



This document has been prepared by **Parsons Brinckerhoff** for the California High-Speed Rail Authority and for application to the California High-Speed Train Project. Any use of this document for purposes other than this Project, or the specific portion of the Project stated in the document, shall be at the sole risk of the user, and without liability to PB for any losses or injuries arising for such use.



## System Safety Reviews

The purpose of the System Safety Review is to ensure:

- Consistent application and appropriateness of safety analysis techniques

System Safety Reviews:

RAMS Reviewer:	-- Original signature on file -- _____ Ibrahim Muftic, RAMS Manager	<u>August 9, 2013</u> Date
Internal Safety Reviewer:	-- Original signature on file -- _____ Gulzar Ahmed, Safety Specialist	<u>August 9, 2013</u> Date
PB System Safety Manager:	-- Original signature on file -- _____ John Sheehan, Safety Manager	<u>August 9, 2013</u> Date

Note: Signatures apply for the PHA Report revision corresponding to revision number in header and as noted on cover.



## TABLE OF CONTENTS

<b>SYSTEM SAFETY REVIEWS .....</b>	<b>I</b>
<b>TABLE OF CONTENTS .....</b>	<b>II</b>
<b>ABSTRACT .....</b>	<b>1</b>
<b>1.0 INTRODUCTION.....</b>	<b>2</b>
<b>1.1 PURPOSE OF TECHNICAL MEMORANDUM.....</b>	<b>2</b>
<b>1.2 STATEMENT OF THE ISSUE.....</b>	<b>2</b>
1.2.1 DEFINITION OF TERMS .....	3
<b>2.0 DEFINITION OF TECHNICAL TOPIC.....</b>	<b>4</b>
<b>3.0 ASSESSMENT / ANALYSIS .....</b>	<b>6</b>
<b>3.1 PAST AND CURRENT METHODS OF DETERMINING ACCEPTABLE RISK IN THE U.S. TRANSPORTATION INDUSTRY .....</b>	<b>6</b>
<b>3.2 COMMON SAFETY METHOD – THE EUROPEAN APPROACH TO HAZARD RISK ASSESSMENT .....</b>	<b>9</b>
<b>3.3 OTHER INTERNATIONAL APPROACHES TO RISK ACCEPTANCE.....</b>	<b>13</b>
<b>3.4 RISK ASSESSMENT PROCESS .....</b>	<b>13</b>
3.4.1 SEVERITY OF CONSEQUENCE.....	14
3.4.2 FREQUENCY OF OCCURRENCE.....	15
3.4.3 RISK ASSESSMENT MATRIX.....	17
<b>3.5 POTENTIAL APPROACHES TO RISK ACCEPTANCE CRITERIA .....</b>	<b>18</b>
3.5.1 ALARP - AS LOW AS REASONABLY PRACTICABLE .....	18
3.5.2 GAMAB - GLOBALEMENT AU MOINS AUSSI BON .....	20
3.5.3 MEM (MINIMUM ENDOGENOUS MORTALITY).....	21
<b>4.0 SUMMARY AND RECOMMENDATIONS.....</b>	<b>21</b>
<b>4.1 SUMMARY .....</b>	<b>21</b>
<b>4.2 RECOMMENDATIONS.....</b>	<b>21</b>
<b>5.0 SOURCE INFORMATION AND REFERENCES.....</b>	<b>22</b>



## ABSTRACT

Determining the criteria for accepting hazard risk is a fundamental element of hazard management. An organization must assess its needs and priorities in order to determine its appetite for residual hazard risk, that is the risk the remains after the application of mitigation measures. How much mitigation is applied? When have sufficient mitigation measures been applied and further application is either not helpful or even harmful?

The Technical Memorandum establishes a process by which the California High-Speed Rail Authority can consistently determine levels of acceptable risk for all project facets: operations, infrastructure, systems, and rolling stock.

The process is based upon the European *Common Safety Method* and conforms to FRA requirements for risk-based hazard management. The ALARP Principle is also recommended for Risk Acceptance Criteria for explicit risk estimation.

TM 500.06 Appendix A will replace Sections 4.0 to 4.2 of the *Safety & Security Management Plan* (SSMP).



## 1.0 INTRODUCTION

Hazard management is the process of identifying, assessing, and mitigating or eliminating hazards in order to achieve a level of hazard risk that is acceptable to the responsible party. The Federal Railroad Administration (FRA) defines a hazard as “any real or potential condition (as identified in the railroad’s risk-based hazard analysis) that can cause injury, illness, or death; damage to or loss of a system, equipment, or property; or damage to the environment”<sup>1</sup>. The FRA also defines risk as “the combination of the probability (or frequency of occurrence) and the consequence (or severity) of a hazard”. In the context of this Technical Memorandum, the term “risk” will be used to apply only to hazard risk as opposed to project risk or other types of risk.

The common term “safe” in risk-based decision making has a certain amount of uncertainty since it cannot mean a zero chance of an adverse event occurring. Zero risk is not a realistic goal for the hazard management process as it relates to an operating railroad; there is always residual risk when the train leaves the station. As there is no physical system that has a zero failure rate, no software design can foresee every possibility and no human being makes zero errors, the key is to reduce the hazard risk to an acceptable level, known as residual risk, through the application of appropriate mitigation measures.

Determining what level of risk is acceptable is a policy decision of the responsible party. Making sound defensible decisions should be the focus of the risk management process, not necessarily the quantitative risk estimate or a risk acceptance guideline. In most of the cases, safety related decisions are about available options and there are no simple numerical solutions or distinct lines on a graph separating acceptable from unacceptable.

Decision making in a risk based approach may be complicated since risk management is often a shared responsibility and the varied interests of the stakeholders can lead to different and conflicting opinions about the outcomes. It includes traditional/deterministic analyses complemented by risk assessment methodologies. This Technical Memorandum proposes a method by which the California High-Speed Rail Authority (Authority) can accept the residual risk consistently across the system and throughout the system lifecycle. This Technical Memorandum has been developed by reviewing the past and current regulations and guidance for risk acceptance, both domestically and internationally.

