Research on organization-level safety assurance system

CHEN Lei

(Beijing National Railway Design and Research Institute of Signal and Communication, Beijing, China)

Abstract: The safety culture, the safety organization structure, the project safety assurance work, the monitor on project safety work, and the key safety control points (the safety milestones) are the five key points of safety assurance system. This paper presents an organization-level safety assurance system for signalling systems, which combines mature European safety assurance concepts and best practices. Engineering practices show that the safety assurance system can be effectively applied to the safety management of R&D projects of signalling systems and system integration projects of the CTCS-3 signalling and communication systems of passenger dedicated lines in China.

Key words: safety management, safety assessment, safety assurance system,

1. Introduction

Safety is such a major issue in railway that passengers, customers, operators, and contractors are all concerned about. Today the trend in safety management is moving from accident driven and reactive approach into a proactive and goal setting approach. Safety assurance is a systematic and proactive way by adopting and implementing appropriate processes, procedures, tools, rules and methodologies throughout the life cycle of products, processes, systems and operations to gain confidence in integrity and correctness of safety.

Being the most important signalling system supplier and system integrator in China, Beijing National Railway Design and Research Institute of Signal and Communication (hereafter: CRSC) takes safety as its primary goal. With massive constructions of high-speed railway in China, complexity and novelty challenge the traditional way of safety management, and safety assurance has been paid more attention to than ever before. An organization-level Safety Assurance System (SAS) fitting for all safety-related R&D projects and system integration projects will greatly improve the safety management of CRSC in this fast developing environment.

This paper presents an organization-level SAS for signalling systems, which combines mature European safety assurance concepts and best practices. The following sections are focused on the five key points of SAS, which are the safety culture, the project safety organization structure, the project safety activities, the monitor on project safety work, and the key safety control points (the safety milestones).

2. Safety Culture

For an organization to deliver safety critical products and system integration services, an open and clear safety culture is essential. A good safety culture can make everyone aware of the importance of safety, continually improve safety and give the first priority to safety in all that they do.

The safety policy of CRSC is the best way to define and promote the organizational safety culture and a guiding principle of safety activities in daily work, which has been approved by the chief engineer. The headline of safety policy is described as “Safety is the life and commitment of CRSC”. In order to make each person to understand the meaning and the heart of the safety policy headline, there are detailed items to interpret why safety is the life of CRSC and what measures CRSC takes to fulfill the promise on safety.

The following item is an example of detailed safety policy: the dynamicity of the safety policy implies that any measure that may facilitate refining or improving the safety policy shall be welcomed and encouraged. This supportive safety culture can greatly motivate employees to pay more attention to safety and do innovation on safety technique and safety management.

A continuous training helps the stuff to form good safety attitudes to follow all safety process and never attempt to ignore safety problems. The safety training is specified for different attendees and is carried out periodically by safety organization of CRSC.

3. Project safety organizations and independence

Due to technical and managerial complexity of signalling products and projects, a large amount of work about safety techniques and safety management is needed. Now MOR of China has introduced the best practices of independent safety assessment for generic products and generic applications, and innovated system assessment for CTCS-3 signalling system integration projects. The supplier or the system integrator is required to provide enough safety evidence to the assessor, and prove that enough measures of quality and safety management and technical safety have been adopted to control the risks within an acceptable level. Therefore, the project safety organization is to be established, in order to complete the work as follows:

- Safety assurance for the project, mainly including: hazard analysis for all the system and subsystem levels at different phases of the project; management of the hazard log, safety requirements and safety-related application conditions; safety coordination of different system levels and different subcontractors; etc.
- Project safety monitoring, mainly including: regular and irregular safety audit; witness and sampling of project verifications and tests; safety validation at system level; internal safety assessment and safety milestone management inside the enterprise; etc.

Different persons with different independent requirements are needed to fulfill the above responsibilities. Based on these requirements, the SAS of CRSC specifies that the safety organization of a safety-related project should be set up according to the guidelines shown in the following figure.

