# Human Factors in the Development of Safety-Critical Railway Systems

**Simon Zhang, Weihang Wu**

**Technical Director, Senior Consultant**

**Lloyd's Register Rail (Asia) Ltd**


## SUMMARY

Existing CENELEC railway safety standards such as EN50126/9 mandate that human factors be addressed in the entire system lifecycle. In particular, the EN50126 standard has identified the five known human factors influencing the system development process. However, there is growing concern about the adequacy of existing standards and practices on managing these factors. The authors' empirical studies in the Chinese railway signalling industry have shown that the outcome of different manufacturers using the same SIL development process varies thereby resulting in different safety risks associated with the system under development.

This paper discusses the extent to which the human element contributes to the effectiveness of the process implementation and the level of confidence during the system development stages. A number of finer-grained human factors such as training, working attitude, stress, project schedule, team management style and enterprise culture and their effect on delivering safety-critical systems solutions have been discussed. Consequently, a human factors evaluation framework is proposed. This framework can be seen as an extension of existing railway safety standards.

## INTRODUCTION

Traditionally human factors engineering/study in railway signalling systems has been mainly focused on the Human-Machine Interface (HMI) design with an objective to reduce operator and maintainer error and/or its impact on system safety when the equipment/system is in its operation and maintenance stages. It is true that the operation and maintenance stages are the longest phase of a system's whole life span and the operators/maintainers are prone to make mistakes that may affect system safety. Human errors occurring in the pre-service phase of a system are typically in the form of specification errors, design errors, inadequate testing or manufacturing defects. These errors if not detected, may be embedded in a system under development and may be activated when in operation, thereby compromising the safety integrity level (SIL).

This paper presents a brief review of existing standards and practices to handling human factors during the system development process. The limitations of existing standards are then discussed in the context of the Chinese railway signalling industry. The risk based approach described in the Yellow Book [1] is then examined. The paper goes on to propose a human factors evaluation framework that refines the known human factors into a set of finer-grained attributes as well as the applicable means of evaluation.

The aim of the paper is to stimulate debate on a number of key issues when dealing with human factors in system design and development. This paper will not present all the answers. Rather, it will have served its purpose if it leads people to question the limitations of existing standards and practices.

## APPROACH OF THE STANDARDS

Not surprisingly, existing CENELEC railway safety standards [2, 3, 4] mandate that human factors be addressed in the entire system lifecycle. It is worth quoting the statement from clause 4.4.2.5 of part 1 of the EN50126 standard [2] here, as it makes the role of human factors in the railway industry much more special:

> *"Railway applications typically involve a wide range of human groups, from passengers, operational staff and staff responsible for implementing systems to others affected by the railway operation, such as car drivers at level crossing. Each is capable of reacting to situations in different ways. Clearly, the potential impact of humans on the RAMS of a railway system is great. Consequently, the achievement of railway RAMS requires more rigorous control of human factors, throughout the entire system lifecycle, than is required in many other industrial applications."*

Notably, the EN50126 standard [2] outlines a number of human factors influencing different system lifecycle stages. For instance, human factors in system design and development include:

- human competency;
- human independence during design;
- human involvement in verification and validation (V&V);
- the interface between human and automated tools;
- systematic failure prevention processes.

Although the EN50126 standard offers little guidance on how to manage the above factors in practice, the EN50129 standard [3] does briefly prescribe some process frameworks and good practices to be used to address some of the human factors with respect to different SILs. For example, it recommends the training and qualification/experience of staff as the key attributes of assessing human competency. An appropriate degree of independence between roles such as Verifier, Validator and Design/Implementer should be established with respect to the required SIL. A large number of generic measures such as human review, audit and rigorous testing are also identified as part of preventing systematic failure processes.

The use of the EN50126/9 standards is now quite widespread in many countries' railway industries and their guidelines are often viewed as the "accepted wisdom". Based on the authors' experience in applying the standards in the Chinese railway signalling industry, there is a growing view that the standards may not provide the whole story.

The standards are effectively concerned with the quality and repeatability of a development process. Yet our experience shows that the way different users interpret and execute the process can vary significantly due to a series of human factors such as the environment, human motivation and culture. This, of course, raises the question of whether the guidelines from the existing standards are adequate, taken in isolation, for the development of safety-critical railway systems especially in those developing countries like China.

