A Lean approach to CENELEC compliance

Dr. Andrew Hussey

Ansaldo STS Australia
U2/93 Francisco St, Belmont, WA

andrew.hussey@ansaldo-sts.com.au

Abstract

Safety-critical System development is an activity that usually involves multiple organisations that must co-ordinate and communicate to deliver the required safe System function. Without adequate and complete communication of information between organisations, safety hazards and corresponding safety requirements may be overlooked – particularly during early lifecycle activities, resulting in late lifecycle rework, which is both costly and time consuming.

This paper presents the outcomes of experiences in working in an industrial context with the CENELEC standards EN50126 and EN50129. We examine techniques for balancing customer and supplier obligations under CENELEC, as well as an integrated approach to communicating information between customer and supplier to ensure overall compliance with the CENELEC standards as well as minimisation of risk of overlooked safety hazards and requirements. The methods applied are presented in the context of a Lean management framework, enabling a trace to be made from the proposed methods to the overall organisational values and principles.

The paper considers the use of information abstraction as a technique for managing customer and supplier communication of safety hazards and requirements. By defining and agreeing on the level of abstraction of information passed between customer and supplier, the dialogue between customer and supplier is formalised, communication efficiencies are achieved and an integrated customer-oriented outcome is realised.

Keywords: Customer-oriented, Integrated, CENELEC, Information Abstraction, Lean

1 Introduction

The CENELEC standards EN50126 [EN50126] and EN50129 [EN50129] provide a framework for hazard analysis and Safety Case development. These standards map out the activities that an organisation needs to perform so as to derive the hazards for a system, mitigate those hazards and develop and document a safety argument that can be presented to others to explain how the hazards have been managed so as to reduce risk to acceptable levels.

The EN50126 process is simple to apply and works well when a single organisation is responsible for the work that is to be undertaken, but becomes more complex to apply when work is to be carried out by a supplier on behalf of a customer organisation (the typical industrial scenario). In this latter scenario, depicted in Figure 1-1 (taken from EN50126 and elaborated to show responsibilities), the boundary between customer and supplier responsibilities is unclear and there is possibility for activities to be overlooked and/or faults introduced in the requirements or design, leading to expensive and time-consuming rework later in the development lifecycle. It is well known that the later that faults are detected in the System lifecycle, the more expensive is the process for removing those faults (e.g. refer to [Stecklein04]).

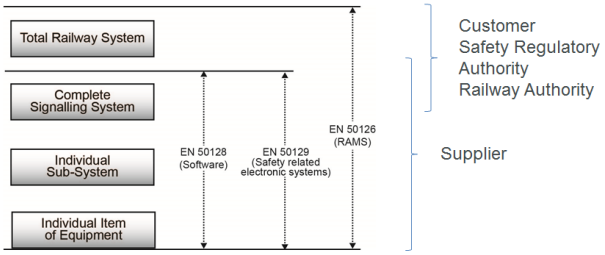

Figure 1-1: EN50126 responsibilities

The process for Safety Management advocated by CENELEC is depicted as a "waterfall" of activities as per Figure 1-2 (taken from EN50126). In this paper, we consider mainly the early lifecycle activities relating to Concept, System Definition and Operational context. The objective of these phases (per EN50126 Table 1) is to investigate scope, context, purpose and environment of the system, as well as define the system and its mission profile, system boundary, scope of operational requirements and the Safety organisation.

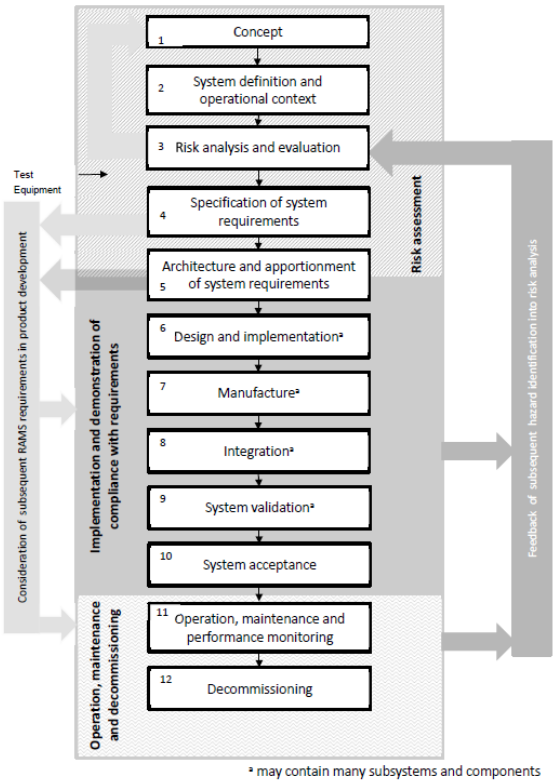

Figure 1-2: EN50126 process

This paper proposes an integrated approach for sharing hazards and safety targets between the customer and

supplier. Four key contributions and additions to current learning are discussed:

1. The customer is active in the translation of railway-level targets to focus on the System that is being developed by the supplier;
2. The customer is required to begin analysis of the operational impact of the System early in the development lifecycle;
3. The supplier is required to engage with the customer to ensure that the System that is built will meet the provided targets;
4. The delineation of abstraction levels for customer and supplier helps to ensure that each party remains focused on the problems that are most pertinent to their tasks in the development of the System.

The approach is presented in the context of Lean management concepts. In particular, the methods proposed are assessed in the context of the corresponding overarching values and principles, demonstrating how value-creation is achieved.