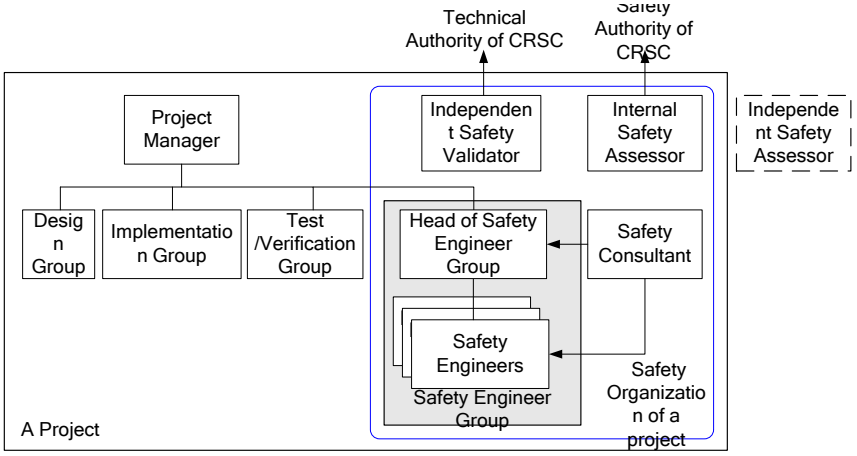

Figure1 Safety organization of a project

A typical configuration of safety organization of a project is: a safety engineer group with a head, a safety consultant, an independent safety validator and an internal independent safety assessor.

The safety engineer group is mainly responsible for organizing and coordinating related project persons to conduct safety assurance activities, safety coordination among different subsystems, collecting safety related evidence, coordinating with subcontractors and monitoring the safety assurance activities of subcontractors. It is important to note that only under the close cooperation with the project staff, can safety engineers take safety assurance activities effectively, so independence from the project is not required.

In order to help the safety engineer group working more efficiently and professionally, the safety organization usually has a specialist on safety assurance as a safety consultant, who will provide necessary directions for the activities of the safety engineer group.

The major duty of an independent safety validator is to validate the output of verification and test activities during different phases of the project, monitor the relevant quality and safety processes, ensure the independence between the test/verification activities and the design/implement activities; meanwhile, validate the whole project on the basis of tests and analysis. The validator is independent from the project and reports directly to the technical authority of CRSC. When a hazardous deviation in the safety assurance is found, the validator has the right to ask the technical authority to suspend the project and improve its safety status.

The responsibility of the internal safety assessor mainly includes: monitor the safety assurance activities by means of safety audit and witness; provide safety certificate at the safety milestone for the project to enter the next phase, after having audited and assessed the project safety evidence provided by the safety engineer group. The safety assessor is independent from the project, reports directly to the safety authority of CRSC, and takes control of the project safety assurance work by the way of providing safety certificate or not at the safety milestone.

4. The project major safety assurance activities

As an important part of the project activities, safety assurance activities are not necessary to be kept independent from the project activities. The safety engineer group is the organizer, coordinator, information collector and sometimes the leader of the safety assurance activities, while the implementation still relies on the project staff and relevant specialists.

Safety assurance activities are taken according to the requirements of the project safety plan and the SAS of CRSC. The safety plan is made at the early phase of the project based on the project plan, the project contract, and the SAS requirements, and is changed and updated according to the actual implement of the project.

On the basis of the start time and the time span, safety activities can be divided into continuous safety activities and discrete safety activities. These two types of activities are interrelated and interdependent, eventually make up of the project safety activities as a whole, and are recorded in the project safety case.

4.1 Discrete safety assurance activities

Discrete safety assurance activities refer to those will be done at specific phases of project lifecycle based on the project features. They are different in time spans and methods in the light of the project actual activities.

The safety engineer group should organize proper hazard analysis and risk mitigation activities for different lifecycle of the project according to the safety plan. The hazard analysis includes Preliminary Hazard Analysis (PHA) for early high level architecture of the system, System Hazard Analysis (SHA) for the system architecture, Sub-System Hazard Analysis (SSHA) for specific subsystems, Interface Hazard Analysis (IHA) for the physical and functional interfaces outside of and inside the analyzed component, and Operational & Support Hazard Analysis (O&SHA) for man-machine interfaces, engineering processes and maintenances.

