

Chapter 9

Safety Requirements

Your organisation must set safety requirements for any change, to reduce the risk associated with the change to an acceptable level.

9.1 Guidance from volume 1

Safety requirements are requirements that should be met to make sure that the safety risk presented by a change is reduced to an acceptable level. Safety requirements may specify:

- features or functions of the change, including any which help people avoid dangerous mistakes,
- what the change must not do to ensure safety,
- environmental conditions under which the change must operate to stay safe,
- targets for carrying out a function reliably, or reliably avoiding a dangerous state,
- features of the design and build processes, and
- operational procedures and restrictions.

You will set some safety requirements to meet regulations or standards. Others may arise when you identify hazards and assess and reduce risk.

9.2 Background

A project carrying out safety-related work should identify the hazards and accidents that may result from the work, assess the risk associated with these, reduce the risk ALARP and set Safety Requirements to ensure this level of risk is met. There is a legal requirement to assess the risks involved in safety-related work. Safety Requirements should also be consistent with the operator's stated targets.

Safety Requirements may be quantitative or qualitative. Good engineering practice for meeting integrity requirements for components susceptible to systematic failure is to use Safety Integrity Levels (SILs). SILs are described in section 9.6 below.

The activity of establishing safety requirements follows and builds on the work described in the previous chapter. If you have not already done so, you should read the Background section of the previous chapter as it also provides important background for this chapter.

The Safety Requirements Specification consolidates information provided by these activities into specific requirements, which form the basis against which the safety of the system is tested and assessed.

The activity of establishing Safety Requirements is iterative to reflect the iterative nature of safety analysis.

This chapter is written for people writing or reviewing Safety Requirements.

9.3 Reducing risk

The following is a widely accepted order of precedence for reducing risk

- 1 Respecify or redesign to eliminate hazards or reduce their likelihood.
- 2 Reduce risk in the design, by adding safety features.
- 3 Reduce risk by adding warning devices.
- 4 Reduce risk through procedures and training.
- 5 Reduce risk by adding warning signs and notices

For any given hazard you should first seek to set Safety Requirements to eliminate it. Only where this is not possible should you proceed to set Safety Requirements on the design of the system. And only when all reasonably practicable risk reduction has been accomplished on the design should you consider procedures and training as risk reduction options.

9.4 Overview of process

Setting safety targets is normally done by working from a fault tree (or similar representation of cause and effect logic) and the event probabilities to:

- a) derive numerical accident targets which conform to the ALARP principle, that is either they are tolerable and further risk reduction is not reasonably practicable or they are negligible;
- b) derive hazard occurrence rate and/or unavailability targets which are consistent with (a);
- c) (if systematic failure modes exist) relate hazards to system functions and derive SILs for the system functions that are consistent with (b).

The requirements may be apportioned further to sub-systems of the hierarchy and aligned with the system design. In general, systematic targets should not be set below sub-system function level. Refer to IEC 61508 [F.14] or ENV 50129:1998 [F.13] for further guidance on this decomposition.

Any functional requirements on the system or equipment that are necessary to reduce risk to an acceptable level should be incorporated as qualitative safety requirements.

The analyst may set other qualitative safety requirements such as conformance to external standards and should do so whenever:

- such conformance is assumed in the calculation of safety targets; or
- such conformance is otherwise required to reduce risks as low as reasonably practicable.

If the seven-step process described in chapter 8 is being used, then some requirements will arise from the fifth step, Options Analysis. However requirements may also arise from relevant regulations, standards and codes of practice.

9.5 Apportionment of random failure targets

It is not generally necessary to descend the fault tree fully, that is to set targets for base events. The analyst should set targets at a level coincident with the hierarchical breakdown of the system being developed.

9.6 Assignment of Safety Integrity Levels

There are well-established techniques for assessing and controlling random failures but practice is not as advanced in the treatment of systematic failures. Current best practice is to define a number of Safety Integrity Levels (SILs) representing different levels of rigour in the development process and to relate these to approximate probability targets.

Five levels are defined. There are four safety-related SILs, ranging from SIL 4, the most stringent, to SIL 1, the least stringent. Functions which are not relied upon at all to control risk may be described as having SIL 0. Each level is populated with increasingly stringent processes and techniques.

Systematic failures are of particular concern in software-based systems and have generally been applied to these sort of systems, and, in particular to the software within them. However hardware can exhibit systematic failures and SILs are applicable to them as well.

Each integrity level is associated with a target probability of failure. One widely accepted association is shown in Table 9-1, which is derived from IEC 61508 [F.14]. The Low Demand column should be used if demands are expected to occur:

- no more than once per year, and
- no more than twice as often as the system is checked out.

Otherwise use the Continuous/High Demand column.

