Safety assurance for a signalling system based on quality management

F. Yan
School of Electronics and Information Engineering,
Beijing Jiaotong University, China

Abstract

The fast development of the Chinese railway and metro system and the extensive use of modern complex electronic programmable systems in signalling systems have posed a great challenge to the safety of railway. The conventional means of equipment testing and quality management are no longer considered adequate. The development of safety science has helped both the industry and authorities in the area of safety assurance in railway. The developments of safety theories and research have resulted in the creation of a number of European standard, best practice and government regulation. Some of the CENELEC EN standards have been adopted by the International Electrotechnical Commission (IEC) and hence these standards have become international standards. Compliance with these standards means international recognition of the product/system. This paper, while giving an overview of the quality management framework, explores how the Chinese rail industry could develop its own safety assurance and certification framework.
Keywords: safety assurance, quality management, railway signalling system.

1 Introduction

The service provided by rail transportation is influenced by functional and performance characteristics. The extensive use of modern complex electronic programmable systems in signalling systems has posed a great challenge to the safety of railway. The conventional means of equipment testing and quality management are no longer considered adequate. This paper, while giving quality an overview of the quality management framework, explores how the Chinese rail industry could develop its own safety assurance system.

WIT Transactions on Information and Communication Technologies, Vol 47, © 2014 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK140421

The remainder of this paper is organized as follows: Section 2 presents the conventional quality management framework briefly. In Section 3 we present a Safety Assurance Strategy for the signaling product and our conclusions are presented in Section 4.

2 Quality management framework

In recent years the importance placed on achieving "quality" within all fields of endeavour has increased enormously. Over the years, many industrialists and academics have attempted to characterize quality and it is defined in many ways, including:

- Fitness for use;
- Conformance to requirements;
- The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs.

Quality management aims to maintain and improve all aspects of the quality of products and services supplied by an organization and the processes within that organization. This activity may be divided into quality assurance and quality control. From its definition it is clear that quality management covers a number of activities. These may be categorized into the broad areas of:

- Defining the production process and the management system;
- Management of resources;
- Auditing and corrective action.

Since quality relates to the ability of a product to meet its requirements, it is clearly of fundamental importance to safety. To understand the role of quality in enhancing safety, we need to look at quality systems in a little more detail. Although the objectives of quality assurance and quality control are obviously closely linked, their methods of implementation are very different.

Quality assurance concentrates on the process of manufacture and attempts to ensure that work is performed correctly. Quality control aims to ensure that the product is correct, where the term "product" represents what is delivered to the customer. A product in this context may be some kind of system or component, or some form of service.

A management system needs to cover all aspects of the work throughout its complete lifecycle. Resources in this context include the provision of suitably qualified staff and would include such issues as training. Auditing is used to ensure that the various activities of the management system are implemented correctly. It should be noted that quality assurance is not concerned with the design and testing of a system, but is involved in ensuring that the design and testing operations are performed correctly. This is an ongoing activity that continuously strives for improvement through a process of iteration. The actions that are required during the various lifecycle phases are as follows:

- Contract review
- Requirements
- Development planning
- Quality planning
- Design and implementation
- Testing and validation
- Acceptance
- Replication
- Delivery and installation

Quality control came to prominence in the field of high-volume mechanical manufacture. This often uses techniques of statistical quality control to systematically reduce the errors associated with a particular manufacturing process. This information is often compared with the specification for this part and the difference used to modify the production process. The modifications might be used to improve the tolerance of a component or to reduce the number of components that fail some form of acceptance test.

When quality control is applied to the production of computer-based system, the basic principles are similar to those described above but the detail may be very different. As before, a comparison is made between the output of the process and the original specification, and the performance of the production process is then assessed. On the basis of this assessment modifications may be made in an attempt to fine-tune the operation. Unfortunately, this process may be far from easy. When this approach is applied to hardware components or subsystems, the characteristics to be assessed include not only functionality, but also more complex issues such as reliability, maintainability and safety. For safety critical systems the required values for some of these factors are beyond our ability for measuring. Regarding software the situation is even more complicated. First, it is generally impossible to test a program completely to determine its correspondence to the functional aspects of the specification. Secondly, the requirements of the software will include features such as reliability, efficiency or portability, which may be extremely hard to quantify. Quality control depends on our ability to measure parameters within the product that we wish to control. Unfortunately, in highly complex systems this is often very difficult.

Although quality control alone cannot guarantee product quality, it does play an important part in the overall task of producing a high-quality system. In practice, quality management requires both quality assurance and quality control, to achieve the best results.

Unfortunately, for highly critical projects the quality assurance procedures of ISO 9000 are not sufficiently rigorous and a more stringent quality system is necessary. This will normally require an accurately defined management and reporting structure and a strict system of auditing. Although quality management is vital in all safety-critical projects, safety assurance methods are also required to achieve an adequate integrity level of safety.

3 Safety assurance strategy

Safety assurance is defined as all those planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy the given requirements for safety.

When the "product" concerned is a safety-critical system, the main objectives of a safety assurance system are:

- To increase the safety of the product;
- To provide a foundation for the safety justification (safety case).

Contributions to the safety justification of a critical system represent a major aspect of safety assurance. As safety cannot be demonstrated by testing alone, a system's acceptance must be based on confidence gained in other ways. Key factors in any safety case are the development and production processes used and the safety assurance methods used to oversee them.