Safety engineers take different types of hazard analysis when dealing with system levels or subsystems/subcontractors levels. The following table gives the usual hazard analysis types carried out in a signalling system integration project.

Table 1 Illustration of hazard analysis types in a system integration project

Levels being analysed	PHA	SHA	SSHA	IHA	O&SHA
System levels	√	√		√	√
Subsystems/ subcontractors levels			√	√	√

It should be noted that SHA of the system level is generally on the basis of the PHA result and conducted based on the hazard analysis result of the subsystem/subcontractor level. The risk caused by human participation or engineering process should be paid enough attention to because of the features of human activities, that is, to analyze the human factor through O&SHA.

Commonly, each hazard analysis concludes hazard identification, cause analysis, consequence analysis, and loss analysis. Hazard identification involves identification and ranking potential conditions for human injury or damage to the environment. Cause analysis involves establishing the primary causal factors which may give rise to a hazard and estimating the likelihood of occurrence of each hazard. Consequence analysis is to assess intermediate conditions and final consequences, which may arise from a hazard, and estimate the likelihood of accidents arising from each hazard. Loss analysis requires getting a credible loss estimate, so as to evaluate whether the newly-identified risk could be accepted.

HAZard and Operability Studies (HAZOP), brainstorming, Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and other methods can be chosen to do hazard analysis depending on different situations

Generally speaking, discrete safety assurance activities carried out by safety engineers include: to select a proper hazard analysis activity according to features of the object to be analysed at an appropriate project lifecycle, organize the project staff and related specialists, adopt proper hazard analysis methods, identify the relevant hazards, analyse the cause and the potential consequences and estimate the loss.

4.2 Continuous safety assurance activities

Continuous safety activities include hazard log maintenance, verification, safety validation, internal safety audit and internal safety assessment, which will be performed throughout the entire project lifecycle.

For a complex CTCS-3 system integration project or metro signalling system integration project, the safety engineer group should include safety engineers for different specialties or subsystems in line with the system structure, to maintain separately the hazard log of each subsystem and a hazard log of system level. For other projects, to maintain one overall hazard log of the project is a good practice. Hazards recorded in each subsystem or system hazard log mainly include hazards already known in contracts and standards, hazards identified in hazard analysis, hazard or safety-related application conditions introduced from outside and those found in generic products or generic applications. The safety engineer group is responsible to collect hazards, organize the related managers and technicians to review these hazards regularly or irregularly, decide and assess hazards, and determine whether to register a new hazard into a hazard log by reviewing.

Once a hazard is registered into a hazard log, the related persons must analyze the hazard and identify the hazard mitigating measures to reduce the frequency of hazard occurrence or/and the severity of the consequences. If hazards or safety related application conditions could be controlled within the project scope, corresponding safety requirements are to be generated, in order to request the project design and implementing team to control or mitigate the risk within an

acceptable level. If the risk can't be mitigated within the project, and other systems or operators outside the project are needed to deal with it, safety-related application conditions are to be made and sent to the responsibility party of the hazard by safety engineers in a written and traceable manner. Safety engineers should also keep trace of the risk handling by the responsibility party.

Working closely with the project staff, safety engineers continuously trace the implement of safety requirements and safety-related application conditions. When the related responsibility party confirms that requirements or application conditions have been effectively fulfilled and the hazard has been controlled or mitigated, safety engineers review the test report or verification report, in order to confirm whether the corresponding hazard has been closed, and then change the hazard status of the hazard log.

Before the formal delivery of the system, all the hazards recorded in the hazard log should been closed or under control, and the overall risk of the system is under the acceptable level.

5. Monitoring on project safety activities

Considering the complexity and novelty of the signalling system, the SAS of CRSC defines 3 types of monitoring, including internal project monitoring, safety validation and internal independent safety assessment. All these activities are to complete the following work:

- to confirm that the project has the capability to fulfill the requirement of project safety objective,
- to ensure the effective implementation of SAS of CRSC in the project, and
- to ensure the sustained compliance of the project with the SAS of CRSCD and related safety standards.

