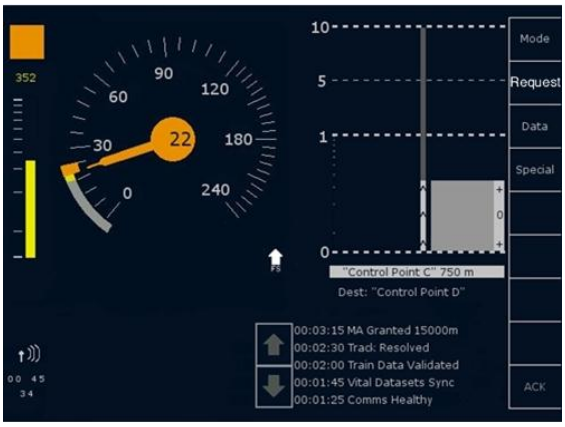

Figure 1: Example PTC DMI

An example DMI configuration is provided in Figure 1. The DMI has a touch sensitive screen which is used to

receive input directly from the driver. Data entry is managed through selecting menu items from the right, and entering data, or confirming data as shown in Figure 2.

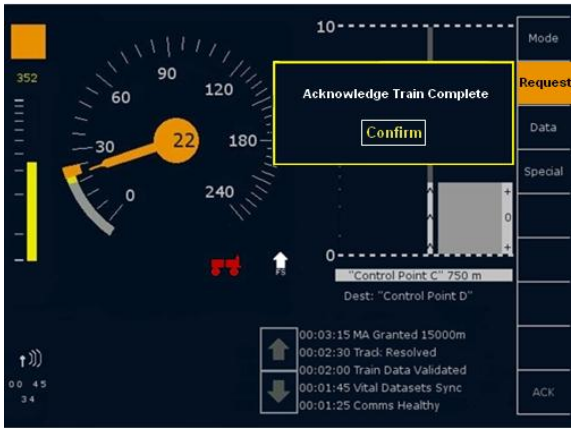

Figure 2: Confirmation overlay.

It is the second interface that this paper is concerned with. In summary the following functions are provided by the DMI:

1. Display LoA information;
2. Display Maximum allowed speed, and upcoming speed changes;
3. Display warnings of impending violation, and notification of enforcement;
4. Display driving mode (i.e. whether the train is under active supervision or not;
5. Receive train configuration particulars; and
6. Receive driver confirmation of internal data; and
7. Confirmation for significant alerts.

Items 5, 6 and 7 in the above list have been selected to demonstrate the analysis methodology. These functions were selected as they involve user input and multiple interaction steps, which present immediate opportunities for error. Functions one to four involve general information gathering and situation awareness. Such functions are subject to latent understanding failures and require a more thorough understanding of the context of use than is feasible to provide in this paper.

4.2 Use Cases

To demonstrate the simple task analysis three functions have been selected. To provide context, a brief summary of the requirements is provided, followed by the use case sequences. Whilst the sequences could be represented as either sequence diagrams or UML Use cases, a tabular format is provided in Table 2 to provide an example of a simple, yet effective representation.

1. Track Selection: At the commencement of a mission the PTC system may not be able to accurately resolve which track a train is on in multiple tracking areas. The PTC shall request Driver selection of current track occupancy from a list of available tracks.

2. Enter Train Data: At the commencement of a mission the PTC shall default to "worst case" train configuration, i.e. most restrictive braking enforcement calculations assuming maximum length and weight. To allow for reduced headways the PTC shall allow the driver to enter the current configuration of the train. The driver shall be required to confirm train configuration prior to any modification of the braking calculations.

3. Confirm Integrity: Should the PTC detect a loss of train integrity (defined to be a significant change of detected length, or an unexplained loss of brake pressure) it shall immediately alert the driver to the loss of integrity, and notify the central authority server (In the ERTMS concept this is referred to as a Radio Block Centre, or RBC) to prevent roll-up of protection behind the train. The PTC shall allow the driver to "acknowledge train integrity" (despite the system detection of loss of integrity) thereby removing the alert and allowing for roll-up behind the train.

