Fail-Safety Requirement for Railway Signalling Equipment

G Pavan Kumar, IRSSE, Director(Signal), RDSO

Abstract

This article defines requirements for acceptance and approval of safety related electronic systems in the Railway Signalling field. Safety related electronic systems for signalling include hardware and software aspects. This article is concerned with the evidence to be presented for the acceptance of safety related systems, it specifies those life-cycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. Safety justification for the whole of the life-cycle is therefore required.

1 Introduction

This article is applicable to safety-related electronic systems (including sub-systems and equipment) for railway signalling applications. This article is intended to apply to all safety-related railway signalling systems/sub-system/equipment. However, the hazard analysis and risk assessment processes are necessary for all railway signalling systems/sub-systems/equipment, in order to identify any safety requirements. If analysis reveals that no safety requirements exist (i.e.: that the situation is non-safety related), and provided the conclusion is not revised as a consequence of later changes, this safety analysis ceases to be applicable.

This article applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of complete signalling systems, and also to individual sub-systems and equipment within the complete system.

It should also be applied, as far as reasonably practicable, to general-purpose or industrial equipment (e.g.: power supplies, signals, etc.), which is procured for use as part of a safety-related signalling system. As a minimum, evidence shall be provided in such cases to demonstrate either that the equipment is not relied on for safety, or that the equipment can be relied on for those functions which relate to safety.

2 Origin of Rail Safety

The objective of Rail Safety is to provide for safe Rail Operations. The Rail Safety centers on the safety of rail operations, management of safety risks, continuous improvement in rail safety management and public confidence in the safety of rail transport. It contains a number of overarching policy principles relating to shared responsibility, accountability for managing safety risks, integrated risk management, enforcement, transparency and consistency.

Compliance to Rail Safety is an essential part and hence the systems, sub-systems which form part of Railway Signalling Applications have to be cleared for Fail-Safety.

3 Safety Acceptance & Approval

3.1 Safety Case

The Safety Case contains the documented safety evidence for the system/sub- system/equipment and shall be structured as shown in the following chart. The safety case shall discuss about evidence of quality management, safety management, functional safety and technical safety.

3.2 Evidence of Quality Management

The purpose of the quality management system is to minimize the incidence of human errors at each stage in the lifecycle and thus to reduce the risk of systematic faults in the system, sub-system or equipment. Typical example is shown in the Figure 2.

3.3 Evidence of Safety Management

The second condition for safety acceptance which shall be satisfied is that the safety of the system, subsystem or equipment has been, and shall continue to be, managed by means of an effective safety management process, which should be consistent with the management process for RAMS. The purpose of this