## OBSERVATIONS FROM THE CHINESE RAILWAY SIGNALLING INDUSTRY

China has experienced a large number of railway construction projects at an astonishing speed in both high-speed mainline railways and metro systems in the past few years. A major railway accident occurring on 23 July 2011 has brought the Chinese railway industry to almost a halt on new development. The accident investigation report [5] concludes that the accident was due to serious design flaws in control equipment and improper handling of the lightning strike. It is outside the scope of this paper to examine the causes of this particular accident, but it serves to highlight the critical impact of design on system safety and reinforces the need for us to consider the general case of whether existing practices regarding human factors in system design and development are adequate.

In recent years the authors have been heavily involved in the Independent Safety Assessment (ISA), Railway Product Certification (RPC) and training consultancy for various safety-critical railway signalling systems in China. Most Chinese signalling suppliers claim that they have carried out the development process in accordance with the existing CENELEC railway safety standards in terms of a specific SIL. Our assessment findings in the past have shown that the outcome of different manufacturers using the same SIL development processes varies thereby resulting in different safety risks associated with the systems under

development, though the ultimate risks are still within acceptable safety levels. Underlying their compliance argument there is an implicit assumption that humans behave in the same manner with respect to the same applicable safety standard and associated processes, which does not necessarily hold in practice. The following subsections describe our findings with respect to the five human factors in system development.

**Human Competency**

Although both EN50126 and EN50129 standards mandate that all personnel with responsibilities within the RAMS process be competent to perform those responsibilities, the competence requirements for important roles, such as the verifier and validator, are undefined within the standards. The authors have seen that some organisations consider the need for independence as the only criteria for arranging the safety organisation. To achieve this independence requirement they would choose a member of staff from another department as the validator, who may have inadequate experience of the system being developed. as they may have the impression that the EN50129 standard is not prescriptive in any specific competence requirements on the validator. In this case, the lack of adequate experience of the subject being validated could be worse than a lack of independence. We should stress that the standards EN50126/9 do require both competence and independence and there is limited guidance in PD CLC/TR 50126-2:2007 [8] which also makes reference in a footnote to guidance published by the IET on the issue of competence of safety related practitioners. It is a matter for the railway organisations concerned to define their competence requirements in detail.

Most Chinese signalling suppliers have set up a safety department and introduced a number of safety related roles in the department which serve the various functional/delivery units. Many organisations consider these functional units as profit centres and people tend to stay in these units as they can rapidly gain access to the key corporate technologies and develop technical competence. Safety engineers thus face a dilemma. On the one hand, they are required to focus on the generic safety processes and have a very limited opportunity to develop domain competence. On the other, they feel like their analytical skills such as fault tree analysis (FTA), failure modes and effects analysis (FMEA) can be learnt by other domain engineers and thus they could be easily replaced. These concerns have been evident in many safety engineers, and it may lead to them wishing to move to the delivery units rather than remaining within the safety team. Organisations need to consider how skilled domain engineers can support the safety department, perhaps via secondments or providing expert support in reviewing projects where they are not directly involved.

The training and qualification systems in China are far less regulated and have been abused to some extent. Evidence for training and qualification of staff should be evaluated discreetly. In many cases it is necessary to further assess the corresponding training organisations and educational institutes in order to obtain an appropriate level of trust associated with the training records and qualifications. In any event, plans should be put in place for the on-going development of the team to ensure they remain competent and grow their capabilities further.

**Human Independence during Design**

Most modern railway signalling systems are complex and large. A "systems engineering" approach to designing such systems is usually required, which decomposes a system into a set of subsystems and facilitates the assignment of those subsystems to development teams to accomplish certain tasks. Effective design of each subsystem requires active cooperation of all team members of that subsystem in meeting the task requirements. Project managers may have the authority to delegate specific tasks to team members but working behaviours and performance of team members should be significantly independent. The network of human independence required to accomplish a given task should be based on the shared responsibility of all members including the project manager.

However, many Chinese railway organisations are state-owned enterprises and have rigidly hierarchical organisational structures. For these organisations, the integrating force towards functional performance is authority. Managers operate projects through clear-cut relationships and tight controls over the project

members. Such leadership patterns may compromise the human independence during design, particularly when dealing with professionals and domain specialists. Consequently, the authors have seen two extremes: either the project manager dictates every design decisions (e.g. selection of system architectures), leaving no space for the designers for any improvement or optimisation; or the project manager does nothing technical but just signs any document when required, thereby failing to help the team or group meet its goal and potentially removing a key control in the assurance of the design output.