2 Acronyms, Abbreviations and Definitions

2.1 Acronyms and Abbreviations

Acronym	Description
AC	Application Condition
ALARP	As Low As Reasonably Practicable
ASTS	Ansaldo STS
CBA	Cost Benefit Analysis
CCB	Configuration Control Board
ERE	Explicit Risk Estimation
HAZOP	Hazard and Operability Analysis
ONRSR	Office of the National Rail Safety Regulator
RISSB	Rail Industry Safety and Standards Board
RSNL	Rail Safety National Law
SFAIRP	So Far As Is Reasonably Practicable
SIL	Safety Integrity Level
THR	Tolerable Hazard Rate
VoSL	Value of Statistical Life

2.2 Definitions

Barrier to Escalation

A Mitigation that limits only the consequences of the corresponding Hazard occurring e.g. a protective wall that prevents a chemical escaping from an area of a plant.

Cause

A Safety Risk is considered to be a Cause of a System Hazard if it appears as a node in the corresponding Fault Tree for that System Hazard.

Control

A Mitigation that limits the likelihood of the corresponding Hazard occurring e.g. a device that checks the temperature of a boiler and raises an alarm if it exceeds permitted limits.

Demand Rate

The average rate at which a System function will be exercised.

Duty Holder

The persons identified by the RSNL as having a duty of care to ensure Safety SFAIRP.

Functional Failure Analysis

A Safety analysis conducted by examining Functions of a System via keyword failure prompts (such as “Too much”) to determine potential hazardous failure modes of those functions.

Mitigation

Control or Barrier to Escalation.

Office of the National Rail Safety Regulator

The Office of the National Rail Safety Regulator (ONRSR) is an independent body corporate established under the Rail Safety National Law (South Australia) Act 2012. The primary objectives of ONRSR are to encourage and enforce safe railway operations and to promote and improve national rail safety.

Rail Safety National Law

The Rail Safety National Law was first enacted in South Australia and each state and territory has passed a law explaining that the Rail Safety National Law (being the schedule to the South Australian law) is the rail safety law in that state or territory or replicates that law. The law establishes the ONRSR as the body responsible for rail safety regulation in that state or territory.

Requirement

(1) A condition or capability needed by a user to solve a problem or achieve an objective.

(2) A condition or capability that must be met or possessed by a product, service, or product component to satisfy a supplier agreement, standard, specification, or other formally imposed documents.

(3) A documented representation of a condition or capability as in (1) or (2).

Refer to IEEE Standard Glossary of Software Engineering Terminology [IEEE90].

System

The abstraction level related to the Scope of Work under analysis. The System is composed by a set of Subsystems and Interfaces.

System Hazard

A state of a System with the potential for loss of life or injury.

Subsystem

The lower abstraction level, in relation to the Scope of Work under analysis. The Subsystem is a component of the main System.

Tolerable Hazard Rate

The rate at which a particular hazard can be tolerated to occur, while maintaining Safety.

Value of Statistical Life (VoSL)
The additional cost that individuals would be willing to bear for improvements in safety (that is, reductions in risks) that, in the aggregate, reduce the expected number of fatalities by one.

3 Literature Survey

The fundamental concepts underlying Lean management are described in [Womack90]. A Lean organisation is active at various levels of abstraction:

- Values – defining the organisations ethics
- Principles – defining how the organisation 'thinks'
- Methods – defining how the organisation works
- Tools – defining the specific tools used to perform work

To succeed in applying Lean Management techniques, we need to not just consider the Methods and Tools but even the company Values and Principles. The objective of Lean Management is primarily to reduce variation in process, avoiding waste - standardisation is a core Method towards achieving Lean.

This paper is mainly concerned with describing Customer-oriented Methods and Tools for CENELEC compliance, setting them in the context of overarching Lean Values and Principles. To be "Lean" these Methods and Tools need to improve the efficiency of the organisation's activities, via the smooth flow of activity and the efficient use of resources [Womack96]

User-oriented requirements development techniques are already commonly in industrial use. These user-oriented techniques focus on the user and hence customer requirements.
Task models enable identification of requirements and analysis of designs for new requirements and user training needs [Johnson90]. Task models examine the knowledge or competence required to operate a system [Hoppe90].
For the purpose of safety-critical systems, the task analysis may describe procedures for normal operation of the system, maintenance procedures and also procedures for emergency situations [Redmill97]. The description of procedures for normal operation and maintenance should include any recovery steps by which errors of the user are detected and corrected to avoid an accident [Kirwan92]. Task Analysis may be conducted within the context of an overall Cognitive Work Analysis (CWA) [Vicente99]. The CWA informs the task analysis process and provides a functional model of the workplace within which tasks will be performed. The task analysis may be represented as an event tree to trace from errors made by the operator to resulting accidents (see for example [Kirwan92]).
For the purpose of setting acceptability targets for hazards and/or accidents, event-trees can be used to construct fault-trees, which trace from a hazard/accident to causes. The operator causes of hazards/accidents are represented as nodes within the fault tree. The fault tree summarises a collection of scenarios that can lead to a particular hazard/accident. Fault trees can be used in conjunction with scenario-based requirement techniques such as use-cases (e.g. [Cockburn01]).

4 Strategy Overview

For the purpose of this paper, the goals of the safety programme are to deliver a system with safety risk acceptable to the Operator, and to provide evidence that this risk is acceptable.

