Practical Considerations in the Application of Safe SFAIRP

Dr. Andrew Hussey, Mohan Murari, Martin Hughes & Maria Hill
Hitachi Rail

Andrew.Hussey@hitachirail.com; Mohan.Murari@hitachirail.com;
Martin.Hughes@hitachirail.com; Maria.Hill@hitachirail.com

Abstract

The Safety Apportionment process is a key step in the overall EN50126 safety management process, whereby the Safety Integrity is determined for each hazard and then apportioned to the related functions of subsystems and components that will implement that Safety Integrity. Some of the key objectives of that process are to document the achieved fail-safety and to justify the proposed architecture and design.

The apportionment of Safety is dependent on the determination of TFFR for each safety function, which in turn relies on the THR for the resulting hazards in the case of functional failure. The assignment of the TFFR and resulting SIL is nominally a top-down process, allocating a safety budget to the subsystems and components of the system.

The proposed design is then examined from the perspective of redundancy and the capacity to achieve that TFFR. While the EN50126 Safety Apportionment process is inherently top-down, the Safe SFAIRP obligation imposed by the Rail Safety National Law is inherently bottom-up, considering the achieved safety reliability as well as the safety reliability that could reasonably be achieved via alternative design options.

In this paper, we examine some of the challenges arising from application of the bottom-up Safe SFAIRP obligation in conjunction with the top-down EN50126 Safety Apportionment process, including the reverse Safe SFAIRP which is applicable for specific cases. We also consider some of the limitations of the available Safety Apportionment techniques.

Keywords: *Safety Systems, Safety Apportionment, Railway, Signalling, Safe SFAIRP, EN50126*

1 Introduction

The CENELEC standard EN50126 has been commonly applied to railway signalling Systems Engineering as part of the overall CENELEC lifecycle, in conjunction with EN50128 and EN50129. One objective of the EN50126 standard is to provide a framework for the development of safe Signalling Systems, based on the required Safety Reliability of the Safety Functions implemented by that System. Based on the application of the EN50126 process, a corresponding Functional Failure Rate may be claimed for the System in respect of its Safety Functions. Implicitly, the application of EN50126 should lead to more robust systems with fewer faults.

The process advocated in EN50126 commences with the identification of Safety Targets in respect of tolerable accident rates then assigns Tolerable Hazard Rates to associated hazards based on the probability of occurrence of intermediate events leading from hazard to resulting accident. This process can however be shortcut via the use of Risk Acceptance Principles as per the Common Safety Method, whereby Codes of Practice and/or Reference System arguments may be used to arrive at the proposed THR for particular hazards. In any case, the focus in EN50126 early in the lifecycle is to look outwards from the system hazard to consider what is the necessary safety integrity taking account of the environment in which the system is being operated.

From the CENELEC perspective, the examination of TFFR and internal causes of System Hazards comes after THR has been defined for the corresponding hazard. At that point, using the Architecture as a guide, TFFR can be apportioned to Subsystems, based on the hazard THR.

The Rail Safety National Law in Australia imposes the duty of Safe SFAIRP , which is an overarching duty of care to ensure that reasonable measures have been implemented in addressing all potential safety risks. The Safe SFAIRP duty has been interpreted in the ONRSR guideline ONRSR (2021) in respect of how reasonableness shall be judged. One of the commonly accepted interpretations is that where the cost of implementing a safety-related improvement is sufficiently low so as to be less than the benefit x the gross disproportion factor, then the improvement should be implemented. This is irrespective of whether the improvement is needed to achieve the overall THR for the hazard from a purely quantitative perspective.

Therein lies a potential conflict between EN50126 and Safe SFAIRP , which we will examine in more detail in this paper. From CENELEC perspective, the process is primarily top-down and driven by the apportionment of overall safety targets, while from the Safe SFAIRP perspective, the process is primarily bottom-up, for each potential control, and in respect of whether it is reasonable.

In this paper, we examine a case study system and several of its Safety Functions, to consider to which extent such conflicts exist, and what are some of the strategies for overcoming those conflicts as well as other identified challenges.

The key benefits of this paper are:

1. advancement of knowledge of the CENELEC risk apportionment approach.
2. improved understanding of applying Safe SFAIRP in practice.
3. sharing experience from use of risk apportionment in an industrial case study.

