How to Improve the Safety of Signalling Systems with a Shortened Construction Period in Engineering Construction Projects?

Guoliang Gao

Deputy Director of Safety Assurance Department

Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.

1 SUMMARY

How to improve the safety of signalling systems with a shortened construction period to the greatest extent? Firstly, on the basis of special attention to top-level design (i.e. overall engineering design), minimal modification of proven equipment should made and hazard log based analysis on systematic risk assessment should be conducted to improve safety through measures in design and technology terms. Secondly, such agile development practices in software engineering as iteration, refactoring and continuous integration, should be adopted to improve the quality and efficiency of the development of signalling systems. Thirdly, automation tools should be applied to improve efficiency and minimize human errors. This paper describes the methods for improving the safety of signalling systems in these three aspects and, in particular, proposes the possibility of utilizing agile development practices in the development of signalling systems.

2 INTRODUCTION

With an ever-accelerating pace of life, there is an ever-increasing lack of patience in general. This phenomenon is also noticeable in the engineering construction of safety-critical signalling systems during the construction of railways, especially in China, a developing country with rapid economic growth.

In spite of their significance as safety-critical systems, signalling systems only account for quite a small part in the construction of railways in general, and newly-built railways in particular. A great deal of time necessary for the commissioning of signalling systems tend to be taken up by the construction of such systems as civil engineering, permanent way and rolling stock systems, which tend to attract more attention of employers and investors due to their possession of obvious attributes of railway infrastructure. Secondly, in consideration of the remarkable impacts of these systems on signalling systems, adjustment of the schemes for these systems tends to necessitate considerable modification of signalling systems, and in turn, bring substantial uncertainty to signalling systems in such aspects as station layout and key signalling data.

This state of affairs gives rise to the great challenge of ensuring the safety of signalling systems. In most cases, it is inevitable to experience external influence and pressure, and it is up to builders of signalling systems to explore the significant research subject of identifying their own methods to minimize the negative impacts on safety and maximize the safety of signalling systems.

3 NOTATION

RA:	Railway Authority
RSI:	Railway Support Industry
NCR:	Non-Conformities Record
XP:	eXtreme Programming
TDD:	Test-Driven Development
CI:	Continuous Integration

4 REASONS

In China, a developing country with rapid economic growth, the construction period of signalling systems tends to be shortened to a large extent either explicitly or implicitly during the construction of railways. This can be attributed to various factors, which can be classified into the following three general types.

4.1 Social Influence

In China, trains remain the major means for intercity transport. With a large number of passengers vis-à-vis a small number of trains and an ever-increasing desire of the general public for shortened journey time, there is an ever-rising expectation of the whole society for shortened construction period of railways. Furthermore, with an ever-accelerating pace of life, there is an ever-increasing lack of patience in general. This phenomenon is also inevitable in the engineering construction of safety-critical signalling systems during the construction of railways, especially in China, a developing country with rapid economic growth.

4.2 Small Share of Signalling Systems in Total Budget for Railway Construction

In spite of their crucial role in railway systems in ensuring the safety of train operation, signalling systems only account for quite a small share in the total budget for the construction of railways in general and newly-built railways in particular. Such systems as civil engineering, permanent way and rolling stock systems tend to attract more attention of employers and investors due to their possession of obvious attributes of railway infrastructure, the construction of which tend to take up a large amount of time necessary for the construction of signalling systems in such aspect as installation and commissioning.

4.3 Restriction and Limitation of Other Systems to Signalling Systems

In consideration of the remarkable impacts of such systems as civil engineering, permanent way and rolling stock systems on signalling systems, adjustment of the schemes for these systems tends to necessitate considerable modification of signalling systems and, in turn, bring substantial uncertainty to signalling systems in such aspects as station layout and key signalling data. It is often the case that the installation of signalling equipment is required before the completion of system design, which has significant impacts on the design, development, installation and testing of signalling systems.

Of these three types of factors, those related to “social influence” are beyond the control of supply industries of signalling systems; those related to “small share of signalling systems in total budget for railway construction” can be addressed through joint efforts of the railway industry as a whole to enhance the common understanding of the significance and crucial role of signalling systems, and through publicity and accident explanation measures to attract the genuine attention of Railway Authorities (RAs) and safety authorities to signalling systems; and those related to “restriction and limitation of other systems to signalling systems” can be handled through sufficient communication efforts of engineers of signalling systems to send a clear message to RAs, safety authorities and builders of other systems about the serious impacts of these systems on signalling systems. All these efforts and measures are aimed at minimizing the external impacts and influences on signalling systems and should be accompanied by pragmatic internal efforts of builders of signalling systems to improve the safety of signalling systems.