### 1.1 PURPOSE OF TECHNICAL MEMORANDUM

Accepting residual risk is a policy consideration for the Authority. The purpose of this memo is three-fold:

- To define the issues surrounding risk acceptance criteria including the need, goals, and expected output of establishing risk acceptance criteria
- To review past and current risk acceptance methodologies
- To recommend a model for risk acceptance criteria for adoption by the Authority

### 1.2 STATEMENT OF THE ISSUE

The California High-Speed Train System (CHSTS) will be designed, built, and operated to an acceptable level of safety, expressed as acceptable residual hazard risk. Risk acceptance criteria describe the baseline by which the Authority can determine acceptance of residual risk. The risk acceptance criteria for the CHSTS must be established so that the Authority can make a consistent, informed decision about how to accept residual risk.

---

<sup>1</sup> 49 CFR Part 270 System Safety Program; Proposed Rule, Federal Register, Vol. 77, No. 174, September 7, 2012



### 1.2.1 Definition of Terms

Include technical terms, acronyms, foreign phrases/terms, etc. and or terminology that may have specific connotations with regard to the CHSTS.

<u>Authority</u>	California High-Speed Rail Authority
<u>Hazard</u>	Any real or potential condition that can cause injury, illness death; damage to or loss of a system, equipment, or property; or damage to the environment.
<u>Residual Hazard Risk</u>	The hazard risk that remains after the application of mitigation measures to reduce the severity and/or probability associated with a hazard.
<u>Risk</u>	The combination of the probability (or frequency of occurrence) and the severity (or consequence) associated with a hazard.

### Acronyms

<u>ALARP</u>	As Low As Reasonably Practicable
<u>ANSI</u>	American National Standards Institute
<u>AREMA</u>	American Railway Engineering and Maintenance-of-Way Association
<u>CENELEC</u>	European Committee for Electrotechnical Standardization
<u>CFR</u>	Code of Federal Regulations
<u>CHSTS</u>	California High-Speed Train System
<u>CSM</u>	Common Safety Method
<u>DoD</u>	Department of Defense
<u>EN</u>	European Norm
<u>FRA</u>	Federal Railroad Administration
<u>FTA</u>	Federal Transit Administration
<u>GAMAB</u>	Globalement Au Moins Aussi Bon - Translated as a level of hazard risk globally at least as good as the one offered by any equivalent existing system
<u>MEM</u>	Minimum Endogenous Mortality
<u>PHMSA</u>	Pipeline and Hazardous Materials Safety Administration
<u>PTC</u>	Positive Train Control
<u>RAC</u>	Risk Assessment Code
<u>RAMS</u>	Reliability, Availability, Maintainability, and Safety



## 2.0 DEFINITION OF TECHNICAL TOPIC

Risk can take many forms: physical, financial, legal, project, etc. Within the scope of this Technical Memorandum risk is concerned with the physical risk associated with railroad operations. FRA defines risk in the context of railroad operations as follows:

*Risk means the combination of the probability (or frequency of occurrence) and the consequence (or severity) of a hazard.<sup>2</sup>*

Risk can be expressed quantitatively (calculated failure rate for example) or qualitatively (categorized representation of the probability and severity).

No outward activity is without some form of risk: indeed when we leave the house in the morning there exists the risk that we may not come back in the evening. Managing risk allows an organization to enjoy the benefits of its operation while keeping the associated risk at an acceptable level.

The American National Standards Institute (ANSI) defines acceptable risk as follows:

*“Risk that is accepted for a given task or hazard. For the purpose of this standard the terms “acceptable risk and “tolerable risk” are synonymous. The decision to accept (tolerate) risk is influenced by many factors including culture, technological and economic feasibility of installing additional risk reduction measures, the degree of protection achieved through the use of additional risk reduction measures, and the regulatory requirements or best industry practice. The expression “acceptable risk” usually, but not always, refers to the level at which further risk reduction measures or additional expenditure of resources will not result in significant reduction of risk”<sup>3</sup>*

In other words, an acceptable risk is a risk for which the probability of an incident or exposure occurring and the severity of harm or damage that may result are acceptable to the responsible party without further reduction. Perceptions (both internally and publicly) of the risks and the value of risk reduction measures can influence the decision to accept a risk or not. Risks that are acceptable in one industry or company may not be acceptable in another; also the same risk within one organization which might be acceptable for the employees with certain skill sets might not be acceptable for the customers. Risk reduction measures must be acceptable in the particular setting being considered, and their applicability and effectiveness must be re-evaluated as the system matures or more information is known about the nature of the risk.

Risk acceptance can be defined in different ways including a cooperative approach by stakeholders, regulatory entities, or both. Cooperative approaches that bring together technical and political/ societal interests have the ability to bring synergy to the process.

The simplest framework for defining risk acceptance is to distinguish between those hazards that require mitigation, and those that do not based on the risk level associated with the hazard. Unfortunately, the complexities and uncertainties of railroad operation make it difficult to simply estimate the risk and to easily identify those hazards that require mitigation and those that do not.

---

<sup>2</sup> 49 CFR Part 270 System Safety Program; Proposed Rule, Federal Register, Vol. 77, No. 174, September 7, 2012

<sup>3</sup> ANSI B11.0 Safety of Machinery: General Requirements and Risk Assessment, American National Standards Institute, 2010



A common approach is often described as an inverted triangle dividing the risk into three regions<sup>4</sup>:

- An upper region where the level of risk is regarded as unacceptable whatever benefits the activity may bring;
- A middle region where risks may be tolerated if they cannot be practicably reduced further;
- A lower region where the level of risk is regarded as acceptable without any mitigation.

The upper region includes risks that are intolerable and their acceptance cannot be justified on any grounds. Risk reduction in this region must occur or the system is not allowed to operate. The lower region contains the commonplace risks that are broadly acceptable, making further risk reduction efforts unwarranted.