2 Acronyms, Abbreviations, and Definitions

2.1 Acronyms and Abbreviations

Acronym	Description
ALARP	As Low As Reasonably Practicable
ATSB	Australian Transport Safety Bureau
CoP	Code Of Practice
ETCS	European Train Control System
GAME	Globalement Au Moins Equivalent
GBMS	Global Business Management System
MEM	Minimum Endogenous Mortality
NCO	Network Control Officer
ONRSR	Office of the National Rail Safety Regulator
RAMS	Reliability Availability Maintainability & Safety
RSNL	Rail Safety National Law
RTIO	Rio Tinto Iron Ore
SFAIRP	So Far As Is Reasonably Practicable
SIL	Safety Integrity Level
SSA	System Safety Assurance
STS	Hitachi Rail STS
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate
TIRF	Tolerable Individual Risk of Fatality
TMS	Traffic Management System
TVCS	Tunnel Ventilation Control System
VHMI	Vital Human Machine Interface
WSP	Wayside Standard Platform

Table 1:Acronym Table

2.2 Definitions

Following are the definitions useful for this paper as per EN 50126;

2.2.1 Hazard

Condition that could lead to an accident.

2.2.2 Risk Assessment

Overall process comprising a risk analysis and a risk evaluation

2.2.3 System

Set of interrelated elements considered in a defined context as a whole and separated from their Environment.

3 Literature Survey

EN50126 acknowledges that different risk acceptance regimes exist, in respect of determining what is acceptable risk e.g. ALARP, GAME, MEM etc. H.H. Kron (2003) notes that simple safety targets like TIRF (tolerable individual risk of fatality) and THR (tolerable hazard rate) are not sufficient alone for risk acceptability.

The obligation to apply Safe SFAIRP in Australia is mandated by the Rail Safety National Law RSNL (2012), but also appears in safety standards such as AS7472 RISSB (2018)

Tim Procter (2019) has considered the interaction between Safe SFAIRP and traditional Safety Assurance activities. He states: "The Safe SFAIRP concept is explicitly included in Australian rail System Safety Assurance approaches, but often in a manner that indicates a belief that the implementation of SSA discharges all SFAIRP duties. However, although there is considerable overlap, SSA approaches do not align precisely with Safe SFAIRP principles – particularly when attempting to demonstrate diligence in safety-related decisions-making."

Procter notes that, in practice, the Courts determine what is Safe SFAIRP post-event on a case-by-case basis, with the benefit of hindsight.

Procter concludes that to demonstrate Safe SFAIRP, in addition to the requirements imposed by traditional SSA, it is also necessary to show:

1. *That there is a formal argument as to why all credible, critical hazards have been identified.*
2. *That for each significant hazard all recognised good practice controls are in place, and if not, have been tested for reasonableness, and in the circumstances demonstrated as being unreasonable.*
3. *That further possible practicable controls are considered (even if the risk is considered to be reduced to a 'tolerable' level), and that when considering further precautions, the hierarchy of controls is applied*
4. *That a quality assurance system is in place to ensure all reasonably practicable controls are implemented and remain effective.*

Procter concludes that system safety approaches can end up focusing on maintaining detailed records and following standard activities at the expense of considering what actually constitutes good safety decisions in the specific project context. Rather, as Procter states, to achieve a successful synthesis of SSA and Safe SFAIRP it is critical to remember that SSA is a tool used to achieve a goal, not a goal in itself. The goal is safety, and in the Australian/New Zealand context that is eliminating or (failing that) reducing risk Safe SFAIRP.

Similarly, Steve Dawkins (2021) also notes that *"It is not a Safe SFAIRP argument to list all the treatments identified and imply they amount to Safe SFAIRP, there should also be an argument why these treatments, taken together, represent Safe SFAIRP explicitly".*

The purely top-down approach to risk management has in any case its challenges. Tracy A. White (2011) shows that the precise meaning of acceptability and the underlying concept of ALARP is poorly understood and articulated. Lack of clarity, as to the actual level of risk being exposed can in part be attributed to poor articulation of the risk.

The need to address the topic of the interaction between System Safety Assurance and Safe SFAIRP has also been noted by the ATSB in their issue number RO-2018-014-SI-01, which led directly to the publication of AS7472 RISSB (2018) and AS7473 RISSB (2020) by

RISSB and the creation of the note Importance of a *System Engineering Approach* by the ONRSR.

Similarly, Howard Parkinson (2013) notes the conflict between standards-based approaches and formal risk assessment including cost-benefit analysis. Parkinson states that it seems clear that there is a continuum between the two positions and that the core issue is in knowing what to do and if that is enough.

Our survey of the literature confirms the need for a comprehensive assessment of the differences between EN50126 and Safe SFAIRP, along with their impact for System development.

4 Safe SFAIRP

In this paper, we examine application of the principle of Safe SFAIRP.

Under section 46 of the RSNL (2012), 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 the RSNL as the duties to 'ensure Safe SFAIRP'. The persons identified by the RSNL as Duty Holders have a duty of care to ensure Safe SFAIRP.

The concept of Safe 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 ONRSR (2021), 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 practically reasonable.