From a Lean perspective, key Values at the Supplier may include Collaboration and Respect (in ASTS, these Lean values are reflected in the ASTS core values of People, Team Spirit and Integrity, as well as the Hitachi Group values of Harmony and Sincerity). Correspondingly, a key Principle is early lifecycle Communication of Hazards between the Supplier and the Operator.

Lean Management concepts don't specify any particular activities for performing the work done by a specific organisation. It's not a prescriptive checklist but a paradigm within which processes for an organisation can be developed so as to minimise waste. Hence it's not Lean Management *per se* but the derived processes for communication of hazards early in the lifecycle that give us the perceived advantages in terms of better identification of safety hazards and requirements and less rework.

In Australia, the method of demonstrating the safety of the System may be based on:

1. Ongoing compliance with best practice in terms of legislation, standards and guidelines. AS 4292-1 [AS4292] and the Rail Safety National Law [RSNL12] are considered to reflect world-wide best practice at a railway authority level and is the minimum (along with a common law duty of care) that Australian operators need to comply with.
2. Collaborative compliance with the CENELEC rail safety standards, with a well-defined Hazard interface between Operator and the Supplier for early lifecycle Communication of Hazards, to provide assurance for achieving system safety in a development project, and to enable compliance with (1).
3. Systems engineering good practice involving the production of system safety cases supported by structured techniques, e.g. hazard identification, causal analysis, consequence analysis, human factors analysis etc.
4. Independent safety assessment and audit of the System and software.
5. Safety risk assessment in accordance with the operator's risk criteria.

Risk needs to be apportioned by the Operator between System solutions and external railway operational and infrastructure solutions (e.g. rules and procedures). The Operator chooses, when they define the scope of work for a System, whether to manage hazards via procedures or via technical means. This philosophy is an input to their analysis.

The Supplier also analyses operational risks (i.e. OSHA) "bottom-up" during the preliminary Risk Assessment (in

the Risk Analysis and Evaluation phase of the EN50126 lifecycle) and System Hazard Analysis (during the Architectue and Apportionment phase) with more detailed Human Factors Analysis during the later design phases.

The approach advocated in this paper is consistent with the ONRSR guidelines for Major Projects [ONRSR16a], relating to when Quantitative Risk Assessment should be performed, as well as principles of shared responsibility and accountability for rail Safety.

4.1 Risk Acceptance Strategy

A dual strategy may be used, involving both quantitative and qualitative targets.

Safety risk assessment is provided using the Operator's Risk Assessment matrix/criteria and requires combining the frequency of the occurrence of a hazardous event with the severity of the consequence to establish the level of risk generated by a hazardous event.

Risk associated with hazards is reduced So Far As Is Reasonably Practicable (SFAIRP), taking account of all factors affecting reasonable practicability of mitigations, including level and nature of the risk, technical difficulty and resulting acceptability.

Risks in the first instance may be eliminated where feasible in terms of system scope and where reduction of risk to a reasonable level is not possible. Removing a function from consideration means the risk associated with performance of that function is no longer applicable in terms of the System analysis. When elimination is not possible, and where reduction of risk is reasonably practicable, risks may be dealt with through technical mitigations. Where technical mitigation is not possible, non-technical mitigations such as procedures may be introduced provided risk reduction is reasonable. The Operator's acceptability criteria are applied to the residual risk classes.

4.2 Safety Acceptance Strategy

The introduction of the System may involve a variation to accreditation for the operating railway as it can affect:

1. Safe movement of trains;
2. Safe working procedures used by all operating staff;
3. Skill levels of technical maintenance staff.

The Office of the National Rail Safety Regulator is the Regulator who will endorse the System and the change to accreditation for the Operator. Submission to the Regulator will be managed by the Operator.

The safety acceptance strategy for the Supplier is based on developing and implementing appropriate safety requirements (functional and non-functional) and achieving the safety targets identified by the Operator, as demonstrated by the Supplier's Safety Case, along with a supporting Hazard Log. These targets are supplied by the Operator with the intent that they be used as part of the overall SFAIRP submission to the Regulator.

5 Meaning of SFAIRP

Under section 46 of the RSNL [RSNL12], Duty Holders are required:

a. to eliminate risks to safety so far as is reasonably practicable; and
b. if it is not reasonably practicable to eliminate risks to Safety, to minimise those risks so far as is reasonably practicable.

The above duties are referred to in this work instruction as the duties to 'ensure Safety SFAIRP'. The persons identified by the RSNL as Duty Holders have a duty of care to ensure Safety SFAIRP.

The concept of SFAIRP is to achieve the best possible Safety outcomes, to the extent that is 'Reasonably Practicable'.

In this context, and under the RSNL (s47), reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure safety, taking into account and weighing up all relevant matters including:

a. the likelihood of the hazard or the risk concerned occurring; and
b. the degree of harm that might result from the hazard or the risk; and
c. what the person concerned knows, or ought reasonably to know, about the hazard or risk, and ways of eliminating or minimising the risk; and
d. the availability and suitability of ways to eliminate or minimise the risk; and
e. after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

The ONRSR has published a guideline with respect to understanding the SFAIRP principle [ONRSR16b] – the remainder of this Section summarises key observations from that guideline, which is also closely aligned with the Common Law relating to Duty of Care.

What is reasonably practicable is determined objectively. This means that a Duty Holder must meet the standard of behaviour expected of a reasonable person in the duty holder's position and who is required to comply with the same duty.