5 TECHNIQUE MEASURES

Measures in design and technology terms strive to minimize risks and improve the safety of signalling systems at the fundamental. But these measures are involved in various aspects and multiple levels, to achieve favourable results under the condition of shortened construction period as a result of these types of external pressure, it is essential to focus on the critical issues. Overall design is one critical issue because of its significance as overall technical analysis and design developed on the basis of overall system architecture and system/subsystem interfaces and with consideration to specific railway layout, and its impacts on apportionment of system, subsystem and equipment functions and characteristics of interfaces. Risk analysis is another key issue because of the significance of risk-based safety management as the key to ensuring the safety of safety-critical signalling systems.

5.1 Overall Design

Overall design denotes to technical design at system level developed on the basis of system requirements and applicable technical standards and specifications, in accordance with the restrictions and conditions of existing subsystems and equipment and with special attention to the actual conditions of specific railways and provides the following three major types of outputs:

Type I: signalling layout;
Type II: architecture design of signalling systems, including system composition, subsystem division, apportionment of system requirements, subsystem interface and network composition;

Type III: system interface specification, including interface description, interface definition and information exchange.

From the status and role of overall design, it can be concluded that adjustment of overall design has significant impacts on modification of signalling systems, and consequently on their construction period and safety. Then, how to minimize the impacts of adjustment of overall design on subsequent modification of subsystems and equipment and, in turn, on construction period and safety?

5.1.1 Special Attention to Overall Design

Firstly, from the perspective of system engineering, construction of signalling systems requires special attention to overall design to avoid its random modification. Secondly, according to the layered system model (EN 50126-2: 2007) [5], development of overall design requires sufficient consideration to the interactions and mutual influences of various subsystems of signalling systems, between signalling systems and other systems at the same level, and among signalling systems, other systems at higher levels and environment. Thirdly, adjustment of overall design requires strict change control.

According to the system lifecycle recommended in EN 50126-1: 1999 phase 4--System Requirements is followed by phase 5—Apportionment of System Requirements [1]. On the surface, apportionment of system requirements to various subsystems and components is achieved upon specification of system requirements. In essence, however, “overall system design” is also involved as an important but implicit stage either hidden between these two phases or incorporated into phase 5, in that apportionment of system requirements to subsystems or components is impossible without overall design of system requirements, which determines the types of subsystems in signalling systems and the means of interaction between their subsystems.

During overall system design, it is critical to give sufficient consideration to the interactions and mutual influences between signalling systems and other systems at the same level, other systems at higher levels and environment, an important link to minimize external influences. It is therefore necessary to arrange for sufficient communication between supplies of signalling systems and other systems at the same level and at higher levels to standardize interface definition at an early date.

5.1.2 Minimization of Modification of Equipment

Some subsystems and components are in existence before the commencement of overall system design. On the one hand, these subsystems and components may pose restrictions and limitations to overall system design. On the other hand, overall system design may necessitate change requests for these subsystems and components. As a result, overall system design requires sufficient consideration to the restrictions and limitations of existing subsystems and components and their deviations from system requirements specification, and sufficient analysis of the possible impacts of overall system design on existing subsystems and components. These measures are aimed at adapting to the restrictions of existing subsystems, while minimizing modification of existing subsystems and components and components under the precondition of compliance with system requirements without degradation of safety performance. This can not only lower the requirements for construction period, but also mitigate the impacts of modifications to safety performance. It is self-evident that the less the modification to existing subsystems and components, the lighter the workload for development and the lower possibility of new risks.

5.2 Risk Analysis

According to the requirements specified in EN 50126: 1999, system hazard analysis should be carried out to give sufficient consideration to the impacts of personnel, processes and system modes (normal, degraded and emergency modes) to safety. Systematic methods to improve the safety of signalling systems require risk analysis and assessment not only through systematic and structured processes but also in a continuous manner at various stages of the lifecycle.

The general risk analysis process includes the following two types of steps: [1]

a) risk assessment steps comprising:

- system definition,
- hazard identification (preliminary and detailed) including hazard log,
- consequence analysis,
- risk assessment and allocation of THRs, where appropriate;

b) hazard control steps comprising:

- hazard control, including causal and common cause analysis.