Risks falling in the middle region are reduced through the application of mitigations until the cost of further mitigation is disproportionate to the benefit gained. The middle region is also known as the tolerable region and is where the majority of risk management activities occur. Even though a risk may be classified as tolerable, mitigation measures should be sought to further reduce the level of such risk; the objective being, the more acceptable the risk the better it is. The three-region approach to risk acceptance is shown in Figure 1:

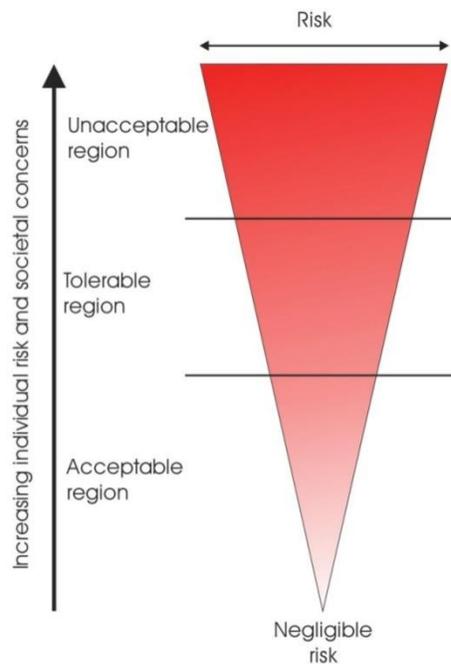


Figure 1 – Acceptability of Risk<sup>5</sup>

**Goal of Risk Acceptance Criteria** - The goal of establishing risk acceptance criteria is to define the upper and lower boundaries of the tolerable region, and to define a clear, consistent, and realistic methodology for assessing the need for further risk reduction measures within the tolerable region.

<sup>4</sup> *ANSI Z690.3 Risk Assessment Techniques*, American National Standards Institute, 2011

<sup>5</sup> *Transit Safety Management and Performance Measurement*, Federal Transit Administration Office of Safety and Security, 2011



**Outcome of Risk Acceptance Criteria** - Establishing risk acceptance criteria will allow the application of an informed hazard management process to prioritize the expenditure of resources on those hazards which fall in the upper and middle region. The Authority will be confident in the knowledge that they applied risk reduction measures appropriately and effectively, leading to acceptance by FRA, other third parties such as regulators and the insurance community, and the general public.

### 3.0 ASSESSMENT / ANALYSIS

Methods for identifying and describing hazard risk acceptance criteria will be explored in this section. Typical U.S. approaches will be explored, as well as approaches taken by public transit industries in countries around the world. Emphasis will be placed on similar foreign high-speed rail systems as well as on the intent and requirements of the FRA.

#### 3.1 PAST AND CURRENT METHODS OF DETERMINING ACCEPTABLE RISK IN THE U.S. TRANSPORTATION INDUSTRY

Determining risk acceptability is a rather subjective exercise dependent on the cultural, financial, political, and legal priorities of the party responsible for the risk. Performance is balanced with the desire to not kill or injure persons, damage property, discredit a reputation, or subject the responsible party to disciplinary action. In the end, organizations as well as individuals accept certain amount of risks every day. Should the Company place the order with a new vendor who has a lower price and comparable reputation? Should the train be allowed to depart with a defect that is within tolerance? Should a person walk across the street against the flashing red hand on the signal? These may be rather simple decisions based on past experience and the priorities and needs of the responsible party, yet they may be just as easily approached in a different way by a party with different priorities and needs. Determining exactly what is acceptable in the particular setting being considered is a challenge that many organizations struggle with. In the interest of public safety the Federal government has begun to address the issue of risk acceptance in a variety of ways.

**MIL-STD-882 and Others** - The basis for many risk assessment strategies within the transportation industry is the U.S. Department of Defense (DoD) Military Standard 882E (MIL-STD-882E)<sup>6</sup>. This standard is referenced as a foundational document for risk-based hazard analysis in several Department of Transportation regulations including 49 CFR Part 229 Locomotive Safety Standards, 49 CFR Part 236 Signal and Train Control Systems, The Federal Transit Administration's (FTA) guidance documents *Transit Safety Measurement and Performance Measurement* (2011) and *Hazard Analysis Guidelines for Transit Projects* (2000), and FRA's guidance document *Collision Hazard Analysis Guide: Commuter and Intercity Passenger Rail Service* (2007). MIL-STD-882 is also referenced in the American Public Transit Association's *Manual for the Development of System Safety Program Plans for Commuter Railroads*.

MIL-STD-882E was developed to guide the use of a system safety approach to managing the risks associated with DoD operations. Indeed, the standard states "This system safety standard practice identifies the Department of Defense Systems Engineering approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated." While

---

<sup>6</sup> U.S. Dept. of Defense Military Standard 882E, *Standard Practice for System Safety*, May 2012



not directly written for transportation applications the great value of MIL-STD-882E is that it provides a clear, consistent, and broad-ranging methodology for managing hazards using a system safety approach including organizational structures, hazard identification and assessment, design order of precedence, and documentation. Section 4.3.5 of MIL-STD-882E requires risk reduction as follows:

*Mitigation measures are selected and implemented to achieve an acceptable risk level. Consider and evaluate the cost, feasibility, and effectiveness of candidate mitigation methods as part of the Systems Engineering and Integrated Product Team Processes. Present the current hazards, their associated severity and probability assessments, and status of risk reduction efforts at technical reviews.*

MIL-STD-882E does not go into great detail as to how the decision for acceptability is to be made by the responsible authority at the technical review when considering the cost, feasibility, and effectiveness of the candidate mitigation methods.

The FTA describes the criteria for tolerating the risk in the tolerable region of Figure 1 as follows<sup>7</sup>:

*If the risk cannot be reduced to or below the acceptable level, it may be regarded as “tolerable” if all of the following three conditions are satisfied:*

- *The risk is less than the predetermined unacceptable limit;*
- *The risk has been reduced to a level that is as low as reasonably practicable; and*
- *The benefits of the proposed system or operation are sufficient to justify accepting the risk.*

*Even though a risk may be classified as acceptable or tolerable, measures should always be sought to further reduce the level of such risk. Risks beyond the tolerable level are unacceptable.*

*It should be noted that when a transit agency “accepts” a risk, this does not mean that the risk is eliminated; some level of risk still remains. However, the agency has accepted that such risk is sufficiently low that it is outweighed by the benefits of the existing operation.*

Thus the ALARP (As Low As Reasonably Practicable) principle is introduced into the U.S. transportation industry as a method for determining risk acceptability.