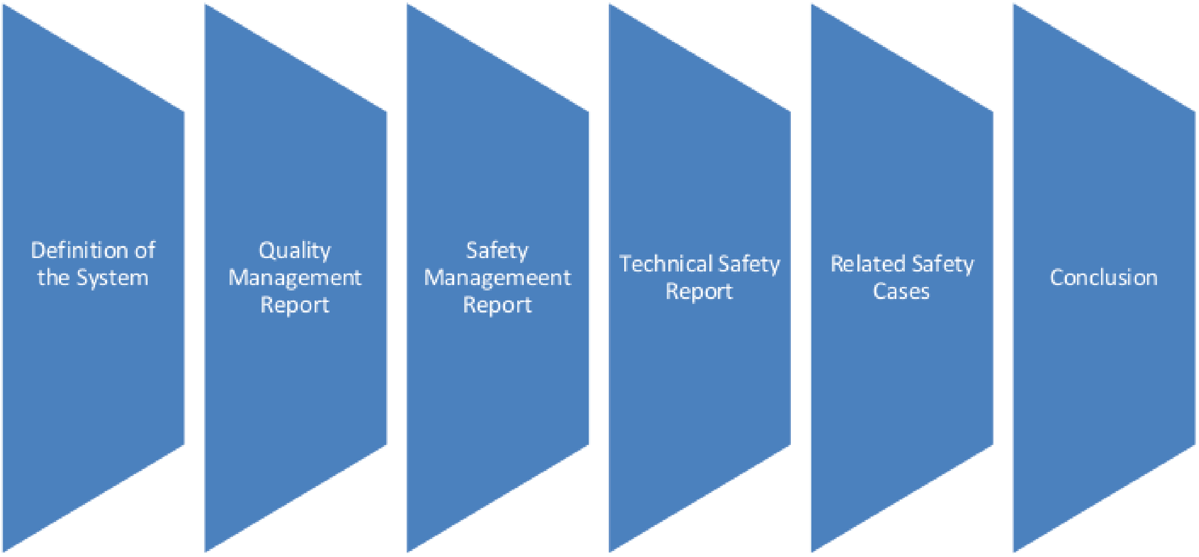


Figure 1: Safety Case

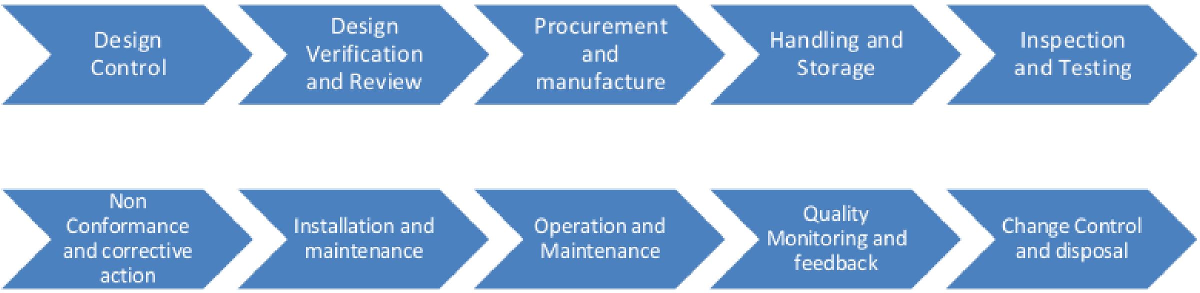

Design Control
Design Verification and Review
Procurement and manufacture
Handling and Storage
Inspection and Testing
Non Conformance and corrective action
Installation and maintenance
Operation and Maintenance
Quality Monitoring and feedback
Change Control and disposal

Figure 2: Quality Management Evidence

process is to further reduce the incidence of safety-related related human errors throughout the lifecycle, and thus minimize the residual risk of safety-related systematic faults. The elements of the safety management process are briefly summarized in the Figure3.

3.4 Evidence of Functional & Technical Safety

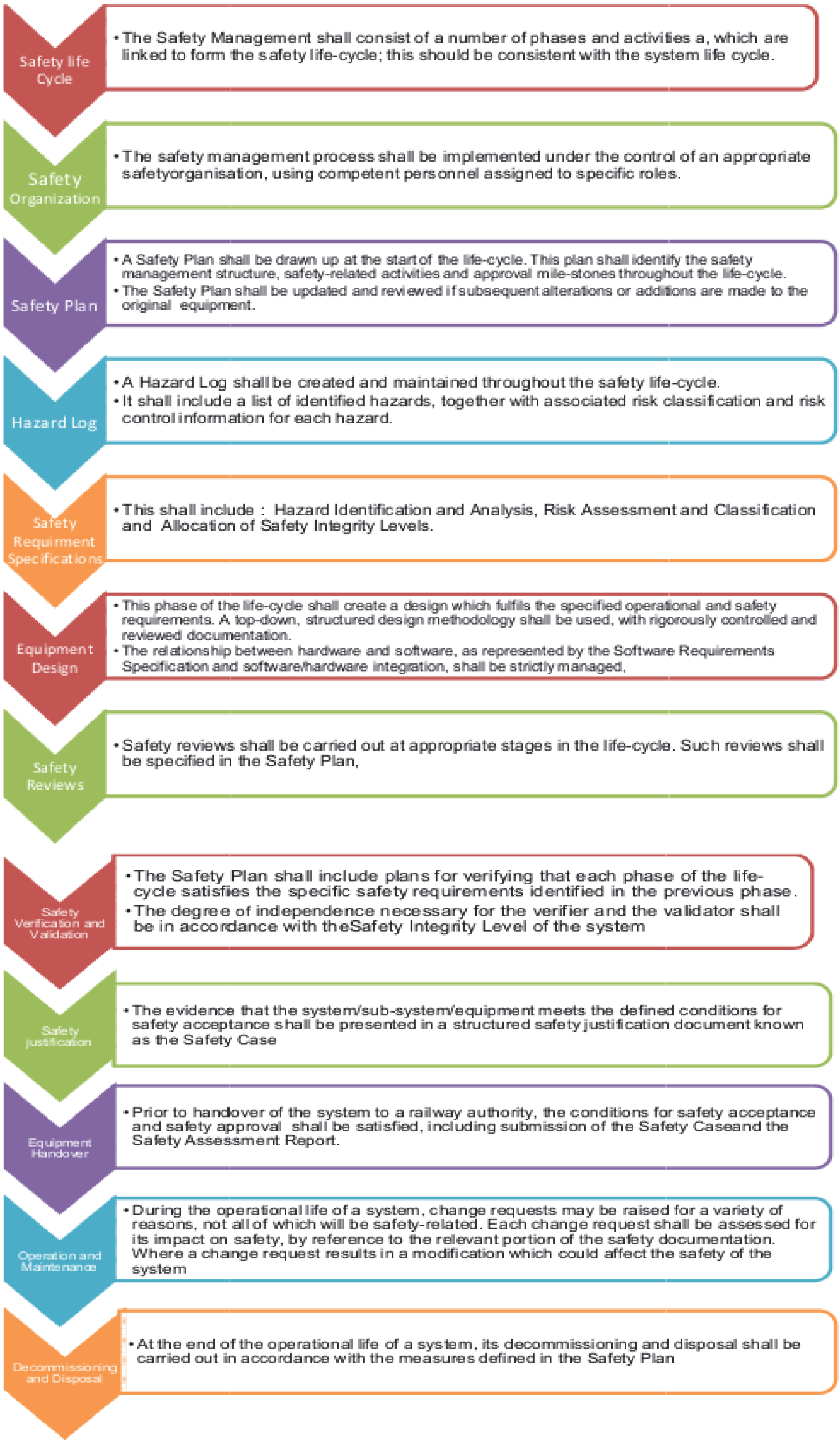
In addition to the evidence of quality and safety management, described above, a third condition shall be satisfied before a system/ sub-system/ sub-system/ equipment system/equipment can be accepted as adequately safe for its intended application. This consists of technical evidence for the safety of the design, which shall be documented in the Technical Safety Report.