ID	Goal	Main Task	Alternate Path(s)
1	**1. Track selection**	1. DMI displays candidate list of tracks received from DB	
2		2. scroll and select track	
3			2a.1. scroll
4			2a.2. close window
5	**2. Enter data**	1. Select data menu	
6		2. Select driver ID/train ID/train data	
7		3. Enter data via keypad	
8			3a.1. navigate text via arrow keys
9			3a.2. delete text via delete key
10			3a.3. return to 3
11		4. observe entered data on confirmation window	
12		5. confirm or reject entered data	
13	**3. Confirm integrity**	1. Observe Loss of integrity	
14		2. select Request menu	
15		3. select Train Integrity menu	
16		4. select Acknowledge	

Table 2: Example Sequences

4.3 FMECA

To demonstrate the application of FMECA to the task sequences identified in Table 2 an analysis of Function 3 (Confirm Integrity) is provided in Table 3. In the interests of space only Steps 1 and 4 are shown. The outcome of failures to perform steps 2 and 3 were determined to be equivalent to failure to identify a loss of integrity from a system point of view.

The table shows possible error modes for IDs 13 and 16 in the task analysis. There are two error modes for ID 16 and these are shown as 16a and 16b.

Comparing the pre-mitigation risk likelihoods of line item 13 with line item 16b it is clear that item 16b is more critical (several orders of magnitude), even taking into account the subjective nature of the failure rate calibration. As such it is reasonable to apply further risk reduction to incorrect confirmation of integrity.

ID	13	16a	16b
Goal	**3. Confirm integrity**		
Main Task	1. Observe Loss of integrity (B7)	4. select Acknowledge	
Alternate Path(s)	-	-	-
Failure mode(s)	Fail to observe loss of integrity, proceed on mission without conducting rest of task	Fail to acknowledge (cancel request)	Acknowledge that train is complete when wagons have been left behind or are being dragged.
Local Effect	Fail to confirm integrity, RBC prevents roll-up behind train	Fail to confirm integrity, RBC prevents roll-up behind train	Fail to initiate safeworking procedures to protect following trains
System Hazard	Obstruction left on track / track damage	See line 13	Obstruction left on track / track damage
HEART task Category	F (taken to be top of the band as no external checking)	-	F (taken to be top of the band as no external checking)
Category nominal unreliability	0.007	-	0.007
Error Producing Conditions	8. Channel capacity overload 6, APE = .2 there is a lot of information on the display, only a small icon indicates integrity loss, audible alert should draw TD attention	-	4. A means of suppressing or overriding information or features which is too easily accessible 9, APE = 1 as the interaction for confirming loss is the same as confirming completeness and the warning will be removed from the DMI.
HEP	0.014	-	0.063
External Triggers / Conditions	Integrity failure must lead to wagon left behind or track damage (ARTC input) RBC Failure to protect following traffic (SIL 4)	-	Loss of integrity leads to wagons left on track (or track damage sufficient to cause derail)
Adjusted likelihood of hazard	4.424E-13	-	1.26E-05
Severity of accident	5	-	5
Risk	M	-	H
Recommended mitigations	No further reduction required	-	Recommend system allows for confirmation that integrity is lost, and design support in other system to protect following rail traffic. Additionally, require drivers to enter actual train length at train creation to reduce false positives. Results in moving Nominal Unreliability to the bottom of Band F (8E-4) and reduce APE to .2
Post-mitigation Likelihood	4.424E-13	-	4.16E-07
Post-mitigation Severity	5	-	5
Post-mitigation Risk	M	-	M
Comments	Assume design shall be updated to include Audible alert on detection of loss of integrity Assume integrity is lost once every 1000 train hours.	-	Design is such that drivers are not required to enter train length on train creation, leading to default (worst case) figures being used) Assume that confirmation of integrity involves procedural checks such as walking the train length or seeking confirmation from crossing trains. Assume integrity is lost once every 5000 train hours. (comparable railway experienced 30 coupler separations in 150000 train hours)

Table 3: Example Sequences

To determine the most effective mitigation the engineer must examine the selected EPC(s) and determine to either remove them, or reduce their APE. As the currently proposed PTC DMI only allowed for operator confirmation that integrity had not been lost it was identified that to allow the driver to confirm that the train had lost integrity would reduce the likelihood of inadvertently suppressing the information. By extension, this also prevents the driver form unwittingly allowing following traffic into an area where there may be significant track damage (dragging wagons) or standing vehicles (where part of the train has separated). Furthermore it was identified that requiring the driver to enter the train length at train creation would reduce the number of "false alarms", leading to reduction in learned behaviour of ignoring integrity alerts.