There are two elements to what is reasonably practicable. A Duty Holder must first consider what can be done - that is, what is possible in the circumstances for ensuring safety. The Duty Holder must then consider whether it is reasonable, in the circumstances to do all that is possible.

This means that what can be done should be done unless it is reasonable in the circumstances for the Duty Holder to do something less.

Mitigations shall be selected for a particular Safety Risk (i.e. Hazard Cause) based on:

- the objective severity of the risk, in terms of likelihood and consequence;

- the objective reasonably known ways to mitigate that risk;
- the availability/suitability of the objectively known options for reducing risk;

The question of what is reasonably practicable is to be determined objectively, and not by reference to the Duty Holder's capacity to pay or other particular circumstances. A Duty Holder cannot expose people to a lower level of protection simply because it is in a lesser financial position than another Duty Holder.

If a particular Duty Holder cannot afford to implement a reasonably practicable risk control, the Duty Holder should not engage in the activity that gives rise to that hazard or risk.

6 Integrated Customer-oriented Process

In accordance with EN50129, it is the responsibility of the Railway Authority, to outline and document the system (independent of technical realisation), to identify the top-level hazards relevant to the system, to analyse the consequences, to define the risk tolerability criteria, to derive the tolerable hazard rates (i.e. safety targets) for top-level hazards, and to ensure that the resulting risk meets the risk tolerability criteria.

The Supplier, as System Integrator, is responsible for deriving corresponding system Safety Requirements (functional and non-functional) and apportioning these safety targets to each of the subsystems.

Per EN50126, risk assessment and selection of the risk tolerability criteria shall involve selecting and applying one of the three risk assessment principles: code of practice, reference system or explicit risk estimation (ERE). There is a need to link the activities of the Operator, at the Concept phase of the EN50126 lifecycle, with the activities of the Supplier during System Definition, Risk Assessment and subsequent phases.

When apportioning safety targets and requirements to subsystems, the associated Tolerable Hazard Rate (THR) or corresponding derived Safety Integrity Level (SIL) rating (based on the comparison table between SIL and hazardous failure rates shown in IEC 61508 [IEC61508]) is assigned at the same time. For systematic failures, a requirement is considered non-safety-related if its derived tolerable hazardous failure rate is less than the threshold for SIL1. For random failures the required maximum failure rate is governed by the THR.

The Customer may be the Operator, or a parent organisation of the Operator. The Operator's Railway Hazard and RAM Risk Log is used to manage top-level railway hazards as well as required procedural/operational mitigations and any other external mitigations that are not part of the System being developed by the Supplier.

The initial safety targets for the Project are defined in terms of the following:

1. Safety targets (Tolerable Hazard Rates) for individual top-level railway hazards and risks and/or cumulative risks that have been derived by the Operator from the hazard identification and risk assessment based on the Operator's criteria for acceptable risks.
2. System-level hazards that have been derived by the Supplier via bottom-up hazard analysis activities including Functional Failure Analysis and HAZOP. The functional hazards have been mapped to: (a) corresponding top-level railway hazards to determine whether the System is introducing any new hazards; (b) corresponding System Railway Events to enable assignment of SIL and THR.
3. Safety requirements and corresponding SILs (where applicable) are derived by the Supplier for the System to mitigate the system-level hazards.
4. Safety targets e.g. Safety Integrity Level (SIL) and corresponding Tolerable Hazard Rates (THR) for safety-related subsystems are allocated by conducting relevant analyses to derive subsystem safety requirements as a part of the Safety Apportionment, e.g. Fault Tree Analysis.

The Safety Targets for the System are provided to the Supplier by the Operator. These Safety Targets are derived by the Operator via a top-down Fault Tree-based analysis, starting from Railway Hazards (these are either already known, or derived as a result of bottom-up feedback from the Supplier hazard analysis). For example:

"Train collides with another rail vehicle on the mainline"

In this paper, we mainly concern ourselves with ERE, but it's also possible to set targets via codes of practice and reference systems.

Ideally, the activities of the Operator to derive Safety Targets occurs before a contract is made with the Supplier. However, another approach can be to let the contract in at least two stages, first performing the Safety analysis and then to build the corresponding System.

The format of the Fault Trees is as shown in Figure 6-1 for the basic 'AND' and 'OR' gates as well as 'TRANSFER'.

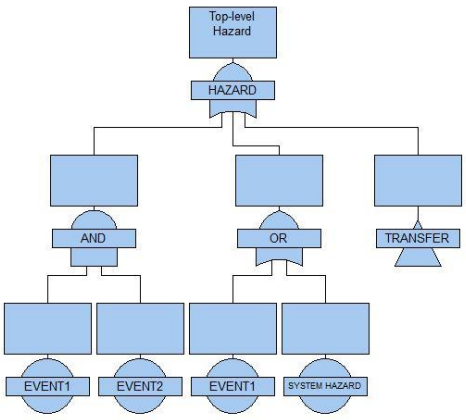

Figure 6-1: Fault Tree Format

As well as these basic symbols, a Fault Tree may combine any of the event and gate symbols given in Tables 6-1 and 6-2.

BASIC EVENT	Basic event for which failure and repair data is available.
CONDITIONAL	Similar to basic event but represents a conditional probability.
UNDEVELOPED	Represents a system event that is yet to be developed.
HOUSE EVENT	Represents definitely operating or definitely not operating (Boolean) events.
TRANSFER	Indicates that part of the fault tree is developed in a different diagram or on another page.