The safety assurance principles are listed below [1]:

- Identify what may go wrong
- Find measures to eliminate, reduce the significant risks
- Plan and implement the cost effective measures, monitor and review assumptions and performance
- Ensure sufficient and competent organisation
- Develop contingency measures to limit losses when all else fails

3.1 Risk management

When we consider the safety of a signalling system, we must compare the total risk of the related safety functions and the tolerable risk, which is set by the authorities. If the residual risk cannot meet the requirements, then, measures must be taken to control the risk. Risk is a combination of the frequency or probability of a specified hazardous event and its consequence [2]. We should assure:

- Sufficient hazard identification and analysis
- Effective hazard handling in design and implementation
- Clear evidence of hazard handling and safety management
- Verify correctness of risk assessments and SIL allocations
- Justify safety requirements at different levels of the system

3.2 Process management

The process for a signalling system is based on a safety lifecycle model introduced in EN50129 [3]. The lifecycle is represented in a V shape arrangement to show how the system has been developed and integrated.

In each stage, the necessary technologies and methods must be adopted according to EN50129 and the system safety requirements. We employ a practical safety assurance process:

1) Safety requirements

The conceptual process for the definition of these requirements is as follows:

- Identify goals – the stakeholders' main aims and desires.
- Model the environment and properties.
- Derive more detailed requirements based on real-world constraints.

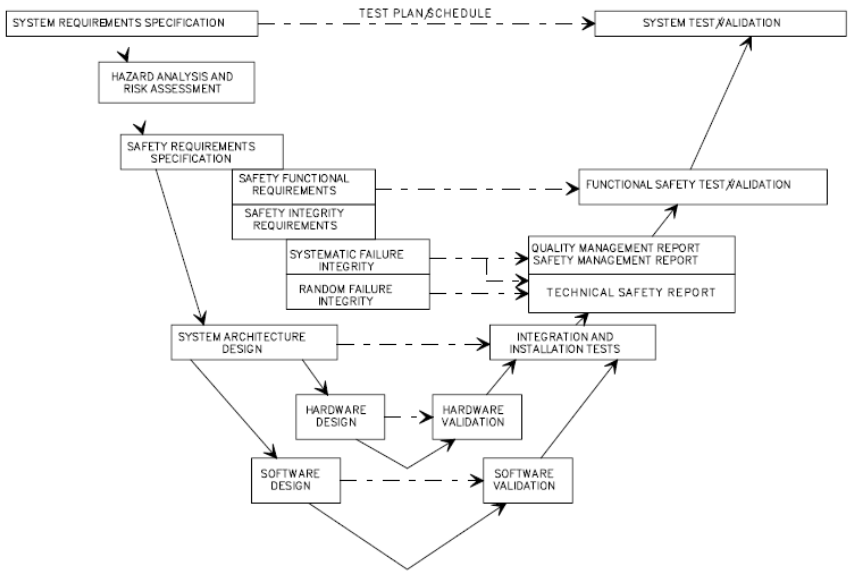

Figure 1: Safety lifecycle.

2) Hazard analysis

- Preliminary hazard analysis
- System hazard and risk analyses
  - SHA
  - FMECA
  - OSHA
  - FTA
- Software hazard analysis

3) Design for safety

- Eliminate and minimize hazards by design
- Assure safety critical function
- Incorporate safety devices into the design

4) Safety verification

- Quality assurance during manufacturing
- Verifications
  - System integration
  - Test and commissioning, system validation
- Safety audits
- Safety case
- Hazard log review
- Operation and safety report (OSR)
- FRACAS

Before safety certification, we should confirm the following:

- Verify the quality of all plans in product development lifecycle
- Verify plans consistency with standards and QA/QC records
- Confirm development activities and milestone records compliance with plans and standards
- Justify the quality of the process and management system
- Document evidence, justification conclusion in Assessment Matrix

3.3 Document management

Along with the system development, we need a series of documents to be used as safety evidence:

- Safety assurance plan
- Preliminary hazard analysis
- System hazard analysis
- Subsystem hazard analysis
- Interface hazard analysis
- OSHA
- Hazard log
- HW FMECA
- Safety V and V evidence
- Final safety case

4 Safety certification in China

Certification is the process of issuing a certificate to indicate conformance with a standard, a set of guidelines, or some similar document. The advantages of safety certification are obvious:

- Verify the safety properties of a delivered system in meeting the operational safety
- Lay the function of mutual trust between vendors and customers

- Clarify legal safety responsibilities of the involved parties
- Demonstrating safety confidence for government, communities, and passengers

While the safety certification concept is widely accepted in China we should develop a practical framework. For safety-critical systems, the certification process starts with the initial requirements analysis. During the project phases, appropriate documentation and supporting data will be produced and submitted to the authority. Usually, a series of reviews will be conducted and if all terms of the verification plan are met, the certificate or license issued.

There are three main certification patterns.

- Vendor warranty approach
- Railway authority centric (government)
- Third party certification

We should select an efficient collaboration means and set up confidence among vendor, authority and the operation company. As far as we know, Guangzhou and Wuhan Metro take third party certification; Shanghai metro take Vendor warranty approach; authority Centric Beijing Metro is thinking about an interoperability solution for signalling systems.

5 Conclusions

The local Chinese equipment suppliers, while competing against each other in the home market in a bid to uphold their market shares, are increasingly looking ambitious within the lucrative international market. In this paper we present a safety assurance strategy based on quality management. This paper also explores how safety assurance and standard compliance can give these enterprises competitive advantages based on their quality management.

Acknowledgements

This paper is supported by Beijing Higher Education Young Elite Teacher Project (ID: YETP0540), Beijing Transit Research Project (ID: 2012KJ-008) and Beijing Jiaotong University Basic Research Fund (ID: 2012JBZ014).

References

[1] Neil, S. (1996) *Safety-Critical Computer Systems*, Addison-Wesley.
[2] CENELEC EN50126, (1999) Railway applications-The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), BSI.
[3] CENELEC EN50129, (2003) Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, BSI.