The Dept. of Transportation’s Pipeline and Hazardous Materials Safety Administration (PHMSA) defines an acceptable level of risk as:

*“Acceptable Level of Risk for regulations and special permits is established by consideration of risk, cost/benefit and public comments. Relative or comparative risk analysis is most often used where quantitative risk analysis is not practical or justified. Public participation is important in a risk analysis process, not only for enhancing the public’s understanding of the risks associated with hazardous materials transportation, but also for insuring that the point of view of all major segments of the population-at-risk is included in the analyses process. Risk and cost/benefit analysis are important tools in informing the public about the actual risk and cost as opposed to the perceived risk and cost involved in an activity. Through such a public process PHMSA establishes hazard classification, hazard communication, packaging, and operational control standards.”<sup>8</sup>*

---

<sup>7</sup> *Transit Safety Management and Performance Measurement*, Federal Transit Administration Office of Safety and Security, 2011

<sup>8</sup> U.S. Dept. of Transportation, PHMSA Website Glossary of Terms <http://www.phmsa.dot.gov/resources/glossary#A>



The cost/benefit analysis prescribed by PHMSA falls in line with the ALARP principle; however the addition of the requirement for consideration of public comments adds a new element of complexity to the process, changing the perspective from which the risk is considered acceptable.

Even the United States Coast Guard is challenged with defining acceptable risk:

*In deciding how to manage risk, one key question is whether or not a risk is acceptable. Many factors influence our perception of acceptable risk. These include the following: familiarity, frequency, control, media attention, consequence, suddenness of consequence, personal versus societal, benefit, and dread. With so many factors influencing our ideas about risk, it is nearly impossible for us to define "acceptable risk". For example, what risk is acceptable with the carcinogens benzene in gasoline and asbestos in public buildings? Even though defining acceptable risk is difficult, we should not give up on the idea. By setting a risk standard, organizations can more easily identify high-risk operations, can more appropriately allocate resources, and can measure the effectiveness of their risk reduction efforts.<sup>9</sup>*

**Position of the FRA** – When Congress passed the *Rail Safety Improvement Act of 2008* it required certain railroads (including those providing intercity rail passenger transportation) to:

*Develop a comprehensive safety risk reduction program to improve safety by reducing the number and rates of accidents, incidents, injuries, and fatalities that is based on the risk analysis required by subsection (c) through —*

- (A) The mitigation of aspects that increase risks to railroad safety; and*
- (B) The enhancement of aspects that decrease risks to railroad safety.<sup>10</sup>*

Despite these rather scant instructions for managing risks, the FRA is increasingly turning to the use of risk-based hazard assessment methodology when promulgating new safety regulations. Positive Train Control (PTC) regulations contained in 49 CFR Part 236, Subpart I requires railroads to submit a description of the safety assurance concepts that are to be used for system development and a risk assessment of the as-built PTC system described. MIL-STD-882 is recognized as providing appropriate risk analysis processes and several examples of domestic and international safety analysis programs are provided for processor-based signal and train control systems<sup>11</sup>. The FRA, however, does not currently prescribe a particular risk acceptance methodology.

In order to comply with the Rail Safety Improvement Act of 2008, FRA has developed proposed rules for intercity passenger railroad that are based on the requirement for a risk-based hazard management program. The Notice of Proposed Rulemaking, however, simply requires the railroad to describe "how decisions affecting safety of the rail system will be made relative to the risk-based hazard management program"<sup>12</sup>. The FRA does not require, prescribe, or approve particular risk acceptance criteria except in the realm of Positive Train Control and signal system safety cases that require achievement of a level of safety equal to or greater than a reference system. In the context of high-speed rail, however, FRA has made it known that they would want to see providence in international high-speed rail practice with a proven safety record. The Final Rule for System Safety Programs is expected in spring of 2013.

<sup>9</sup> U.S. Coast Guard, Risk-Based Decision Making Guidelines, Volume 2, Chapter 3

<sup>10</sup> One Hundred Tenth Congress of the United States, H.R. 2095, *Rail Safety Improvement Act of 2008*, 2008

<sup>11</sup> 49 CFR Part 236, Appendix C

<sup>12</sup> 49 CFR Part 270 System Safety Program; Proposed Rule, Federal Register, Vol. 77, No. 174, September 7, 2012