By allowing the engineer to identify these design clarifications it was determined that this would reduce the nominal unreliability as well as the APE. Note that the Error Producing Condition was not completely removed as it is still possible to incorrectly suppress the alarm.

4.4 Outcomes

In terms of Norman's [Norman90a] model of human-machine interaction, the design of the system is prone to "slips" whereby the Driver confirms integrity when the train is not in fact whole. Similarly, using Reason and Embrey's [Reason86] list of human error mechanisms, the most prominent cause for item 16b is Stereotype takeover. The error reduction strategy chosen is a simple form of prevention by software changes, as discussed by Kirwan [Kirwan90]. In terms of the comparative assessment, the nominal likelihood calculated moves from 1.26E-05 to 4.16E-07. The reduction in likelihood is modest but may be sufficient where there are other factors necessary for an accident to occur. The analysis and proposed design solution indicates that risk has been reduced, but that the risk for 16b remains significant, and further attention may be necessary for risk to be reduced sufficiently in accordance with the overriding SFARP principle, as required by the Rail Safety Act.

4.5 Limitations

It is noted that the methodology presented in this paper is limited to those instances where qualitative analysis is appropriate. This is due to the comparative nature of the analysis; if human error contribution to overall system performance requires quantification, then a formal HRA will need to be conducted. The methodology also assumes that the task model is simple enough to be presented in the FMECA format discussed here. As such the level of abstraction must be selected carefully.

5 Conclusions

This paper has discussed a new approach to early-lifecycle analysis of HMIs, to determine risk and assess possible design mitigations. Four key contributions and advances over current learning within the domain of analysis and assessment of safety-related human-machine interfaces. These contributions/advances have been demonstrated in the paper as follows:

1. Analysis is conducted early in the development lifecycle, before significant effort has been expended on developing the HMI, so that the development work can be guided from the outset by the analysis. This is demonstrated by the analysis in the case study, which is based on a functional task model of the system and does not require detailed design mockups or storyboards;
2. The method requires minimal human-factors expertise and can be performed by ordinary engineers. The authors of the paper are not HMI experts, but have used the combined method demonstrated in the paper to propose changes to the case study HMI that would be later tested to show that they improve the overall safety of the system;
3. The method utilises and combines well understood safety-analysis techniques with HMI-analysis methods, meaning that safety engineers do not need to retrain, but instead are extending and building on their existing knowledge. The case study shows how we have combined FMECA, a commonly used safety-analysis technique, and a simplified version of HEART, an accepted HMI-analysis method;
4. The method uses a quantified analysis to make comparative assessments of risk, to guide overall development direction. This has been demonstrated by section 4.4 in the case study, which shows how we have used comparative assessments to claim that the revised HMI is safer than the original proposal.

To further demonstrate the effectiveness of this methodology it has been proposed for application to analysis of a train control system. This will allow us to refine the approach and integrate it into our safety lifecycle.

6 References

[Bainbridge87] L. Bainbridge. Ironies of Automation, In J. Rasmussen, K. Duncan and J. Leplat, editors, New Technology and Human Error, chapter 24, pages 271-283, John Wiley and Sons, 1987.

[Byers00] J. C. Byers, D. I. Gertman, S. G. Hill, H. S. Blackman, C. D. Gentillon, B. P. Hallbert, and L. N. Haney. Simplified Plant Analysis Risk (SPAR) Human Reliability Analysis (HRA) Methodology: Comparisons with other HRA Methods.. Idaho National Engineering and Environmental Laboratory, 2000

[Carroll90] J. M. Carroll and M. B, Rosson. Human-Computer Interaction Scenarios as a Design Representation, In *HICSS-23: Hawaii International Conference on System Sciences*, pages 556-561, IEEE Computer Society Press, 1990.

[Chudleigh93] M. F. Chudleigh and J. N. Clare. The benefits of SUSI: Safety Analysis of User System Interaction, In J. Gorski, editor, SAFECOMP'93: Proceedings of the 12th International Conference on Computer Safety, Reliability and Security, pages 123-132, Springer-Verlag, 1993.

[Hollnagel98] E. Hollnagel. Cognitive Reliability and Error Analysis Method – CREAM. Oxford: Elsevier Science.

[Hoppe90] H. U. Hoppe. A Grammar-Based Approach to Unifying Task-Oriented and System-Oriented Interface Descriptions, In D. Ackermann and M. J. Tauber, editors, *Mental Models and Human-Computer Interaction 1*, pages 353-373, Elsevier Science, 1990.