Low Demand Mode of Operation (probability of failure on demand)	Continuous / High Demand mode of operation (Dangerous failure rate per year)	Safety Integrity Level
$\geq 10^{-5}$ to 10^{-4}	$\geq 10^{-5}$ to 10^{-4}	4
$\geq 10^{-4}$ to 10^{-3}	$\geq 10^{-4}$ to 10^{-3}	3
$\geq 10^{-3}$ to 10^{-2}	$\geq 10^{-3}$ to 10^{-2}	2
$\geq 10^{-2}$ to 10^{-1}	$\geq 10^{-2}$ to 10^{-1}	1

Table 9-1 - Safety Integrity Levels

Target probabilities of failure for systematic functions should be set to achieve an acceptable level of risk for the overall system.

Each sub-system within the overall system will generally take the maximum SIL of all the functions that it implements. The components within that sub-system may then be allocated SILs according to the guidance given in section 9.7.

However, if it can be clearly demonstrated that a sub-system's functions are wholly independent of each other (that is, the immediate effects of a function's failure are restricted to that function), then these functions (or groups of functions) may be considered as sub-systems in themselves and assigned SILs accordingly. In this way, the apportionment of SILs need not be confined to physically separate units.

It is very difficult to prove functional independence within a sub-system and so it is important to take care in assigning functions to sub-systems. If possible, functions with differing SILs should be segregated either physically or logically.

Once the SIL for a sub-system has been established then appropriate techniques to develop the sub-system to that level can be established by reference to tables in standards including ENV 50129:1998 [F.13], IEC 61508 [F.14] and DEF-STANs 00-54 [F.15] and 00-55 [F.16].

9.7 Apportionment of Safety Integrity Level

Having set a SIL for a function to achieve the necessary probability target, the analyst may need to apportion this between lower level functions. By default the lower-level functions will inherit the highest SIL of the top-level functions that they support.

However, it is possible to use a redundant architecture to build high SIL systems from sub-systems of lower SIL by building in back-up or protection functions.

If the architecture ensures that a top-level function can only fail if both a *main* and *backup* function fail and the two functions are independent, then the SIL of the top function may sometimes be higher than that of the main or backup function.

In some cases, there may also be a *combinator* function (for instance a voting scheme) which combines the results of the main and backup functions.

Table 9-2 (derived from DEF-STAN 00-56 [F.4]) shows some combinations which are generally regarded as valid, provided that:

- the lower level functions are physically separated and built using different design principles, and
- the combinator suppresses any hazard for any failure of one lower level function.

Note that the combinator always inherits the top level SIL.

The table should not be repeatedly applied to allow a SIL 4 system, say, to be made of many SIL 1 systems.

Top Level SIL	SIL of Lower Level Function		Combinator (if present)
	Main	Other	
SIL 4	SIL 4	None	None
	SIL 4	SIL 2	SIL 4
	SIL 3	SIL 3	SIL 4
SIL 3	SIL 3	None	None
	SIL 3	SIL 1	SIL 3
	SIL 2	SIL 2	SIL 3
SIL 2	SIL 2	None	None
	SIL 1	SIL 1	SIL 2
SIL 1	SIL 1	None	None

Table 9-2 - Apportionment of Safety Integrity Levels

9.8 Software Safety Requirements

This guidance is applicable to any railway system containing software, including embedded systems such as programmable logic controllers.

For programmable systems, it is normal to derive a Software Requirements Specification (although other titles may be used). This should define the functions that the software must perform which, taken together with the capabilities of the hardware components, will allow the overall system to meet its requirements.

In just the same way as safety requirements are set at the system level and form part of the overall system requirements, it is usual to establish a Software Safety Requirements Specification, either as a subset of the Software Requirements Specification or as a separate document.

The software safety requirements will normally include requirements for features which can tolerate faults as well as requirements for dependability of the software.

prEN 50128 provides guidance on fault-tolerant features.

Dependability should be treated by specifying the SIL of the software. This will be the same as the SIL for the system unless it has been explicitly apportioned as described in the previous section.

Guidance on the development of software for safety-related railway applications can be found in prEN 50128 [F.17] which also describes techniques appropriate to each SIL.

Evidence of validation of the software against its requirements should be produced. If prEN 50128 is used then this is documented in a software assessment report and a software validation report. This evidence will form an important part of the overall system Safety Case.

9.9 The Safety Requirements Specification

The following structure is recommended for a Safety Requirements Specification:

- Introduction.
- Background. A summary of the system and project, including configuration information where appropriate.
- Statement of Safety Requirements. A list of all Safety Requirements.
- Justification of Safety Requirements. The assumptions and calculations supporting the statement of Safety Requirements, including a record of the techniques employed, the manner in which they were applied.
- Reference to safety documentation. References to all documents used together with version numbers.

Other effective formats are in common use. The Safety Requirements Specification does not need to be a separate document. and is sometimes combined with other documents. A Safety Requirements Specification will, however, normally include at least as much information as provided in the structure above.

The Safety Requirements Specification should be submitted to the Safety Authority for endorsement.

9.10 Related Guidance

Chapter 8 provides guidance on the safety analysis processes which should be carried out before setting safety requirements.