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 assessed severity of the risk, in terms of likelihood and consequence;
- the reasonably known ways to mitigate that risk;
- the availability/suitability of the known options for reducing risk;

The question of what is reasonably practicable is to be determined quantitatively, 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.

The ONRSR guideline also consider the case of "reverse Safe SFAIRP", which relates to the situation where a control shall be removed because it may be shown that the control is no longer necessary to ensure safe SFAIRP. In that case, specific guidelines apply, including:

- where the cost of maintaining the control has substantially increased (however in this instance, it may be reasonably practicable to introduce a new control rather than accept an increase in residual risk);
- the risk reduction provided by the control has reduced due to the risk reduction achieved by other or new controls;
- where a risk control interacts adversely with another risk control; or
- it can be shown that the introduction of the control was not necessary to ensure safe SFAIRP in the first place

This is different from EN50126, where a control can be removed provided it is not required so as to achieve the necessary THR, using a quantitative risk assessment.

5 Case Study

The case study involves a project where Hitachi rail has the safety critical role of European Train Control System (ETCS) supplier.

For this case study, we analyse the safety assessments of several critical interfaces and functions of ETCS: the Train Data Entry function, Tunnel Ventilation Control System (TVCS) interface, Track Worker Protection function and the HW Watchdog function.

The Train Data Entry function is integral to the management of rail risks such as derailment or overrun of a Limit of Authority. This requires an assessment of the actual risks for this project, associated with incorrect train data entry leading to an accident.

The TVCS Subsystem, within the normal operation ventilation function, must ensure that, the fans blow smoke in the opposite direction from the escape routes to ensure the safest evacuation condition is possible when a fire occurs in the tunnel. This requires an assessment of the accuracy of the data provided by ETCS to TVCS about the train position in the Tunnel.

Historically procedures are used to manage the risk of the protection of track workers, but there have been efforts to introduce more technical controls (such as a possession management system using handheld terminals) to manage the risk. This required an assessment of what types of controls were appropriate for the management of track worker protection risks for the project.

The watchdog that manages the risk of the display of information incorrectly matching the original VHMI command despite a corruption of the command sent to the WSP, is now obsolete. This required an analysis of the level of the risk and the cost of implementing a new equivalent control or the safety impact of removing it.

6 Outcomes

In this section, we examine each of the case study functions, from the perspective of the top-down quantitative assessment of risk and from the perspective of bottom-up evaluation of Safe SFAIRP, taking into account all the possible risk mitigations.

6.1 Train Data Entry

On the face of it, train data might be critical data, with high potential for resulting in a serious accident, such as a derailment or an overrun of a Limit of Authority. However, deeper investigation of the operating context may limit the actual potential for an accident because the number of actual train types with different braking characteristics is limited.

Top-down considerations based on quantitative assessment point towards high integrity train data checks not being necessary to achieve overall safety targets, because configuring an incorrect train type results nonetheless, in a similar braking model i.e. the THR for the associated Train Data Entry hazard can be increased due to the improbability that incorrect data could result in an accident.

On the other hand, bottom-up Safe SFAIRP considerations from the perspective of potential controls, could indicate the benefit of implementing high integrity checks of the train data.

The project reached the conclusion that high integrity checks of the train data was not necessary, taking into account cost-benefit analyses, as well as detailed examination of the reference systems that determined that where a high integrity check is needed, train types typically differ significantly one from the other.

6.2 Tunnel Ventilation Control

Tunnel Ventilation may be enhanced via accurate knowledge of the train position, since the correct fans in the tunnel can be switched on, to contain the spread of smoke in the tunnel. Overall risk is dependent on the risk for an incident (such as fire) in the tunnel, as well as which other mechanisms are available to manage this risk, outside the signalling system.

Top-down considerations based on quantitative assessment point towards high integrity train position reports not being necessary to achieve overall safety targets, since the risk for a fire to occur is considered to be low.

Bottom-up SFAIRP considerations, however, from the perspective of potential controls, point towards the desirability of high integrity train position reports, which would almost eliminate a possible cause of tunnel ventilation failure.

The project reached the conclusion that high integrity provision of the train position was not necessary, taking into account cost-benefit analyses as well as the applicable reference systems.

6.3 Track Worker Protection

Use of a handheld terminal or similar, even a low integrity device, may drive a change in the achieved risk as compared with historical, procedural, approaches to management of track worker risks. Incorrect performance of procedures is a significant cause of accidents resulting in track worker death or injury.

Previous top-down considerations based on quantitative assessment has pointed towards hand-held terminals not being necessary to achieve overall safety targets – procedures can be considered reliable with consideration of the historical data regarding their application (the procedures can be considered as a Code of Practice under the CENELEC).

However, bottom-up Safe SFAIRP considerations based on more recent reference systems point towards the desirability of handheld terminals to reduce possibility for human error.