### **3.2 COMMON SAFETY METHOD – THE EUROPEAN APPROACH TO HAZARD RISK ASSESSMENT**

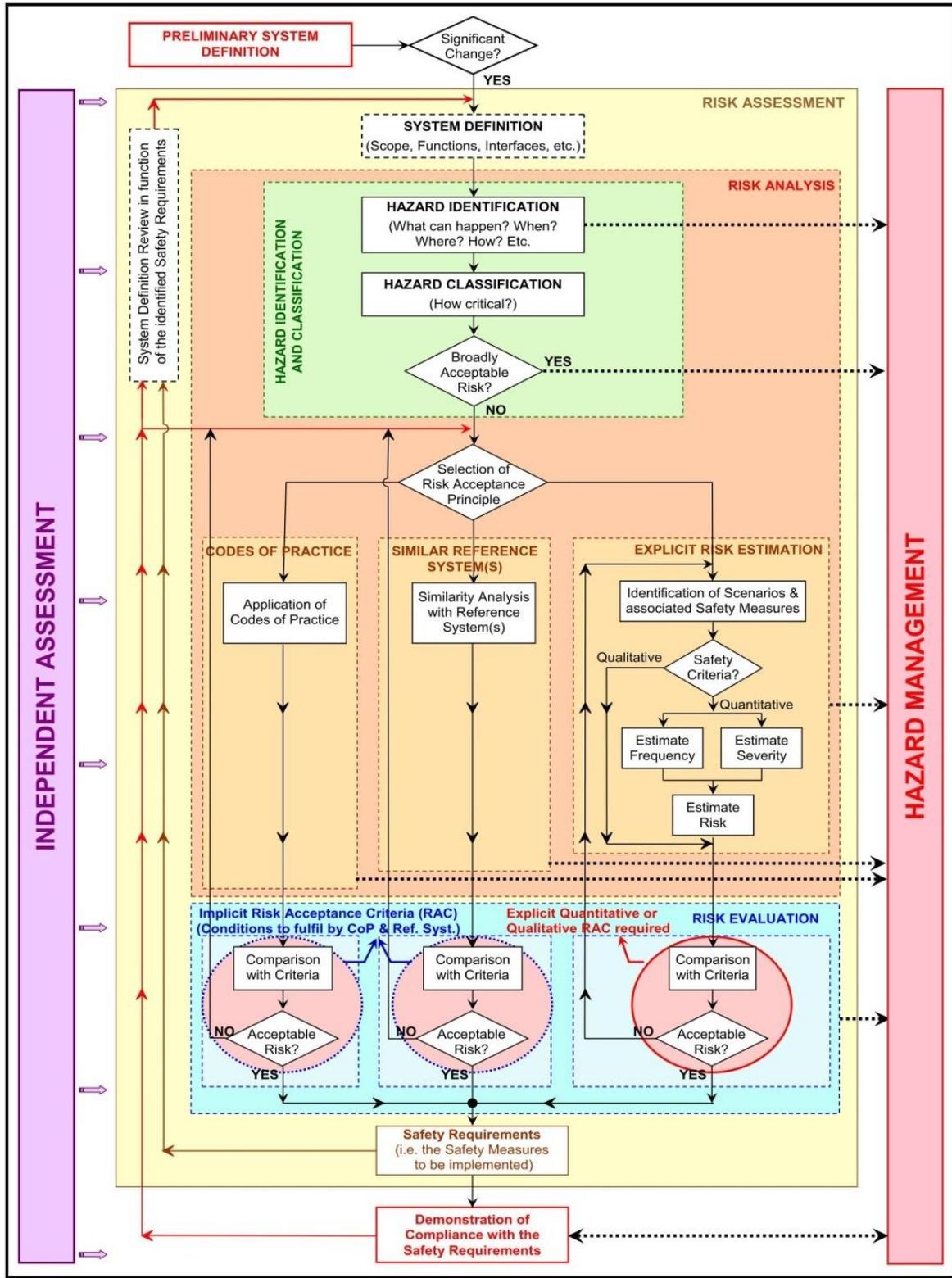
In Europe, hazard management is applied to the railroad industry (including all of the high-speed rail systems) under the regulatory authority of the European Union. European Commission Regulation 352/2009/EC of April 24, 2009 outlines a *Common Safety Method* (CSM) on Risk Evaluation and Assessment for Railways of the European Union<sup>13</sup>. 352/2009/EC is commonly known as the CSM Regulation and is at the heart of the railway safety program in Europe. Figure 2 shows the graphical representation of the risk management framework in the CSM Regulation.

---

<sup>13</sup> European Railway Agency *Common Safety Method on Risk Evaluation and Assessment*, Official Journal of the European Union, 29.4.2009, Regulation 352/2009/EC



Figure 2 – Risk Management Framework in the CSM Regulation<sup>14</sup>



<sup>14</sup> Guide for the Application of the CSM Regulation, ERA/GUI/01-2008/SAF, Version 1.1, page 26



The general principle of the CSM Regulation is as follows:

*The risk management process covered by this Regulation shall start from a definition of the system under assessment and comprise the following activities:*

- (a) the risk assessment process, which shall identify the hazards, the risks, the associated safety measures and the resulting safety requirements to be fulfilled by the system under assessment;*
- (b) demonstration of the compliance of the system with the identified safety requirements; and*
- (c) management of all identified hazards and the associated safety measures.*

*This risk management process is iterative and is depicted in the diagram of the Appendix. The process ends when the compliance of the system with all safety requirements necessary to accept the risks linked to the identified hazards is demonstrated.*

The last sentence is the key CSM Regulation reference to a requirement for an acceptable level of safety. The CSM Regulation defines risk acceptance criteria as:

*'risk acceptance criteria' means the terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further;*

The CSM Regulation includes the standard risk assessment process elements: identification of the hazards, corresponding risks, mitigation measures to reduce the risk, and the resulting safety requirements to be fulfilled by the system under assessment. What sets the CSM Regulation apart from other risk assessment programs is that it provides a methodology for determining when acceptable risk is achieved. The risk acceptability of the system under assessment is evaluated using one or more of the following risk acceptance principles:

- a) The application of relevant codes of practice;
- b) A comparison with similar systems (reference systems);
- c) Explicit risk estimation.

Codes of practice are considered if they are widely acknowledged in the railway domain, are relevant for the control of the considered hazards in the system under assessment, and are publicly available. If one or more hazards are controlled by codes of practices fulfilling these requirements then the risks associated with these hazards shall be considered as acceptable. Examples of relevant codes of practice include FRA regulations found in the Code of Federal regulations, track component standards published by the American Railway Engineering and Maintenance-of-Way Association (AREMA), and the fire & life-safety requirements for structures found in the California Fire Code.

A reference system can be used to determine risk acceptability when it has been proven in-use to have an acceptable safety level, has similar functions and interfaces as the system under assessment, is used under similar operational conditions as the system under assessment and it is used under similar environmental conditions as the system under assessment. If a reference fulfills these requirements then for the system under assessment the risks associated with the hazards covered by the reference system shall be considered as acceptable. An example of a reference system might be the application of access-control fencing standards found on the high-speed railways in Japan.



When the hazards are not covered by codes of practice or reference systems then the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. The acceptability of the estimated risks is evaluated using risk acceptance criteria based on national or European legislation, or industry best practices. Means of the application of a systematic safety management and achieving explicit risk estimation in the international railway community can be found in *European Norm EN 50126-1- Railway applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)*<sup>15</sup> as published by the European Committee for Electrotechnical Standardization (aka CENELEC). EN 50126-2: Systems Approach to Safety provides guidance on the application of three risk acceptance principles: ALARP, GAMAB, and MEM. Each of these principles will be examined individually in Section 3.4.

Explicit risk estimation is the systematic and structured use of all available information to identify hazards and estimate the associated risk. The estimated risk can then be compared against the risk acceptance criteria to determine the acceptability of the risk (i.e. whether additional mitigation measures need to be applied to further reduce the risk). The risk analysis methodology consists of:

1. Hazard identification
2. Estimating the frequency of occurrence and severity of consequence of the identified hazard
3. Determining measures of mitigation to reduce the hazard risk to an acceptable level
4. Identifying the level of residual risk acceptable to the Authority
5. Documenting the risk analysis process

The estimation of risks can be quantitative if sufficient data is available in terms of frequency of occurrence and severity of consequence, qualitative if sufficient is not fully available or known, or a hybrid of the two. Qualitative assessment should be based on the judgment of qualified technical experts following a clear process for defining and analyzing the risk. EN50126-1 provides a good process for qualifying the technical experts, as described in Appendix A of this Tech Memo.