Another interesting phenomenon the authors have observed is the manager's attitude before and after the 7.23 accident. Prior to the accident many managers would sign documents with little scrutiny when asked, while after the accident they are reluctant to sign anything. This is often caused by misinterpretation of their role and responsibility. In some extreme cases the authors have seen detailed project technical documents going to senior management for signature, and they tried to scrutinise technical details aiming to assure themselves that the technical solution is correct. People have not realised that different level of controls and roles are there to tackle the (human error) issue. The key is for the manager to establish that the documents have been reviewed by independent competent people – the manager needs to ensure this has taken place before taking responsibility for the resulting deliverable. Safety assurance does not require the manager to have all the competencies of the team which he manages – but to make sure the team has them and applies the correct controls to the work being done.

**Human Involvement in V&V**

The V&V activities are often seen as an important but difficult and expensive process, especially for developing large or complex safety-critical systems. As pointed out previously, human competency is one of the key factors to the effective achievement of V&V. Just as another example, most organisations will conduct safety audits periodically as suggested by the standards. These weaknesses in the audit teams domain competence can lead to failure to effectively identify issues in the project, or when issues are suspected, failure to effectively articulate the underlying reasons for the concerns. This may then be seen by the project team as the auditors getting in the way of project progress with no credible reason.

Failure to realise the relationship between V&V and process improvement is another key issue. Our assessment experience has found that many managers treat the V&V process as part of a compliance-based process (i.e. how to choose and implement the EN50129 compliant V&V techniques with respect to a specific SIL). As a result, their expectation of the success outcome is very high and they could not effectively learn from the failures identified by the V&V activities. Consequently, the outcome of the V&V process could not be effectively fed back to the system development process.

Finally, the availability of sufficient resources and feasible project scheduling is equally important in order to execute the V&V process correctly. The authors have heard that the verifier and validator complained about the lack of resources or very tight project schedule leading to a rush for completing the V&V activities.

V & V activities present a real opportunity for projects to correct issues early and to build good safety levels into the system at every stage. To achieve this requires the people involved in the V & V process to be competent not just in assessment activity, but also the domain and systems in which they are carrying out the V &V. In a complex system this may often mean the use of teams to carry out the V & V activity, as the competence required may be diverse.

**Interface between Human and Automated Tools**

The use of automated tools has become more and more popular in the railway signalling industry, especially when developing software-intensive systems. Currently the EN50129 standard is concerned about whether the tools are proven in use or validated, and there is lack of guidance on human competence in using the tools. Interestingly, it is not the first time that the developers turned to ask the authors about how to use a specific tool or how to resolve a particular problem arising from using a tool.

Furthermore, the authors have noted that operations of many automated tools such as simulation or data preparation tools require appropriate intervention by humans and the data or events that they have

produced require correct interpretation. It is not difficult to find that the tool and its user/operator together have become a system in which any misbehaviour of the user/operator may in turn have a safety impact on the system under development. Unfortunately, there is lack of consideration on this aspect in the EN50126/9 standard.

### Systematic Failure Prevention Processes

The processes and techniques/measures are prescribed and good practices are presented inherently within the standards. There is hardly any explanation in the standards themselves as to why they are there and what particular risk this process or technique/measure being adopted is intended to address. The readers are supposed to understand the rationale behind this so that they will adopt and adapt the processes to their projects, having taken into account of particular issues like the project context, type of projects, personnel who deliver the project, which may affect the effectiveness of these processes.

This, of course, may again raise the question of human competency, as the competent personnel with known responsibilities (such as V&V) should be able to correctly understand and properly interpret the corresponding process requirements of the standards. However, having put aside the competency factors, it may be worth asking about whether existing guidance on the techniques/measures is adequate. Almost a decade ago, one of the authors wrote an international conference paper [6] and pointed out that there is little guidance from existing software safety standards such as [4, 7] on how to design safety critical software. Clearly, discussing these software design issues here would distract from the main aim of the paper. The point we've made is that simply linking techniques/measures with a level of recommendations does not adequately help define the systematic failure prevention processes.

In the past few years, we have seen an increasing number of clients seeking clarification of the application conditions, limitations and rationale behind particular techniques/measures. Different people may have different background and industry specific experience. Thus they have different understandings of a specific technique/measure. Just like a glossary of technical terms, we need common vocabulary and knowledge framework for describing these techniques/measures.