In some cases, risk analysis is tedious and time-and-energy consuming, and has high requirements for the knowledge, expertise and experience of risk analyzers. Effective and efficient risk analysis in combination with effective measures for strengthening the implementation of risk control measures is the key to improving efficiency and safety.

5.2.1 Risk Analysis Based Approach

According to EN 50126: 1999, risk assessment falls into the responsibilities of RAs, and hazard control the responsibilities of Railway Support Industry (RSI) [1]. However, risk analysis requires expertise and experience is such fields as railway system, functionality, design, operation, maintenance and environment. Therefore, joint efforts of RAs and RSI are required for both risk analysis and hazard control in general and high level risk analysis at system level in particular. Joint efforts for risk analysis at system level of RAs, engineering designers, system integrators and RSI are particularly necessary in China, a country with a fast pace of railway construction, to identify the effective measures for risk control and achieve the interaction and information sharing among these parties in hazard log to some extent.

5.2.2 Qualitative Risk Analysis

Risk analysis can take both a qualitative approach and a quantitative approach. Qualitative analysis is described as a subjective and inaccurate approach dependent on expert judgment and past experience, and is characterized by no requirements for detailed quantitative data, simplicity and convenience, and lower cost vis-à-vis quantitative analysis, but possibility of insufficient analysis for lack of detailed supporting data. By contrast, quantitative analysis refers to an approach on the basis of detailed modelling and substantial data, and features possibility of more sufficient and accurate analysis, but greater complexity and higher requirements for resources.

In consideration of the greater time consumption and higher resource requirements of quantitative risk analysis vis-à-vis qualitative risk analysis, qualitative analysis is sufficient for most hazards and quantitative analysis is necessary only in the event of requirement for more detailed analysis data and evidence. Moreover, qualitative analysis can be performed with quantitative analysis techniques for some cases in the event of no requirement for quantitative calculation but requirement for detailed analysis. This method is especially applicable to system risk analysis on the basis of insufficient basic statistics.

5.2.3 Retrospective Risk Analysis in Combination with Test Non-Conformities Record

In engineering construction projects, signalling systems are subject to different tests at multiple phases corresponding to various phases on the right side of the “V” representation of the lifecycle specified in EN 50126: 1999 [1] from the bottom to the top. These tests in general and system tests in particular generate many Non-Conformity Records (NCR)s and should undergo standardized NCR management and control. During NCR analysis, participation of safety engineers constitutes not only effective retrospection of hazard logs but also an important link of effective checking of risk control measures.

5.3 Other Approaches

At design and technology level, various measures and technologies are available to improve safety and efficiency, but overall system design and risk analysis are beyond doubt the key to these measures and technologies.

6 MANAGEMENT MEASURES

Methods for strengthening development management and improving development efficiency are one effective means of controlling the risk of systematic failures and improving the quality and safety of signalling systems. EN 50126: 1999 [1] recommends a model for system lifecycle, which describes the requirements for design and implementation in phase 6. Meanwhile, EN 50128: 2011 [2] proposes a “V” model for software development lifecycle. These recommended lifecycle models have strict requirements for compliance with the requirement-design-implementation-testing-integration-validation sequence and its procedures. Indeed, strict compliance with the “V” model during the development of safety-critical signalling systems can minimize systematic failures but involves higher costs and faces practical obstacles in engineering construction projects.

During system development and testing, automation tools can realize effective reduction of human errors but requires appropriate safety analysis according to the requirements for each tool class (T1, T2 and T3, as defined in EN 50128: 2011 [2]). Automation tools subject to sufficient verification shall be prioritized for the sake of efficiency and safety.

6.1 Agile Development Practices

In software development sector, such agile development methods and practices as Scrum, agile modelling, Test-Driven Development (TDD) and eXtreme Programming (XP) have achieved rapid development and extensive application. Then, is it possible to adopt appropriate practices subject to verification through extensive application in IT industry during the development of signalling systems to improve efficiency and allow effective reduction of systematic failures?

6.1.1 Iteration development [3]

In the incremental iteration development method, the development process is subdivided into certain iterative lifecycles, which are different with the standard waterfall lifecycle (***Figure 1***).

