

Appendix A

Glossary

This glossary defines the specialised terms used in this volume. Volume 1 uses simpler and more restricted terminology which is introduced in the volume itself.

We have tried to minimise inconsistencies between the terminology used in this volume and that used in other principal sources of information for railway ESM. However it is not possible to eliminate inconsistency entirely because there is variation in usage between these other sources.

accident	An unintended event or series of events that results in harm. <i>Note: this broadly corresponds to a 'hazardous event' in the Railtrack S&SD Safety Risk Model.</i>
accident likelihood	The likelihood of an accident occurring. May be expressed as numeric probability or frequency or as a category.
accident sequence	A potential progression of events that result in an accident.
Accident Sequence Analysis	Derivation of the sequence of events which lead from hazard to accident.
accident severity	A measure of amount of harm. May be expressed as a financial value or as a category.
accident trigger	A condition or event which is required for a hazard to give rise to an accident. <i>Note: this broadly corresponds to a 'precursor (consequence)' in the Railtrack S&SD Safety Risk Model.</i>
ALARP principle	The principle that no risk in the tolerability region can be accepted unless reduced 'As Low As Reasonably Practicable'. <i>See chapter 8.</i>
apportioned risk benchmark	A target for the average individual probability of fatality per annum experienced by a group, arising from a given aspect of the railway's operations

authorisation	The formal permission to introduce a system, product or other change into the railway within specified application constraints.
barrier	(In the context of risk assessment) anything which may act to prevent a hazard giving rise to an accident. Barriers may be physical, procedural or circumstantial
broadly acceptable risk	A risk which is generally acceptable without further reduction.
causal factor	Any event, state or other factor which might contribute to the occurrence of a hazard.
code of practice	A statement of best practice whose use is not mandated by the issuing authority.
compliance	A demonstration that a characteristic or property of a system, product or other change satisfies the stated requirements.
consequence	The results arising from the addition of energy, or exposure, to a hazard. These may range from benign results to accidents. Several consequences may be associated with a hazard.
Data Recording and Corrective Action System (DRACAS)	<p>A closed-loop system for ensuring that failures and other incidents are thoroughly analysed and that any necessary corrective action, particularly if it affects safety, is identified and carried through.</p> <p><i>See appendix E.</i></p>
endorse	Approve a document, piece of equipment, etc, as being fit for purpose.
Engineering Safety Management (ESM)	<p>The activities involved in making a system, product or other change safe and showing that it is safe.</p> <p><i>Note: despite the name, ESM is not performed by engineers alone and is applicable to changes that involve more than just engineering.</i></p>
Engineering Safety Management System	A systematic and documented approach to ESM.
error	A deviation from the intended design which could result in unintended system behaviour or failure.
event	A significant happening that may originate in the system, product or other change or its domain.
Event Tree Analysis	A method of illustrating the intermediate and final outcomes which may arise after the occurrence of a selected initial event.
failure	A deviation from the specified performance of a system, product or other change. A failure is the consequence of a fault or error.

fault	A fault is a defect in a system, product or other change which may cause an error.
Fault Tree Analysis	A method for representing the logical combinations of various states which lead to a particular outcome (top event). <i>See appendix E.</i>
FMEA	Failure Mode and Effects Analysis. A process for hazard identification where all known failure modes of components or features of a system, are considered in turn and undesired outcomes are noted. <i>See appendix E.</i>
FMECA	Failure Mode, Effects and Criticality Analysis. An extension to FMEA in which the criticality of the effects is also assessed. <i>See appendix E.</i>
group	Group of people exposed to railway operations. Such as: employees (trackside staff), passengers and the public.
handover	Used to mean the process of handing over part of the railway to the infrastructure controller so that it can put into or back into service. <i>Note: this process is referred to as 'Handback' within Railtrack.</i>
hazard	A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product. <i>Note: this broadly corresponds to a 'precursor (cause)' in the Railtrack S&SD Safety Risk Model</i>
Hazard Analysis Report	A document identifying the potential hazards and accidents of a system, product or other change and analysing the causal factors of the hazards.
Hazard Log	A document which records details of hazards and potential accidents identified during safety analyses of a system, product or other change and logs safety documentation produced.
HAZOP	Hazard and Operability Study. A study carried out by application of guide words to identify all deviations from the design intent with undesired effects for safety or operability. <i>See DEF STAN 00-58 [F.19]</i>
incident	Unplanned, uncontrolled event, which under different circumstances could have resulted in an accident.