The project reached the conclusion that handheld track worker protection was desirable, taking into account cost-benefit analyses as well as the desired balance between procedural vs technical controls.

6.4 Hardware watchdog removal

The hardware watchdog removal is an instance of reverse Safe SFAIRP. The reverse Safe SFAIRP argument from ONRSR (2021) is applicable on specific cases which include, where the cost of maintaining the control has substantially increased, and where risk is already very low without the control.

Top-down consideration of quantitative assessment of risk implies no need for a SIL 4 VHMI due to the overall low likelihood of the hazardous event (display of information matching the original VHMI command despite a corruption of the command to WSP) occurring.

From a bottom-up perspective the Wayside Standard Platform hot standby solution (WSPHS+) solution exists and could potentially reduce risk further. Hence for Safe SFAIRP such solutions must be considered.

The main alternative control considered based on the outcome safety analysis is the implementation of a replacement for the obsolete VHMI, which would need to be the updated WSPHS+. However, instead other additional controls were considered and accepted, leading to the safety related application conditions that have been imposed and considering that the risk is low with the proposed solution.

The project reached the conclusion that in the case of VHMI, the risk reduction provided by the watchdog control has reduced due to the risk reduction achieved by other or new controls and the hazard for display of information matching the original TMS/VHMI command despite a corruption of the command to WSP can be considered to have a rare occurrence rate, even in the worst case where there is no watchdog present. Hence it may be acceptable to run VHMI on COTS hardware, for a specific period of time.

6.5 Challenges Observed

We observed at least three specific challenges as a result of our analysis of the case study functions:

1. Top-down approaches, applied early in the project may not take into account all the factors necessary to demonstrate Safe SFAIRP.
2. The information needed to properly evaluate Safe SFAIRP is not available until later in the lifecycle when the design is matured.
3. Where reference systems and CoP are not available, additional controls may become known only later in the design process, potentially in conflict with earlier targets. Then Safe SFAIRP may require deeper investigation of potential controls before a target can be assigned, and an apportionment can be performed.

6.6 Approach to reconciling EN50126 and Safe SFAIRP

We derived three potential controls measures for ensuring effective and efficient consideration of Safe SFAIRP within the EN50126 risk assessment process:

1. The top-level target identification needs to consider CoP and Reference Systems so as to take into account, at an early stage, potential alternative controls.
2. The process for determining targets and safety apportionment to system functions must be a series of loops with increasing certainty of the correctness of the outcome over time.
3. Cost-benefit approaches to Safe SFAIRP determination take into account the overall risk so where risk is already very low based on a top-down evaluation, the opportunity for bottom-up consideration of controls to impact that risk is reduced.

7 Future Ideas

The recent release of EN50716 (replacing EN50128) has highlighted the need for flexibility in respect of the applicable lifecycle. Even for EN50126, a customised lifecycle can be beneficial to overcome some of the challenges arising from application of both EN50126 and Safe SFAIRP concurrently. Such a customised lifecycle would allow the design and development process to repeatedly and flexibly loop back to the THR assignment and resulting apportionment. It would be interesting to formalise and therefore examine in more detail the application of such a process to a real-world case study.

8 Conclusion

This paper has considered the relationship between EN50126 and Safe SFAIRP and the impact that Safe SFAIRP compliance has on an EN50126 compliant development process.

The key contributions and additions to current learning discussed in this paper were a consideration of several case study functions, which enabled us to:

1. Gain knowledge about the CENELEC risk apportionment approach.
2. Improve understanding of applying Safe SFAIRP in practice.
3. Examine an industrial case study to consider how Safe SFAIRP is being applied in conjunction with CENELEC in the context of some specific example functions.

9 References

Steve Dawkins (2021):How to Argue Risk is Reduced SFAIRP (https://www.acmena.com.au/insight/how-to-argue-risk-is-reduced-sfairp/), 2021.

H.H. Kron (2003): On the Evaluation of Risk Acceptance Principles, ResearchGate, Jan 2003.

ONRSR (2021): ONRSR Guideline Meaning of duty to ensure safety so far as is reasonably practicable, 17 May 2021.

Howard Parkinson (2013): Compliance versus risk assessment: when have we done enough?, Sage Journals, Vol 224, Issue 4, 2013.

Tim Procter (2019): Compliance vs. Due Diligence: SFAIRP and its Interaction with System Safety and Assurance Approaches, 2019.

RISSB (2018): Railway Operations Management of Change, AS7472, 26 Nov 2018.

RISSB (2020): Complex System Integration in Railways, AS7473, 30 June 2020.

RSNL (2012): Rail Safety National Law (as applicable to each Australian State),2012.

Tracy A. White (2011): The Language of System Safety Engineering: Loose Language Surrounding ALARP, ASSC 2011.