Table 6-1: Primary Event Types

AND	Result event occurs if all input events occur.
OR	Result event occurs if any one of the input events occurs.
COMBINATION	Result event occurs if 'n' of the input events occur.
EXCLUSIVE OR	Result event occurs if one and only one of the input events occurs.
PRIORITY AND	Result event occurs if all input events occur in sequential order from left to right.
INHIBIT	An inhibit gate is essentially an AND gate with an additional conditional event (typically an event external to the configuration represented by the fault tree).
NOT	Result event occurs if the input event does not occur.

Table 6-2: Gate Types

The interaction of the Operator and Supplier whereby the Supplier requires the initial top-down analysis of the System Hazards by the Operator, results in process efficiencies, as from a System Development perspective, the Supplier is the "customer" of the Operator, needing the System Hazards as the input to their System Development process. The resulting process seamlessly integrates the activities of the Supplier and Customer/Operator.

7 System Hazard Analysis

In the preceding Section 6, we mainly discussed the obligations of the Operator as part of the Concept and the relationship of those obligations to the activities of the Supplier in the System Definition and subsequent phases of the EN50126 lifecycle. In this Section, we consider further the corresponding obligations of the Supplier. The System Hazard Analysis (SHA) is compiled using the hazards identified during the Risk Assessment (e.g. via Functional Failure Analysis) and analysis of the proposed high-level System Architecture (e.g. via HAZOP). The process of analysis in two steps via initial Risk Assessment and then SHA (during the subsequent phase that Apportions risks to Subsystems) is part of the EN50126 methodology, with the aim to identify potential hazards in the proposed System concept as early as possible. These System Hazards are Causes in the Operator FTA of the Railway Hazards. The SHA maps the derived functional hazards to the Railway Hazards. The SHA uses this mapping to determine whether the System is introducing any new hazards to the railway. Any new hazards that may have been introduced are communicated to the client for inclusion in the Safety Targets.

The Tolerable Hazard Rates (THRs) are assigned by the Operator to the System Hazards. The SHA Report uses these System Hazards to guide in the assignment of Safety Integrity Levels (SILs) and THRs to the Subsystems of the System.

The primary focus of the SHA is to support the SIL allocation to the system hazards identified in the Functional Failure Analysis. The derivation of mitigations for the System hazards in turn supports the development of the System Requirements Specification. The SHA will be revisited periodically as the project progresses to address any changes to the System Requirements Specification and the Design.

Non-functional Analysis is conducted by qualitatively addressing compressed air hazards, electrocutions, fire and other relevant generic hazards described in applicable checklists. The checklists are reviewed to identify items applicable to the preliminary list of System components. The scope of the analysis, which includes identifying hazards that could arise and the foreseeable consequence of that hazard, may be limited to new and modified components, where the System is an extension of existing equipment. Non-functional Hazards are not assigned a SIL but are treated in accordance with SFAIRP, to reduce risk by identifying appropriate mitigations as per Section 5.

Non-functional analysis is also performed within the scope of the PHA. Non-functional hazards identified in the PHA are integrated into the SHA analysis to provide the total set of non-functional hazards.

8 System Hazards and Mitigations

The outcome of the System Hazard Analysis is a collection of System Hazards, as well as corresponding causes and mitigations. For example, a typical Hazard applicable to railways is "SH-01" as shown in Table 8-1**Error! Reference source not found.**.

The corresponding mitigations for SH-01 include Supervising the Movement Authority Target as a high integrity SIL 4 function of the System. The Movement Authority speed target is one of the speed limits that shall be respected by a train. Supervision of that speed targetas

a SIL 4 function is a Control, which if correctly implemented will result in SH-01very rarely occurring.

System Hazard	Scope
SH-01: Fail to Enforce Operational Speed Limits	A failure that impacts the ability of the System to correctly supervise and/or intervene leading to a Speed Limit Breach (permanent or temporary). This hazard may lead to derailment, or in the case of a Temporary Speed Restriction, a Collision with a Person/Vehicle.

Table 8-1: System Hazard Definition

As well as system functional requirements, the SHA also proposes Application Conditions, which are conditions that need to be fulfilled by the customer either before the System can be put into service, or while the System is in service on a continuing basis. These Application Conditions relate to Co-effectors of the corresponding Hazard, which should also appear as events in the Customer supplied Fault Trees.

Where the SHA derived System Hazards that were not existing as nodes in the customer supplied Fault Trees (and hence for which no targets existed), this is fed back to the customer and the Fault Trees are corrected as appropriate. As noted previously in Section 6, the targets set by the Operator for hazards need not be explicitly quantified but may alternatively refer to codes of practice or other reference systems. The process is iterative and involves the co-operation of both Operator and Supplier to reach a consensus on the overall list of System Hazards that shall be managed by the Supplier.

The collaboration between Supplier and Operator in generating the System Hazards results in resource efficiencies as both parties work from their respective top-down/bottom-up perspectives to realise the same integrated common objective.

The example given is taken from one of the large-scale projects managed by ASTS using the techniques discussed in this paper. In this project, in the order of 10 top-level railway accidents were considered, and about 20-30 System Hazards derived, that would be managed by ASTS via the System under development. The corresponding analysis derived some 500 controls/barriers to escalation and about 1000 application conditions (when limitations/constraints passed up from the Subsystems were also incuded). The Subsystems developed as part of this project were assigned targets of No-SIL, SIL 0, SIL 2 and SIL 4 as appropriate. Throughout the project, the up-front agreed list of System Hazards gave a consistent anchor that enabled us always to answer the question of whether a feature was in the scope of supply of ASTS and in what way the controls and application conditions related to the overall railway safety.