The following figure explains the relationship between safety assurance monitoring and the safety-related project.

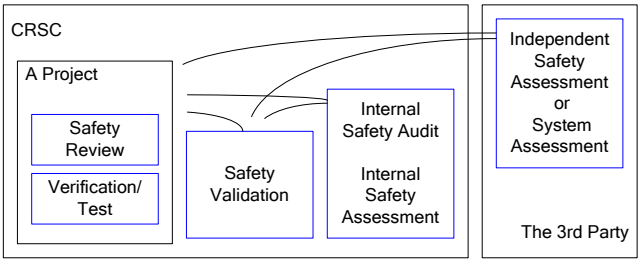

Figure 2 Illustration of the project safety assurance monitoring

The internal project monitoring of safety assurance activities mainly includes safety review and verification/test. Safety review is a special kind of review. According to the project safety plan, safety engineers organize related managers and key staff related to the project safety, to review documents and other work by means of meeting and discussion. The review mainly concerns aspects affecting the safety of project. Safety verification is to determine, in each phase of the project lifecycle and by the way of test and analysis, whether the requirements at the current phase meet the output of the previous phase and the output of the current phase realizes the requirements of the phase. Safety verification should be carried out by qualified people independent from the work to be verified.

Independent safety validation is performed by independent safety validator. It is a kind of activity to demonstrate that the product fulfills requirements in all respects through test and analysis. It mainly consists of two parts: validation of the results of each lifecycle and final output, and validation of the project implementing process.

Internal independent safety assessment monitoring includes safety audit and safety assessment and is completed by internal safety assessor. Safety audit is to audit the evidence that the project is following the safety plan. Safety assessment is focused on the residual risk of the project, that is, to audit the evidence indicating that the safety assurance work can make the project meet safety requirements. Internal independent safety assessment monitoring usually uses the methods of auditing project documents, interviews with the project stuff, and witnessing or participating the project test and analysis activities.

6. Safety milestones

Safety milestone is an indispensable part of the project safety management and an important safety-related event. Safety milestone generally doesn't occupy any resources. It is a time point in project lifecycle, usually related with the submission of deliverables.

For signalling R&D projects, the deliverables are generic products or generic applications. These projects always are self-investigated ones. The users of these deliverables are engineering group of CRSC or the system integration projects. So there is only one safety milestone for these types of projects. The safety milestone is the permission to system delivery. At this milestone, the project must provide evidences that the project has followed the safety plan and the risk is at an acceptable level.

For an engineering project or a system integration project, the SAS of CRSC sets 3 safety milestones as follows, to control the project safety activities:

- Safety milestone 1: permission to field test;
- Safety milestone 2: permission to trial operation; and
- Safety milestone 3: permission to commercial operation.

The aim of setting these 3 safety milestones is to ensure that the whole system is ready for the following work before the project enters the phase of field test, trail operation or commercial operation by methods of audit and assessment of safety-related evidence. Meanwhile, within the safety certificate issued by the corresponding safety milestone, the internal safety assessor also needs to define all safety restrictions for the following project work according to safety evidences of previous activities, such as functional limitations during the system operation, special operation processes and specific inspect methods and processes, in order to make sure that the following activities won't introduce hazard which will cause accidents or casualties.

At safety milestones, if the internal safety assessor concludes that the project is not ready for the next phase, he should document clearly the assessment conclusion in the phase safety assessment report and has the right not to give safety certificate for the particular safety milestone. Safety authority of CRSC will decide whether to allow the project to enter the next phase according to the assessor's opinion.

7. Conclusion

An organization-level SAS is essential for top Chinese signalling product suppliers and system integrators like CRSC. The SAS of CRSC combines European safety assurance concepts and best practices. Engineering practices show that the SAS can be effectively applied to the safety management of R&D projects and system integration projects of the CTCS-3 systems of passenger dedicated lines in China.