The CSM Regulation provides the framework for the risk assessment and evaluation process, but does not prescribe actual risk assessment techniques or processes. Those risk assessment techniques or processes are left up to the responsible party to develop and to demonstrate to the independent assessment body their relevance to the system under assessment. A set of EN50126 standards, which are also adopted by the International Electrotechnic Commission (IEC) as international standards, provide guidance on risk assessment techniques, processes, and documentation relevant to railway applications. The risk assessment methodology found in EN50126-1 is based upon the foundation of the Department of Defense MIL-STD-882 and is consistent with FRA and FTA requirements and guidance. The risk assessment techniques currently found in the CHSTS Safety and Security Management Plan, while consistent with EN50126-1, are updated to reflect conformance to recent changes to the guidance of EN50126-1 as described in Appendix A of this Tech Memo.

---

<sup>15</sup> EN 50126-2 *Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) Part 2: Guide to the application of EN 50126-1 for safety*, CENELEC, 2007



A key distinction of the CSM regulation is the assessment of hazards that arise from the failure of technical systems<sup>16</sup> not covered by codes of practice or the use of a reference system. For such hazards that have credible direct potential for catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to  $10^{-9}$  per operation hour.

The outcome of the three forms of risk assessment is the development of safety requirements that must be fulfilled in order for the risk to be deemed acceptable. Additional key components of the CSM Regulation include the independent assessment of the demonstration of compliance with the safety requirements by an assessment body not affiliated with the responsible party, and explicit requirements for the documentation and management of hazards and mitigations throughout the risk assessment process and the life cycle of the railway system.

### 3.3 OTHER INTERNATIONAL APPROACHES TO RISK ACCEPTANCE

In Japan risk acceptance criteria are not prescribed by regulation. Rather, the railways are left to develop their own risk acceptance criteria based upon their excellent safety record for high-speed operations (nearly 50 years without a fatality). The result is a mix of quantitative and qualitative risk assessments based upon accident/incident data and operational experience. The Japanese also introduce social values into the equations as well, however, allowing for social norms and perceptions in the decision of whether to accept a risk or not<sup>17</sup>. The result is a decision-making process that is influenced by the ownership, pride, and sense of responsibility toward the high-speed *Shinkansen* train system. Considering the different socio-economical, political and regulatory environment in the United States, the Japanese approach to risk assessment is not applicable to the California High-Speed Train System.

The Taiwan High-Speed Rail Corporation follows the EN 50126 standard and has established safety targets to determine the maximum level of tolerable (acceptable) risk. These safety targets are expressed in equivalent fatalities per year and are divided into three categories: passenger risk, staff risk, and public risk. Risk is assessed and the ALARP Principle is then applied by the Taiwan High-Speed Rail Corporation to determine whether additional resources should be applied to reduce the risk below the safety targets. The safety targets were developed internally and reflect the corporate and societal norms specific to the Taiwan High-Speed Rail Corporation. Note that these quantified safety targets are applied to ALL hazards, not just the hazards associated with technical systems as prescribed by the CSM Regulation.

The Chinese high-speed rail system has suffered several serious train accidents and engineering failures and is not to be considered as a standard for acceptable safety performance.

The Korean high-speed rail system applies a risk assessment program modeled after the CSM Regulation.

### 3.4 RISK ASSESSMENT PROCESS

The risk assessment techniques currently found in the CHSTS Safety and Security Management Plan, while consistent with EN50126-1, are updated to reflect conformance to recent changes to the guidance of EN50126-1.

---

<sup>16</sup> By the CSM Regulation "technical system" means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;

<sup>17</sup> *Risk Assessment for JR East*, Ken Kusakami, International Railway Safety Conference 2011, Melbourne, Australia



### 3.4.1 Severity of Consequence

Severity definitions are applied to hazards and used to rate hazard consequences. The objective of establishing severity definitions is to provide a method to prioritize hazards so that the hazard management team can concentrate on the most severe hazards first. Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personal error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. The severity category is assigned to the hazard for a specific condition at a given point in time; the hazard severity definitions should be re-evaluated as the hazard evolves due to changes in environmental conditions, operating procedures, or system or subsystem makeup.

FRA suggests basing the severity definition categories on those found in MIL-STD-882 but with modifications specific to the railway system under consideration<sup>18</sup>. FRA suggests adding a category for multiple deaths, since on a railroad even a minor accident or low-speed collision can lead to the death of an individual and placing a disproportionate amount of hazards in the *catastrophic* category. FRA also suggests considering the level of system loss when assessing the severity of a hazard. Considering system loss is not meant to downplay the occurrence of a serious or fatal personal injury, but the level of system loss provides an additional tool to determine the relative severity of a hazard. For example, an accident that destroys a bridge or tunnel could shut down passenger rail service for an extended period of time. Therefore a hazard that causes this level of disruption should probably be considered critical or catastrophic, even if the hazard does not generate personal injuries. Likewise, the use of monetary value as a marker for severity definition provides an additional tool to determine the relative severity of a hazard but is not used to define the value of an injury or fatality.

The proposed definitions for hazard severity found in Table 1 are based upon Mil. Std. 882E, modified for application to a high-speed train system. The term “equivalent fatality” recognizes that passenger trains carry large numbers of persons, and the cumulative effect of numerous non-fatal injuries must be considered when assessing the severity of a hazard. It is an expression of fatalities and weighted injuries and a convention for combining injuries and fatalities into one figure for ease of evaluation and comparison of risks<sup>19</sup>. Per the latest draft update of EN50126-1, an equivalent fatality may be expressed as 10 major injuries (those requiring hospitalization) or 100 minor injuries (those not requiring hospitalization).