9 SIL Allocation and Apportionment

To guide the allocation of SILs to System Safety Requirements, SILs are assigned to system hazards and causes to denote the required SIL for any System Safety Requirements associated with and mitigating the related causes. The starting point for the allocation of SIL is the clear targets provided by the Operator as per Section 6.

The causes of the System hazards, and corresponding Safety Requirements, as shown in the SHA are allocated SILs as follows:

1. The top-level System Hazards in the SHA are allocated SILs using the derived THRs. Where the hazard derived via the SHA can be mapped to more than one Railway Event, the hazard is assigned the highest SIL associated with the Railway Events;
2. All causes of the system-level hazards (and therefore failure of the corresponding System Safety Requirements) are prima facie allocated the same SIL as the top-level hazard unless the cause is linked to more than one hazard, in which case the assigned SIL is the highest SIL associated with that cause;
3. The assignment of SIL to System Safety Requirements takes into account SFAIRP, and therefore whether a higher SIL is justified based on the cost vs benefit – not all System Safety Requirements that mitigate a particular Hazard need to be assigned the SIL corresponding to that Hazard – only a sufficient set of mitigations to properly manage risk in accordance with SFAIRP;
4. The assignment of SIL to Subsystems takes as an input the trace from System Safety Requirement to Subsystems that is generated as part of the System Architecture definition – Microsoft XL scripts have been created that support the derivation process. The breakdown of the SIL to subsystem functions is achieved via the trace from System Safety Requirements to Subsystem Safety Requirements (part of the overall System Architecture Definition). The scripts support that trace and enable identification of the SIL that will apply for each Subsystem based on the collection of System Safety Requirements that trace to functions of that Subsystem;
5. An FTA may be created to show how the different Subsystems, from a Functional perspective, combine to implement each of the System Safety Requirements;
6. The SIL of the Subsystems is defined by the corresponding highest SIL of the various implemented Subsystem Safety Requirements;
7. Within the Subsystems, the assigned SIL may be further apportioned and decomposed according to the applicable redundancy and component architecture for the Subsystems;
8. Any perceived inconsistencies with the Customer inputs are fed back to the Customer for discussion in the context of the overall SFAIRP argument for the System. Typically,

the discussion of SIL and SFAIRP is contentious and a process needs to be developed by the Operator and Supplier to manage that discussion and any resulting commercial considerations.

10 Applying SFAIRP

Controls considered by ASTS, in accordance with SFAIRP, are typically either engineering controls (including application of Engineering methodologies), implemented by ASTS, or Procedural controls (including use of Personal Protection Equipment such as safety glasses and boots) implemented by the Railway Operator.

Controls are implemented to meet the applicable SIL, as determined via an exhaustive process of hazard identification and risk analysis, described in further detail in the preceding Sections.

The System is considered to be designed in accordance with SFAIRP where controls have been sought where practicable, taking account of the Safety Targets provided by the Operator.

Where Controls have not been implemented, because they were not considered necessary for SFAIRP, applicable Application Conditions are imposed. This also includes where Controls are not fully implemented due to the presence of System defects. All potential defects are discussed by the Operator and Supplier, and a decision is made as to whether the issue is a defect that shall be corrected, or alternatively tolerated (with an Application Condition in the case of Safety impacts). The applicable ASTS Safety Manager and is consulted when deciding the impact of Safety defects and whether the defect can be tolerated with an Application Condition imposed. Application Conditions are discussed in workshops in conjunction with the Customer as well as Ansaldo STS Engineering and System Assurance representatives. In these workshops, the Application Condition is explained by Ansaldo STS, and a conclusion is reached by the Operator as to whether to accept the Application Condition or not. SFAIRP considerations are taken into account in this deliberation, including whether the System could handle the risk via an additional Control, as well as the impact of the Operator failing to correctly perform the Application Condition.

The overall SFAIRP argument for the System considers for each System Hazard, the implemented Controls as well as any Controls that were NOT implemented for that System Hazard. In the case of the Controls that were not implemented, the justification is given, taking into account the various alternative options available. Where the cost-benefit ratio is not obviously grossly disproportionate, a Cost-Benefit Analysis (CBA) may be conducted. Usually, this is done in conjunction with the Operator, because the Railway level implications of any imposed Application Conditions requires statistical data relating to Operating risks that only the Operator can supply.

To apply Cost Benefit Analysis, it is necessary to assume a Value of Statistical Life (VoSL). Currently there is no standard VoSL in the Australian rail industry although various values have historically been published by government departments. However, in 2010 Britain's Rail Industry Safety and Standards Board (RISSB) published its Railway Level Crossing Incident Costing Model (refer to https://www.rissb.com.au/safety/railway-level-crossings/tools-and-guidance/), which utilises a VoSL of A$6,287,873 (2010 figures). The RISSB published VoSL can be considered a lower-limit on the acceptable VoSL for the purposes of CBA calculations for the Australian legal environment. The basic principles of CBA is to calculate the expected "benefit" due to avoided loss of life or injury, using the assumed VoSL and reduced probability (over the predicted lifetime of operation of the System) of the loss of life or injury occurring i.e. the probability of loss of life or injury shall be calculated both with and without the additional Mitigation that is under consideration. This expected "benefit" is compared to the anticipated "cost" of the additional Mitigation.