3.5 Categorization of Risk

The Tolerable Hazard Rates (THR) is a target measure with respect to both systematic and random failure of safety integrity in a system. The following steps are to be followed for carrying out risk analysis.

Safety integrity is specified as one of four discrete levels. Level 4 has the highest level of safety integrity; level 1 has the lowest. Level 0 is used to indicate that there are no safety requirements. A SIL should address qualitative appreciation of factors such as quality and safety management and technical safety conditions.

This safety relies both on adequate measures to avoid or tolerate faults (as safeguards against systematic failure) and on adequate measures to control random failures. Measures against both causes of failure should be balanced in order to achieve the optimum safety performance of a system. To achieve this the concept of Safety Integrity Levels (SIL) is used. SILs



Safety life Cycle

- The Safety Management shall consist of a number of phases and activities a, which are linked to form the safety life-cycle; this should be consistent with the system life cycle.

Safety Organization

- The safety management process shall be implemented under the control of an appropriate safetyorganisation, using competent personnel assigned to specific roles.

Safety Plan

- A Safety Plan shall be drawn up at the start of the life-cycle. This plan shall identify the safety management structure, safety-related activities and approval mile-stones throughout the life-cycle.
- The Safety Plan shall be updated and reviewed if subsequent alterations or additions are made to the original equipment.

Hazard Log

- A Hazard Log shall be created and maintained throughout the safety life-cycle.
- It shall include a list of identified hazards, together with associated risk classification and risk control information for each hazard.

Safety Requirment Specifications

- This shall include : Hazard Identification and Analysis, Risk Assessment and Classification and Allocation of Safety Integrity Levels.

Equipment Design

- This phase of the life-cycle shall create a design which fulfils the specified operational and safety requirements. A top-down, structured design methodology shall be used, with rigorously controlled and reviewed documentation.
- The relationship between hardware and software, as represented by the Software Requirements Specification and software/hardware integration, shall be strictly managed,

Safety Reviews

- Safety reviews shall be carried out at appropriate stages in the life-cycle. Such reviews shall be specified in the Safety Plan,

Safety Verification and Validation

- The Safety Plan shall include plans for verifying that each phase of the life-cycle satisfies the specific safety requirements identified in the previous phase.
- The degree of independence necessary for the verifier and the validator shall be in accordance with theSafety Integrity Level of the system

Safety justification

- The evidence that the system/sub-system/equipment meets the defined conditions for safety acceptance shall be presented in a structured safety justification document known as the Safety Case

Equipment Handover

- Prior to handover of the system to a railway authority, the conditions for safety acceptance and safety approval shall be satisfied, including submission of the Safety Caseand the Safety Assessment Report.