---

<sup>18</sup> *Collision Hazard Analysis Guide: Commuter and Intercity Passenger Rail Service*, Federal Railroad Administration Office of Safety, October 2007

<sup>19</sup> *EN 50126-1 Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) Part 1: Generic RAMS Process*, Draft update, CENELEC, 2012



**Table 1 Hazard Severity Categories**

Hazard Category	Definition
1 Catastrophic	Could result in one or more of the following: <ul style="list-style-type: none"> <li>• Multiple fatalities or equivalent fatalities</li> <li>• Irreversible significant environmental impact</li> <li>• Monetary loss equal to or exceeding \$10M               <ul style="list-style-type: none"> <li>○ Severe damage or total loss of rolling stock</li> <li>○ Severe damage to infrastructure or other severe system loss causing all or a significant portion of the system to be unavailable for normal service for more than 72 hours</li> </ul> </li> <li>• Reputational damage of national impact</li> </ul>
2 Critical	Could result in one or more of the following: <ul style="list-style-type: none"> <li>• A single fatality or multiple major injuries or occupational illnesses</li> <li>• Reversible significant environmental impact</li> <li>• Monetary loss equal to or exceeding \$1M but less than \$10M               <ul style="list-style-type: none"> <li>○ Major but repairable damage to rolling stock</li> <li>○ Major damage to infrastructure or other major system loss, repairable within 72 hours to allow normal service</li> </ul> </li> <li>• Reputational damage of statewide impact</li> </ul>
3 Serious	Could result in one or more of the following: <ul style="list-style-type: none"> <li>• A major injury or occupational illness, or multiple minor injuries</li> <li>• Reversible moderate environmental impact</li> <li>• Monetary loss equal to or exceeding \$100K but less than \$1M               <ul style="list-style-type: none"> <li>○ Minor repairable damage to railcars</li> <li>○ Minor damage to infrastructure or other minor system loss, repairable within 24 hours to allow normal service</li> </ul> </li> <li>• Reputational damage of local area impact</li> </ul>
4 Marginal	Could result in one or more of the following: <ul style="list-style-type: none"> <li>• A minor injury or occupational illness</li> <li>• Minimal environmental impact</li> <li>• Monetary loss less than \$100K               <ul style="list-style-type: none"> <li>○ Minimal infrastructure damage or system loss affecting normal service for less than 12 hours</li> </ul> </li> <li>• Reputational damage of limited or little impact</li> </ul>

It is important to note that the severity categories are only meant as guidance for assessing the relative characterization of the severity of the hazard. The definitions should be as broad as possible, allowing the assessors plenty of leeway for making their qualitative assessment.

### 3.4.2 Frequency of Occurrence

Frequency definitions are used to establish how often identified hazards emerge. Estimating the frequency of occurrence means estimating the likelihood that a hazardous event is to occur for a given number of total events. Frequency can be expressed as a percentage of events, or as a Mean Time To Hazardous Event (MTTHE). The frequency of the hazard can be determined quantitatively (using failure rates or accident incident statistical data) or qualitatively based on the relative frequency of expected occurrence<sup>20</sup>. Quantitative determination is generally preferable,

<sup>20</sup> *Collision Hazard Analysis Guide: Commuter and Intercity Passenger Rail Service*, Federal Railroad Administration Office of Safety, October 2007



but in the absence of applicable quantitative data the use of qualitative estimation is necessary and appropriate<sup>21</sup>.

Table 2 identifies both a qualitative and quantitative definition MTTHE, based upon a railway operation 20 hours per day, 7 days per week, plus a quantitative context for the probability of occurrence of an event.

**Table 2 Hazard Frequency Categories**

Description	Level	Qualitative Definition	Quantitative Definition MTTHE	Quantitative Context (Probability of Occurrence)
Frequent	A	Likely to occur frequently in an individual item or the System; may be continuously experienced in fleet/inventory.	MTTHE < 2 mos	$p > 10^{-1}$
Probable	B	Likely to occur several times in the life of an individual item or the System; will occur frequently in fleet/inventory.	2 mos < MTTHE < 1 yr	$10^{-1} > p > 10^{-2}$
Occasional	C	Likely to occur sometime in the life of an individual item or the System; will occur several times in fleet/inventory.	1 yr < MTTHE < 10 yrs	$10^{-2} > p > 10^{-3}$
Remote	D	Unlikely but possible to occur in the life of an individual item or the System; unlikely but can be expected to occur in fleet/inventory.	10 yrs < MTTHE < 100 yrs	$10^{-3} > p > 10^{-6}$
Highly Unlikely	E	So unlikely that it can be assumed occurrence may not be experienced in the life of an individual item or the System; unlikely but possible to occur in fleet/inventory.	MTTHE > 100 yrs	$10^{-6} > p$
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.	T = 0	p = 0

Frequency level F is used to document cases where an identified hazard is no longer present. No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap probability to level F.

<sup>21</sup> U.S. Dept. of Defense Military Standard 882E, *Standard Practice for System Safety*, May 2012



### 3.4.3 Risk Assessment Matrix

Assessed risks are expressed as a Risk Assessment Code which is a combination of one severity category and one frequency category, plotted on a Risk Assessment Matrix. The Risk Assessment Matrix reflects the amount of risk the Authority is willing to accept, and conversely the amount is risk the Authority is not willing to accept. The region between the Acceptable and Unacceptable regions is the Undesirable/Tolerable region; risks falling within this region must be mitigated toward acceptability using Risk Acceptance Criteria as described in Section 3.5 of this Technical Memorandum.

MIL-STD-882 provides the foundation for most risk assessment matrixes in use in the world today. Indeed, both EN50126-1, FTA's Hazard Analysis Guidelines for Transit Projects, and FRA's Collision Hazard Analysis Guide all point to MIL-STD-882 as guidance for the establishment of a Risk Assessment Matrix. The Risk Assessment Matrix shown in Table 3 is based upon MIL-STD-882(E), modified to suit the particular needs of the CHSTS.



**Table 3 Risk Assessment Matrix**

Probability \ Severity	1 Catastrophic	2 Critical	3 Marginal	4 Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Highly unlikely	1E	2E	3E	4E
(F) Eliminated				

The Risk Acceptance Matrix (Table 4) identifies required actions to reduce risk based on the risk rating. The Authority will accept the residual risk through the Safety and Security Executive Committee process where appropriate; direct approval of individual risk acceptance decisions for hazard risks categorized as *High*, or review and approval of hazard analysis reports for hazard risks categorized as *Moderate*. Hazard risks categorized as *Acceptable* do not require SSEC review and approval.