The entire process of determining whether or not to implement additional controls inherently has commercial impact and this commercial relationship is one of the key drivers for why a process for formalising the exchange of targets between Operator and Supplier is needed. By analysing up front and agreeing on the hazards that will be managed and their SIL, the contractual arrangement is clarified.

11 SFAIRP and SIL

SFAIRP and SIL are related topics but in particular, SFAIRP does not imply that SIL targets have been achieved, and achievement of SIL targets does not necessarily imply SFAIRP without additional considerations relating to the process by which the targets were derived.

SIL targets are derived by the Operator, taking account of all the external factors leading to a Railway Accident. These may be either an explicit SIL, or a THR, from which the Supplier can derive the required SIL. The derivation of the SIL targets should be informed by SFAIRP considerations i.e., the targets should be set so as to reduce risk to an acceptable level, by reducing the probability of a Railway Accident during the lifetime of the System to a level that is considered prima facie to ensure Safety SFAIRP. This is often achieved by demonstrating a residual likelihood per Railway Accident leading to death of < 1/100 years. Each SIL-level increase theoretically produces a reduction in risk of 1 order of magnitude (i.e. 10^{-1}) so that the overall residual likelihood per Railway Accident would be reduced to <1/1000 years, if the applicable hazard was part of the cut-set for the relevant Railway Accident. Assuming a VoSL of A$6,287,873, this equates to a threshold of $1,257,574 for reducing SIL by 1 level when the residual likelihood of death is <1/100 years and assuming a 25 year System lifetime (i.e. the reduction in probability of death for a 25 year lifetime is from 0.23 to 0.03 = 0.2).

12 SIL Assignment

In this Section, we expand on the process required to perform step 4 from Section 9. SIL assignment from System Hazards to corresponding Mitigations is an activity that is required to be performed as per EN50126 [EN50126] lifecycle phase 4.

One approach is for the Supplier to construct a trace table from System Hazards to applicable Causes and Mitigations (whether Controls, actively limiting the occurrence of a Cause, or Barriers to Escalation, limiting only the consequences of the Hazard occurring). Mitigations may be implemented as either System Requirements, or Application Conditions. The THR for each System Hazard shall be respected by the combination of Mitigations that apply i.e. for each Cause, there shall be a suitable mix of Mitigations that achieves the assigned THR (refer to EN50129 [EN50129] for details).

The reliance placed on each of the Mitigations with respect to each Cause shall be determined. In principle a Fault Tree can be drawn with the System Hazard as the root and each Cause as an intermediate node. The leaf nodes of the tree consist of the failure of proposed Controls that prevent the Cause occurring, as well as Demand Rates, whereby the rate of demand for the System Function involving the Cause is taken into account. Demand Rates are especially applicable for example where a Control may be subject to an override in exceptional circumstances e.g. in the case of the Hazard that the authority includes occupied track sections, there is the exception that this can be permitted when Pass at Stop is approved by the Train Controller. The low Demand Rate means that the applicable Controls may be procedural. Refer to Figure 12-1 for an example Fault Tree.

In practice, the Fault Tree is often not explicitly constructed, because the principle of SFAIRP can be applied to each of the proposed Mitigations for each Cause to determine which are needed (and with what SIL) and which are not. Cost Benefit Analysis is applied as necessary to determine the Mitigations necessary for SFAIRP.

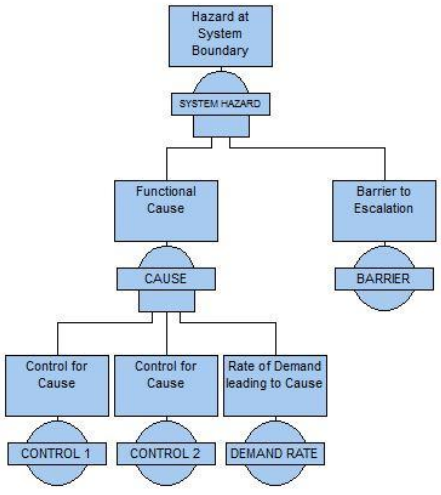

Figure 12-1: Example Fault Tree

If a SIL has been specified for a System Hazard **via a SFAIRP analysis** (as per Section 11) then, at least one Control must be implemented with that SIL (with no exceptions or exclusions). If alternatively, a Barrier to Escalation is implemented with the assigned SIL (with no exceptions or exclusions), then the Risk shall be re-assessed against the reduced consequence after the Barrier is applied – the required SIL for the applicable Controls can be considered to be reduced. Often, a Barrier will render the consequence non-Safety related (only Availability) and in that case, the Design should be considered to be SFAIRP. If there are exceptions/exclusions e.g. due to defects in the implementation as recorded in the applicable defect tracking tool (e.g. Rational Team Concert), or limitations of the design, then those exceptions/exclusions need to be considered separately for SFAIRP (and in effect, are additional Causes). In the case of exceptions/exclusions, there will typically be a Demand rate (i.e. the circumstance whereby the exception/exclusion applies is only sometimes applicable), and the Demand rate, in combination with the proposed Mitigations for the exception/exclusion must meet the overall Tolerable Failure Rate demanded by the SIL for the System Hazard.

From a SFAIRP perspective, the implemented SIL for a Mitigation may anyway be higher than the SIL derived via analysis from the System Hazard, because of usual practice in the industry, or because a higher integrity solution is available at the same cost as the lower integrity solution.