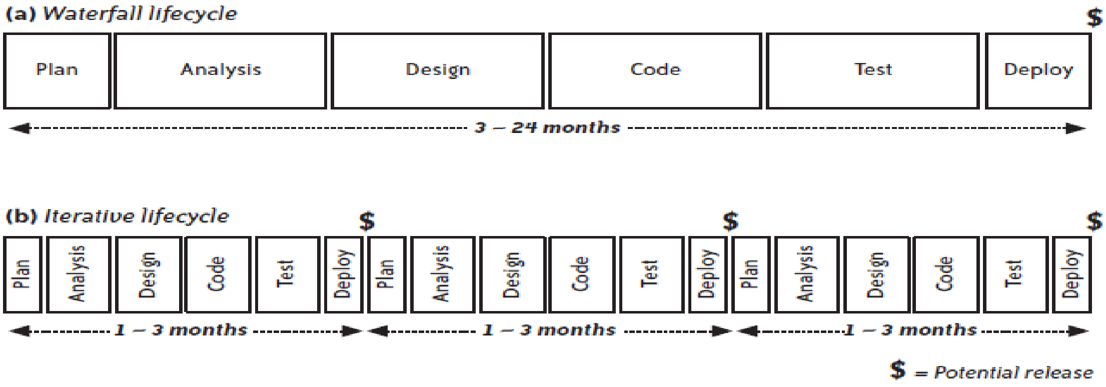

Figure 1: Waterfall lifecycle vs. Iterative lifecycle

In XP, an iteration is the full cycle of requirement-design-code-verify-release. It’s a timebox that is usually one to three weeks long. Each iteration begins with the customer selecting which stories the team will implement during the iteration, and it ends with the development team producing software that the customer can install and use. The beginning of each iteration represents a point at which the customer can change the direction of the project. Smaller iterations allow more frequent adjustment. Fixed-size iterations provide a welltimed rhythm of development.

Incremental iteration development has the advantages of early verification and feedback of requirements to allow timely adjustment of both the direction and the focus of development during the next iteration and prioritize the release of the most important parts. However, a lifecycle model in sole reliance on incremental iteration development has practical difficulties in producing ideal effects, for the simple reason that iterations tend to be smaller in agile development and the achievement of which can be ensured only with the supplementation of such agile development practices as Continuous Integration (CI) and TDD.

6.1.2 Continuous Integration [4]

Continuous Integration is a practice of performing a clean build, full integration, and running all tests every time a change is committed to the code repository. This is accompanied by frequent integration of each developer’s work into the code repository.

There are many problems in today’s typical software development lifecycle that are directly addressed by Continuous Integration.

- Integration has been traditionally seen as very difficult and risky.
- Integration becomes exponentially more risky with time.
- Lack of Integration typically masks a large set of bugs. Many of these bugs can be very serious and can by symptomatic of significant design mismatches in the system.
- A bug is an indication of an error. If that error goes unseen and uncorrected then other code that relies on the error is built upon incorrect assumptions.
- Successful Integration is a prerequisite to successful Functional Testing.
- In the Agile community, Integration includes a fully working system—that is compiling, deploying, and testing— and not just a successful compile.

Continuous Integration reduces time to market and increasing quality to market by finding Integration bugs often and early, thus eliminating “hardening Iterations” and the rework that goes along with it. Continuous Integration also increases visibility of the progress of the project by making it explicit to the development team and stakeholders.

6.1.3 Test-driven Development [3]

Test-driven development, or TDD, is an evolutionary approach to development which combines test-first development where you write a test before you write just enough production code to fulfill that test and refactoring.

Test-driven development is a rapid cycle of testing, coding, and refactoring. When adding a feature, a pair may perform dozens of these cycles, implementing and refining the software in baby steps until there is nothing left to add and nothing left to take away. Research shows that TDD substantially reduces the incidence of defects. When used properly, it also helps improve your design, documents your public interfaces, and guards against future mistakes.

In TDD, the tests are written from the perspective of a class’ public interface. They focus on the class’ behaviour, not its implementation. Programmers write each test before the corresponding production code. This focuses their attention on creating interfaces that are easy to use rather than easy to implement, which improves the design of the interface.

After TDD is finished, the tests remain. They’re checked in with the rest of the code, and they act as living documentation of the code. More importantly, programmers run all the tests with (nearly) every build, ensuring that code continues to work as originally intended. If someone accidentally changes the code’ s behaviour—for example, with a misguided refactoring—the tests fail, signalling the mistake.

TDD uses an approach similar to double-entry bookkeeping. You communicate your intentions twice, stating the same idea in different ways: first with a test, then with production code. When they match, it's likely they were both coded correctly. If they don't, there's a mistake somewhere.