Operation and Maintenance

- During the operational life of a system, change requests may be raised for a variety of reasons, not all of which will be safety-related. Each change request shall be assessed for its impact on safety, by reference to the relevant portion of the safety documentation. Where a change request results in a modification which could affect the safety of the system

Decommissioning and Disposal

- At the end of the operational life of a system, its decommissioning and disposal shall be carried out in accordance with the measures defined in the Safety Plan

Figure 3: Safety Management Evidence

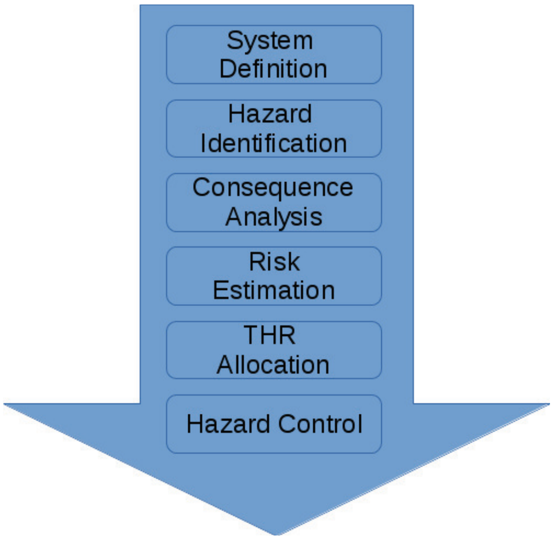


Figure 4: Risk Categorization

are used as a means of matching the qualitative approaches (to avoid systematic failures) with the quantitative approach (to control random failures), as it is not feasible to quantify systematic failures. This balance is expressed in a table, which consists of a list of Safety Integrity Levels 0, 1, 2, 3, 4 and a list of corresponding intervals or bands for tolerable hazard rates $I_0, ..., I_4$.

The SIL table is applicable to safety-related functions or sub-systems implementing one or more of these functions. Having followed the measures and methods required for SIL x there is no requirement to consider the systematic failures when demonstrating the THR is achieved. The SIL table identifies the required SIL for the safety-related function from the Tolerable Hazard Rate (THR). Thus if the THR for a function F has been derived by a quantitative method the required SIL shall be determined by the use of the following table.

THR / hour /function	**SIL**
$10^{-9} \geq 10^{-8}$	4
$10^{-8} \geq 10^{-7}$	3
$10^{-7} \geq 10^{-6}$	2
$10^{-6} \geq 10^{-5}$	1

4 Conclusion

The above article is only introductory in nature. Further techniques and measures for safety related electronic systems used for signalling for the avoidance of systematic faults and to control random and systematic faults, safety planning and quality assurance activities, System Requirements Specification, Architecture of System, Design features such as protection against operating errors, single fault in discrete components/ICs, physical independence within safety related architecture, detection of single faults, relation of safe state, Dynamic fault detection, measures against temperature and voltage variations etc., Failure & Hazard Analysis using methods such as preliminary hazard analysis, Fault tree analysis, Markov diagrams, FMECA, HAZOP etc., Verification and Validation of the system design are to be employed with respect to SIL for assessing the safety integrity of an electronic system used for Railway Signalling.

The information / views expressed in this paper is of the author and are based on his experience on Indian Railways. Comments / observations may be sent to the author at dig5rdso@gmail.com.

G Pavan Kumar, currently working as Director(Signal), RDSO, is a seasoned professional with 15+ years rich experience in Research, Design, Development, Standardization, Project Management (installation, testing commissioning) of Train Collision Avoidance System (An indigenoused Automatic Protection System for Indian Railways), Train Protection Warning Systems, FogPASS, Electronic interlocking system, MSDAC of Thales Make, Panel Interlocking, Electrically Operated Lifting Barriers, Approach warning to LC Gates,Optical Fibre system. He has also been associated with several innovations such as OFC based IBS, PPTC fuses, GPS based GSM Signal Strength Measurement, Remote Work Site Management System, Centralized voice logging for LC Gate communication, Centralized train information display and announcement system etc., that ahve are inducted into Indian Railways.