## RISK BASED APPROACH

It is well recognised that EN50126/9 series standards are process oriented approaches and the Yellow Book [1] proposes an alternative risk-based approach. The difference between the two can be illustrated through a spectrum running from technology based and value based decisions, as shown in Figure 1 below.

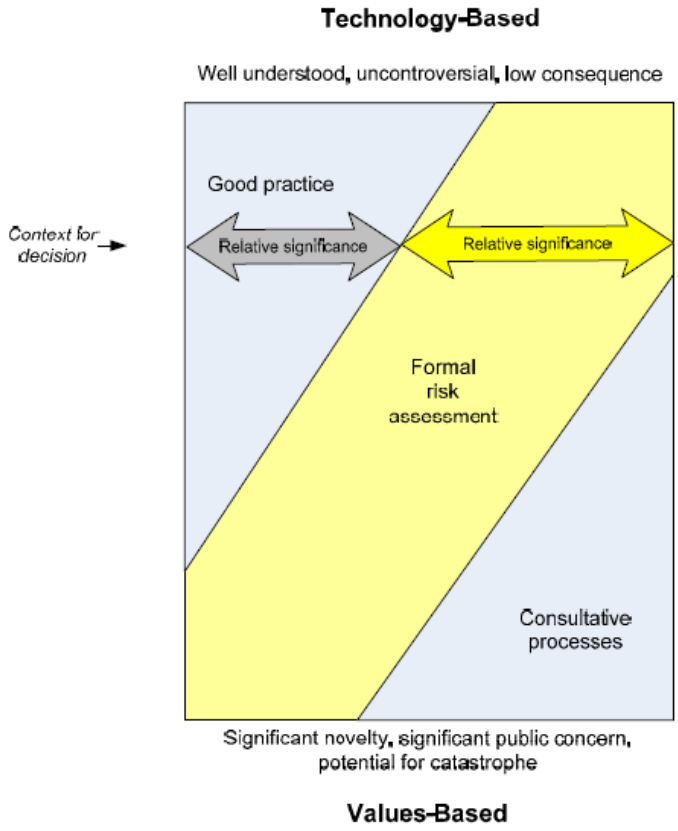


***Figure 1: Compliance-based Vs Risk-based Decision Making***

When all of the risk is covered by the standards, the Yellow Book suggests that evidence of compliance with the standards is enough for demonstration of controlling the risk. Otherwise a risk based approach should be considered. Our limited empirical studies based on the Chinese railway signalling industry cannot be taken as conclusive, but the evidence does support the observation that existing EN50126/9 standards do not adequately address the risk associated with human factors in system development. The risk based approach is thus applicable. We are certainly not suggesting that this leads to the conclusion that the standards are worthless on these aspects; they provide an essential contribution on which we can build.

The approach proposed here is to explicitly identify and evaluate the underlying risk associated with known human factors in system development, apart from making a general appeal to process based compliance. Our human factors evaluation framework is based on the five human factors (such as human competency) identified by the EN50126 standard. For each human factor we have identified a number of finer-grained attributes and relevant means of evaluation, as listed in Table 1.

***Table 1 Evaluation Framework for Human Factors in System Development***

| Human Factors | Attributes | Means of Evaluation |
|---|---|---|
| Human competency | • Role<br>• Qualification<br>• Experience<br>• Training<br>• Domain knowledge<br>• Relevant skills<br>• Organisational culture | • Definition of responsibilities and authority<br>• Definition of competence requirements<br>• Qualified or certified training institutes<br>• Good university degrees<br>• Interviews with staff<br>• Sample check of work – activity monitoring<br>• Review of company profile such as organisational visions and values |

| | | |
|---|---|---|
| Human independence during design | • Management style<br>• Management attitude<br>• Motivation for staff<br>• Leadership pattern<br>• Organisational structure | • Interviews with staff<br>• Review of change management system<br>• Document review of project management plan<br>• Review of company profile such as organisational structure and delegation |
| Human involvement in V&V | • Human competency<br>• Relationship between V&V and process improvement<br>• Project management<br>• Interface between human and tools | • Refer to measures for human competency<br>• Review of V&V plan and relevant reports<br>• Audit on V&V activities<br>• Document review of the project management plan or development plan<br>• Refer to measures for interface between human and automated tools |
| Interface between human and automated tools | • Tool behaviours<br>• Tool related failures<br>• Human competency<br>• Process for using a tool | • Availability of tool specification or manual<br>• Tool validation or alternative means for evidence<br>• Safety analysis over the closed loop process involving both the tool and its user/operator |
| Systematic failure prevention processes | • Human competency<br>• Tactic knowledge<br>• Understanding of safety standards | • Refer to measures for human competency<br>• Document review of planning documents such as the system safety plan, software quality assurance plan, quality management plan, configuration/change management plan etc<br>• Safety audit on the development process<br>• Review of safety management system |