It's theoretically possible for the test and code to both be wrong in exactly the same way, thereby making it seem like everything's OK when it's not. In practice, unless you cut-and-paste between the test and production code, this is so rare it's not worth worrying about. Additionally, when we develop railway signalling software using TDD, Pair Programming can be used to mitigate the risk, as Pair Programming could achieve synchronizing verification on codes by the way.

6.2 Utilization of Automation Tools

It goes without saying that automation tools can achieve substantial improvement in work efficiency and feedback speed during development, data generation and testing. Besides, reliable automation tools subject to sufficient verification can also achieve noticeable reduction of human errors.

According to EN 50128: 2011, these tools can be classified into the following three categories [2]:

1) tool class T1——generates no outputs which can directly or indirectly contribute to the executable code (including data) of the software

2) tool class T2——supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software

3) tool class T3——generates outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system

6.2.1 Automatic Testing Tools

During the establishment of a lifecycle model in reliance on iteration development, effective and agile implementation of iteration development is possible only with the supplementation of such corresponding automation tools as unit testing, automatic building and continuous integration tools, the effective utilization of can bring about considerable reduction of feedback time and improvement of work efficiency. However, most of these tools fall into the category of tool class T2. These automation tools include such types of tools as unit testing architecture tools (e.g. CppUnit), automatic building tools (e.g. Maven, Ant and Automake) and continuous integration tools (e.g. CruiseControl and Hudson).

According to the requirements specified in EN 50128:2011[2]:

1) The selection of the tools in classes T2 and T3 shall be justified. The justification shall include the identification of potential failures which can be injected into the tools output and the measures to avoid or handle such failures.

2) All tools in classes T2 and T3 shall have a specification or manual which clearly defines the behaviour of the tool and any instructions or constraints on its use.

These requirements necessitate in-depth analysis of these tools. If necessary, two independent sets of automation tools can be deployed or alternative tests can be performed prior to the release of signalling systems to avoid failures introduced by automatic testing tools.

6.2.2 Automatic Data Generation and Verification Tools

The engineering construction of signalling systems requires, first, compilation and generation of massive engineering data, second, testing and verification of these data, third, migration of these data to software and hardware systems and, fourth, testing of signalling systems. Input and verification of massive engineering data is not possible by manual means and with some simple tools, and it is essential to apply automatic data generation and verification tools. However, these tools belong to the category of tool class T3. According to the requirements of EN 50128: 2011, these tools should meet the same requirements as automatic testing tools as well as the following requirements [2]:

1) For each tool in class T3, evidence shall be available that the output of the tool conforms to the specification of the output or failures in the output are detected. Evidence may be based on the same steps necessary for a manual process as a replacement for the tool and an argument presented if these steps are replaced by alternatives (e. g. validation of the tool).

Most of these automatic data generation and verification tools are independently developed tools by signalling systems themselves. These tools require not only strict control over tool development but also extensive tests for verification purposes which should be supplemented by manual check if necessary, as well as ergodicity tests during subsequent system tests, to minimize data errors caused by development tools.

7 CONCLUSION

Faced with shortened construction period, supplies of signalling systems encounter the great challenge of improving the safety of signalling systems while meeting the requirements of employers. In this case, strict compliance with the requirements of the lifecycle specified in EN 50126: 1999 may have practical difficulties in producing favourable results, and it is up to suppliers of signalling systems to adopt appropriate response measures to pay special attention to the key links and exercise control over the greatest risks according to the actual conditions of engineering construction projects, to make it possible to bring a favourable situation and achieve the objectives of safety and efficiency. This paper proposes the measures for solving technical problems from the perspective of overall system design and risk analysis and for solving management problems from the perspective of agile development and automation tool utilization so as to maximize the safety of signalling systems under the precondition of improvement of efficiency.

8 REFERENCES

[1] EN50126:1999 Railway applications — the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[2] EN50128:2011 Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems

[3] The art of agile development, by James Shore and Shane Warden, Copyright © 2008 O'Reilly Media, Inc., Printed in the United States of America, Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472

[4] Pattern of agile practice adoption — the technical cluster, by Amr Elssamadisy, © 2007 C4Media Inc., C4Media, Publisher of InfoQ.com.

[5] EN50126-2:2007 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 ..Gao Guoliang...

of Company (if applicable) .. Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.

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

~~Insert Title ..~~How to Improve the Safety of Signalling Systems with a Shortened Construction Period in Engineering Construction Projects?

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: ....

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