13 Assignment of THR

The assignment of THR to Subsystems proceeds in a similar manner as for SIL, but takes account of the Hardware architecture as defined in the System Architecture definition.

1. The assignment of THR to Subsystems takes as an input the trace from System Safety Requirement to Subsystems that is generated as part of the System Architecture definition;
2. A further input is the FTA created to show how the different Subsystems, from a Functional perspective, combine to implement each of the System Safety Requirements;
3. The FTAs for the System Safety Requirements are merged (assuming that each FTA is in an 'OR' relationship with each other FTA) – again, Microsoft XL scripted support for the process has been created;
4. The THR is apportioned, taking into account any available information regarding the performance of the Subsystems (e.g., applicable Subsystem documentation where existing Subsystems are being reused to implement the new System);
5. Within the Subsystems, the assigned THR may be further apportioned and decomposed according to the applicable redundancy and component architecture for the Subsystems;
6. Any perceived inconsistencies with the Customer inputs are fed back to the Customer for discussion in the context of the overall SFAIRP argument for the System.

14 Conclusions

This paper has discussed an integrated customer-oriented approach to CENELEC-compliance. Four key contributions and additions to current learning have been

discussed. These contributions/additions have been demonstrated in the paper as follows:

1. The customer is active in the translation of railway-level targets to focus on the system that is being developed by the supplier;
2. The customer is involved early in the development lifecycle, to begin analysis of the operational impact of the system;
3. The supplier engages with the customer to ensure that the system that is built will meet the provided targets;
4. The delineation of abstraction levels for customer and supplier helps to ensure that each party remains focused on the problems that are most pertinent to their tasks in the development of the system.

This paper has examined techniques for integrating and balancing customer and supplier obligations under CENELEC with respect to derivation of hazards and setting of safety targets. A Fault-tree based technique, in conjunction with bottom-up System Hazard Analysis has been discussed for communicating information between customer and supplier to ensure overall compliance with the CENELEC standards as well as minimisation of risk of overlooked safety hazards and requirements.

The paper considers the use of information abstraction as a technique for managing customer and supplier communication of safety hazards and requirements. The level of abstraction of information passed between customer and supplier is formalised via the Fault-tree and communication efficiencies are achieved. The resulting technique is customer-oriented because it focuses on the needs of the customer, in terms of hazards that must be mitigated, and the corresponding required safety targets that shall be achieved.

The paper demonstrates how the Lean management goals of resource and process efficiency are benefited by the approach taken. Specifically:

- Mismatches between Operator objectives and supplier activities are identified early in the lifecycle
- Collaboration between the Operator and Supplier for definition of the System Hazards enables efficient utilisation of both teams, with minimal rework

In terms of the proposed Values and Principles, the proposed method enhances Collaboration between Customer/Operator and Supplier, while the Principle of early lifecycle Communication of Hazards between the Supplier and the Operator is directly supported by the interface mechanisms described.

15 References

[Cockburn01] A. Cockburn. Writing Effective Use Cases. Addison-Wesley, 2001.

[EN50126] EN 50126-1:2017, Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[EN50129] EN 50129:2003, Railway Applications – Communications, signalling and processing systems – Safety Related Electronic Systems for Signalling

[Hoppe90] H. U. Hoppe. A Grammar-Based Approach to Unifying Task-Oriented and System-Oriented Interface Descriptions, In D. Ackermann and M. J. Tauber, editors, *Mental Models and Human-Computer Interaction 1*, pages 353-373, Elsevier Science, 1990.

[IEC61508] IEC 61508, Functional safety: safety-related systems (1995).

[IEEE90] IEEE 610.12-1990. *IEEE Standard Glossary of Software Engineering Terminology*.

[Johnson90] P. Johnson, K. Drake and S. Wilson. A Framework for Integrating UIMS and User Task Models in the Design of User Interfaces, In D. A. Duce and M. R. Gomes and F. R. A. Hopgood and J. R. Lee, editors, *User Interface Management and Design: Proceedings of the Workshop on User Interface Management Systems and Environments*, chapter 20, pages 203-216, Springer-Verlag, 1990.

[Kirwan92] B. Kirwan and L. K. Ainsworth. *A Guide to Task Analysis*. Taylor and Francis, 1992.

[ONRSR16a] ONRSR. *Major Project Guideline*, rev 1.1, 2016.

[ONRSR16b] ONRSR. *Meaning of duty to ensure safety so far as is reasonably practicable – SFAIRP*, rev 2.1, 2016.

[Redmill97] F. Redmill and J. Rajan, editors. *Human Factors in Safety-Critical Systems*. Butterworth Heinemann, 1997.

[RSNL12] *Rail Safety National Law (South Australia) Act* 2012.

[Stecklein04] JM Stecklein, J Dabney, B Dick, B Haskins, R Lovell and G Moroney, Error cost escalation through the project life cycle, NASA Johnson Space Center, 2004.

[Vicente99] K. H. Vicente. *Cognitive Work Analysis: Towards safe, productive, and healthy computer-based work*. Lawrence Erlbaum Associates, 1999.

[Womack90] J. P. Womack, D. T. Jones and D. Roos. *The Machine that Changed the World*, Rawson Associates, 1990.

[Womack96] J. P. Womack and D.T. Jones. *Lean Thinking: Banish waste and create wealth in your corporation*, Simon and Schuster, New York.