The principle using the above evaluation framework is quite straightforward. Firstly, for each human factor we have refined it into a number of key attributes based on our empirical studies from the Chinese railway industry. For example, one of the key attributes for human competency is domain knowledge, which is surprisingly missing in the EN50129 standard. Indeed there is evidence (albeit mostly anecdotal) which suggests that the most significant factor in achieving low hazardous failure rates is domain knowledge [7]. Secondly, for each attribute, we evaluate the potential risk through the applicable measures. For the same example of the domain knowledge attribute, we could evaluate it through interviewing the staff and carrying out sample check of his/her work. Of course, the risk assessment is conducted in a qualitative manner. Finally, like any other means of safety risk assessment, the outcome of the risk assessment on human factors is to prioritise the risk and identify the applicable risk mitigation measures. For the case of domain knowledge, if we have identified that the member of staff with assigned responsibility (say, for example, for validation) does not have sufficient domain knowledge, we may conclude that the level of confidence associated with the validation work is low and request a re-validation by a competent person.

Like the standards, the nature of our approach is still process based in a way that we have identified some applicable processes and measures. Therefore it is reasonable to assume that our approach extends the existing standard with consideration of human factors on system design and development. The ideas behind

this approach are still in their infancy, but there is some substantive work being undertaken, with an expectation of tangible feedback on the viability of the approach in the near future.

## EVOLUTION OF THE STANDARDS

The authors have noted the recent update of the railway software safety standard EN50128 [4], and some of the issues mentioned in this paper have been addressed in the context of software development. In particular, it introduces detailed guidance on the competency requirements (such as the definition of the roles for the Project Manager, Verifier and Validator) and using support tools for software development. However, there is still a lack of sufficient guidelines on human factors related to human independence, interface between human and automated tools and systematic failure prevention processes.

We also note that the update of the EN50126/9 series standards is currently on the way and believe that they will provide some answer on the concerns we share.

## CONCLUSION

There is a growing concern that the current set of CENELEC railway safety standards may not have adequate guidance on addressing human factors in system development. This paper has highlighted some fundamental issues related to the five known human factors identified by the EN50126 standard. Although our empirical data are based on the Chinese railway signalling industry, we believe that most of the problems are generic and should be applicable to other countries and other railway areas.

Whilst, in this paper, it has only been possible to sketch the basic ideas, there may be a number of ways to elaborating the ideas being developed and experimentally evaluated. It is hoped that this might, in time, provide useful starting points for managing human factors during the system development process.

## References

[1] Engineering safety management (the Yellow Book), Issue 4

[2] EN50126:1999 Railway applications - reliability, availability, maintainability and safety

[3] EN50129:2003 Railway applications - safety related electronic systems for signalling

[4] EN50128:2011 Railway applications – software for railway control and protection systems

[5] The "7.23" Chinese Yongwen line catastrophic railway accident investigation report, http://www.china.com.cn/policy/txt/2011-12/29/content_24282667.htm

[6] WU W, "Safety tactics for software architecture design", in Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC 2004), pages 368-375, IEEE Computer Society Press, 2004

[7] SHOOMAN ML, Avionics software problem occurrence rates, pages 53-64, IEEE Computer Society Press, 1996

[8] PD CLC/TR 50126-2:2007 Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Guide to the application of EN 50126-1 for safety

**APPENDIX 1:**

**APPROVAL TO PUBLISH PAPER**

I/We .....Simon Zhang, Weihang Wu.....

of Company (if applicable) .....Lloyd's Register Rail (Asia) Ltd.....

hereby give permission to the International Railway Safety Conference 2012 (IRSC 2012) to publish the paper titled:

Insert Title ..... Human Factors in the Development of Safety-Critical Railway Systems.....

To be presented at the IRSC 2012 conference to be held at the St Pancras Renaissance Hotel, London, England on 8 - 12 October 2012.

In the following media (tick as appropriate):

☑ Copied to memory stick for distribution to conference delegates

☑ Publish on the IRSC 2012 website

Signed: .. .....

Date: .....31/8/12.....

Please return this form when submitting the final version of the paper.