[Hussey00] A. Hussey and B. Atchison. Hazard Analysis of Interactive Systems, *TR-0018, Software Verification Research Centre, School of Information Technology, The University of Queensland*, May 2000.

[Johnson90] P. Johnson, K. Drake and S. Wilson. A Framework for Integrating UIMS and User Task Models in the Design of User Interfaces, In D. A. Duce and M. R. Gomes and F. R. A. Hopgood and J. R. Lee, editors, *User Interface Management and Design: Proceedings of the Workshop on User Interface Management Systems and Environments*, chapter 20, pages 203-216, Springer-Verlag, 1990.

[Johnson 92] P. Johnson. *Human Computer Interaction - Psychology, Task Analysis and Software Engineering*. McGraw-Hill Book Company, 1992.[Kirwan90] B. Kirwan. Human Reliability Assessment, In J. Wilson and E. N. Corlett, editors, *Evaluation of Human Work*, chapter 28, Taylor and Francis, 1990.

[Kirwan92] B. Kirwan and L. K. Ainsworth. *A Guide to Task Analysis*. Taylor and Francis, 1992.

[Kirwan94] B. Kirwan. *A Guide to Practical Human Reliability Analysis*. Taylor and Francis, 1994.

[Leathley97] B. A. Leathley. HAZOP Approach to Allocation of Function in Safetycritical Systems. In E. Fallon, M. Hogan, L. Bannon and J. McCarthy, *ALLFN'97: Vol 1*, pages 331-343. IEA Press, 1997.

[Mill92] R. C. Mill. *Human Factors in Process Operations*. Institution of Chemical Engineers, 1992.

[Norman90a] D. A. Norman. The Design of Everyday Things. Doubleday, 1990. [Norman90b] D. A. Norman. The 'problem' with automation: inappropriate feedback and interaction, not 'over-automation', *Philosophical Transactions of the Royal Society of London, Series B*, 327(1241): 585-593, 1990.

[RSSB04] Rail Safety and Standard Board (RSSB) Rail-specific HRA technique for driving tasks. Final report, 2004.

[Rasmussen82] J. Rasmussen. Human errors: A taxonomy for describing human malfunction in industrial installations. *Journal of Occupational Accidents*, 4: 311-335, 1982.

[Rasmussen83] J. Rasmussen. Skills, Rules and Knowledge: Signals, Signs and Symbols and Other Distinctions in Human Performance Models. *IEEE Transactions on Systems, Man and Cybernetics*, SMC-13(3): 257-266, 1983.

[Reason86] J. Reason and D. Embrey. Human Factors Principles Relevant to the Modelling of Human Errors in Abnormal Conditions of Nuclear and Major Hazardous Installations. Report for the European Atomic Energy Community, 1986.

[Reason90] J. Reason. *Human Error*. Cambridge University Press, 1990.

[Redmill97] F. Redmill and J. Rajan, editors. *Human Factors in Safety-Critical Systems*. Butterworth Heinemann, 1997.

[Senders91] J. W. Senders and N. P. Moray. *Human Error: Cause, Prediction and Reduction*. Lawrence Erlbaum Associates, 1991.

[Std00-58] UK Ministry of Defence , Draft Interim Defence Standard 00-58/1: A Guideline for HAZOP Studies on Systems which include a Programmable Electronic System, 1995.

[StdIEC-1025] International Electrotechnical Commission, International Standard CEI IEC 1025. Fault Tree Analysis, 1990.

[Swain83] A. D. Swain and H. E. Guttmann. *A Handbook of Human Reliability Analysis and Emphasis on Nuclear Power Plant Applications*. USNRC Report Nureg/CR-1278. Washington, DC: USNRC, 1983.

[Vicente99] K. H. Vicente. *Cognitive Work Analysis: Towards safe, productive, and healthy computer-based work*. Lawrence Erlbaum Associates, 1999.

[Whalley88] S. P. Whalley. Minimising the cause of human error. In G. P. Libberton, editor, *10th Advances in Reliability Technology Symposium*. Elsevier, 1988.

[Williams86] J. C. Williams. HEART – a proposed method for assessing and reducing human error. In *Proceedings of the 9th Advances in Reliability Technology Symposium*. University of Bradford, 1986