individual risk	The individual risk experienced by a person, is their probability of fatality per unit time, usually per year, as a result of a hazard in a specified system.
intolerable risk	A risk which cannot be accepted and must be reduced.
loss	A measure of harm to people.
potential equivalent fatality	A convention for aggregating harm to people by regarding major and minor injuries as being equivalent to a certain fraction of a fatality.
Project Manager	The person in overall control of a project. Also responsible for the safety of the products produced during the project, although may delegate this role to a Project Safety Manager (but remains accountable).
Project Safety Manager	The person responsible for safety on a project and for producing all safety-related documentation.
railway operator	An infrastructure controller, train operator or station operator
random hardware failure	Failures resulting from one or more of the possible degradation mechanisms in the hardware. These failures occur at predictable rates but at unpredictable (that is random) times.
reliability	The probability that an item can perform a required function under given conditions for a given time interval.
remit	Terms of reference, in particular for a Safety Audit or Safety Assessment
risk	Combination of the likelihood of occurrence of harm and the severity of that harm.
risk analysis	A structured process which identifies both the likelihood and extent of adverse consequences arising from a given activity of facility.
risk assessment	The combination of risk analysis and risk evaluation.
risk assessment report	A document containing an analysis of the risks of accidents occurring.
risk benchmark	A target for the average individual probability of fatality per annum experienced by a group, for all the railway's operations
risk classification	A scheme to classify risk according to likelihood of harm occurring and the severity of the harm.
risk evaluation	The appraisal of the significance of a given quantitative (or, where applicable, qualitative) measure of risk.

safety	Freedom from unacceptable risk. <i>Criteria for accepting risk are described in chapter 8.</i>
safety analysis	A general term encompassing identifying hazards, analysing hazards and assessing risk.
safety approval	The process by which a Safety Authority grants its approval for a proposed change to the railway to proceed.
Safety Assessment	The process of analysis to determine whether a system, product or other change to the railway has met its Safety Requirements and that the Safety Requirements are adequate.
Safety Assessment Remit	A form capturing a request for a Safety Assessment and the terms of reference.
Safety Assessment Report	A report on the activity carried out to check that the Safety Requirements are being met on a project.
Safety Assessor	The person who carries out Safety Assessments.
Safety Audit	An activity to check and ensure that a project is being run according to its Safety Plan. It will also address the adequacy of the Safety Plan.
Safety Audit Remit	A form capturing a request for a Safety Audit and the terms of reference.
Safety Audit Report	A report on the activity carried out to check that the Safety Plan and safety management procedures are being carried out on a project.
Safety Auditor	The person appointed to carry out Safety Audits on a project.
Safety Authority	The body responsible for certifying that the safety-related system, product or other change is safe, fit for service and complies with all statutory and regulatory requirements.
Safety Case	A formal presentation of evidence, arguments and assumptions aimed at providing assurance that a system, product or other change to the railway has met its Safety Requirements and that the Safety Requirements are adequate. <i>Early issues may present analysis and assessment information, plans and requirements.</i>
Safety Certificate	A certificate authorising system, product or other change for use. Usually refers to third-party equipment.
safety control	A quality control with the potential to reveal hazardous faults.
Safety Engineering	The application of technical methods to ensure achievement of the Safety Requirements.

Safety Integrity	The likelihood of a system, product or other change satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.
Safety Integrity Level (SIL)	Discrete level (1 out of a possible 5) for specifying the safety integrity requirements of the safety functions to be allocated to a system, product or component, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 0 is reserved for functions which are not relied upon at all to control risk.
safety lifecycle	The additional series of ESM activities carried out in conjunction with the system lifecycle for safety-related systems.
Safety Plan	A document detailing the activities to be carried out, and responsibilities of people to ensure the safety of work being carried out.
Safety Planning	An activity to define the activities to be carried out and the staff responsibilities to be assigned to ensure the safety of work to be carried out. Results in the preparation of a Safety Plan.
Safety Records Log	A reference to every safety document produced and used by a project.
safety-related	An item is safety-related if any of its features or capabilities have the potential to contribute to or prevent an accident.
Safety Requirements Specification	Specification of the requirements that a product, system or change to the railway must satisfy in order to be judged safe.
safety standard	A document which establishes criteria or requirements by which the safety of products or processes may be assessed objectively.
safety value	The monetary value of reductions in safety losses likely to be achieved by implementation of a risk mitigation option.
severity	<i>See accident severity</i>
standard	An authorised document, including specification, procedure, instruction, directive, rule or regulation, which sets mandatory requirements for use in service.
system supplier	Any organisation supplying systems or products to be used on the railway.
systematic failure	Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

tolerability region	A region of risk which is neither high enough to be unacceptable nor low enough to be broadly acceptable. Risks in this region must be reduced ALARP (see ALARP principle)
upper limit of tolerability	A measure of the average individual risk of fatality per annum, defined for each group, and representing the boundary between tolerable and intolerable risk for the group.
Value of Preventing a Fatality (VPF)	A defined monetary figure which is used to indicate what it is regarded as reasonably practicable to spend in the expectation of preventing a single fatality.

This page left intentionally blank