**Table 4 Risk Acceptance Matrix**

Hazard Risk Index	Risk Rating	Action Required
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable	Risk must be reduced and managed
1D, 2C, 3B, 4A	Undesirable	Risk is acceptable only where further risk reduction is impracticable. Authority decision required to accept residual risk
1E, 2D, 2E, 3C, 3D, 4B, 4C	Tolerable	Apply mitigations where reasonably practicable. Risk can be tolerated and accepted with adequate controls. Authority review required to accept residual risk.
3E, 4D, 4E	Acceptable	No further risk reduction required
	Eliminated	None

### 3.5 POTENTIAL APPROACHES TO RISK ACCEPTANCE CRITERIA

Where explicit risk estimation is used to evaluate hazard risk, risk acceptance criteria must be applied. EN 50126-2 describes in detail three approaches to risk acceptance criteria that can be applied to railway applications: ALARP, GAMAB, and MEM.

#### 3.5.1 ALARP - As Low As Reasonably Practicable

This principle weighs the benefits of mitigation against the cost in resources to apply the mitigation, usually through the application of a monetary cost/benefit analysis. EN 50126-2 describes the acceptance criteria for the ALARP principle as “Risk reduction needed as long as



the system stays within the tolerable or intolerable region. The reduction actions will be stopped if the system is in the broadly acceptable region or it is in the tolerable region and the needed effort of further risk reduction is grossly disproportionate to the improvement gained.” The ALARP principle is a legislative requirement of the railway industry in the United Kingdom.<sup>22</sup>

Similar legal requirements do not exist here in the United States, however the application of the ALARP Principle for domestic explicit risk estimation would follow the guidance put forth by the ANSI in a second definition of acceptable risk:

*The risk for which the probability of an incident or exposure occurring and the severity of harm or damage that may result are as low as reasonably practicable in the setting being considered*<sup>23</sup>.

FTA also identifies the ALARP principle as a means of placing a risk in the tolerable region of the risk diagram (Figure 1) and further describes the ALARP principle as:

*The acronym ALARP is used to describe a risk that has been reduced to a level that is “as low as reasonably practicable.” In determining the threshold for what is “reasonably practicable” in this context, threshold should be given to both the technological feasibility of further reducing the risk and the associated cost. The ALARP principle makes use of the law of diminishing marginal returns to identify the point beyond which the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained. Additional investments begin to have a declining degree of impact on risk reduction.*<sup>24</sup>

When using the ALARP principle, only those solutions that are technologically feasible are considered, an important point when defining the scope of hazard mitigations.

A strength of the ALARP principle is that it does not require identification of a reference system; however it does require the development of some qualitative metrics for risks that do not have existing estimates of quantitative risk targets.

FRA has also made reference to ALARP, most recently in a report to Congress on the progress of implementing the positive train control requirements of the *Railway Safety Improvement Act of 2008*. The report to Congress (published in August 2012) justifies a proposed extension of the deadline for implementing PTC thusly:

*This suggestion is based on the assumption that the societal objective is to establish levels of risk that are as low as reasonably possible (ALARP). For a risk to be ALARP, it must be possible to demonstrate that the cost involved in reducing the risk further would be disproportionate to the benefit gained. The ALARP principle arises from the fact that infinite time, effort, and money could be spent on the attempt of reducing a risk to zero. It should not be understood as a quantitative measure of benefit against detriment. It is rather a best common practice of judgment of the balance of risk and benefit.*

The last point is an important one. ALARP does not identify a direct monetary value for the hazard consequence, but rather provides a process by which the cost of mitigations to reduce the risk further can be compared against the benefit (in this case risk reduction). For physical elements of the system a cost of replacement and loss of use can be calculated. Calculating the

---

<sup>22</sup> ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation, U.K. Office of Rail Regulation, September 2010

<sup>23</sup> ANSI Z590.3 *Prevention through Design*, American National Standards Institute, 2011

<sup>24</sup> *Transit Safety Management and Performance Measurement*, Federal Transit Administration Office of Safety and Security, 2011



cost of injuries or fatalities, however, is more challenging and controversial. A common method is to equate personal injuries to a common denominator of a theoretical fatality, and then apply a monetary value to cost of preventing a theoretical fatality, known as the “value of statistical life” (VSL). The U.S. Department of Transportation (DOT) defines VSL as:

*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.<sup>25</sup>*

The DOT identified VSL in 2013 at \$9.1 million. The DOT has also identified the VSL coefficients for a range of injury severities (abbreviated injury scale - AIS), as shown in Figure 3.

**Figure 3 – Relative Disutility Factors by Injury Severity Level**

AIS Level	Severity	Fraction of VSL
AIS 1	Minor	0.003
AIS 2	Moderate	0.047
AIS 3	Serious	0.105
AIS 4	Severe	0.266
AIS 5	Critical	0.593
AIS 6	Unsurvivable	1.000

The DOT guidance document goes on to identify the benefit of using VSL when making a cost/benefit analysis of safety improvements:

*These factors have direct application in analyses as a basis for establishing the value of preventing nonfatal injuries in benefit-cost analysis. The total value of preventing injuries and fatalities can be combined with the value of other economic benefits not measured by VSLs, and then compared to costs to determine either a benefit/cost ratio or an estimate of net benefits.*

Clearly, the use of VSL for calculating ALARP has providence within the realm of the U.S. Department of Transportation, including high-speed rail systems.

### **3.5.2 GAMAB - Globalement Au Moins Aussi Bon**

Translated as “All new guided transport systems must offer a level of risk globally as good as the one offered by any equivalent existing system”<sup>26</sup>, GAMAB is the principle risk acceptance criteria as applied in France. EN 50126-2 describes the acceptance criteria for the GAMAB principle as “The new system is less risky or equal compared with the existing (old) system”. A strength of the GAMAB principle is that it keeps, at least, the existing level of safety and tends to improve the level of safety. A weakness of the GAMAB principle is that it requires the identification of a similar reference system with experience data. The complete formulation of this principle

<sup>25</sup> U.S. Dept. of Transportation Guidance *Treatment of the Value of Preventing Fatalities and Injuries in Preparing Economic Analyses*, 2013

<sup>26</sup> EN 50126-1 *Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) Part 1: Basic requirements and generic process*, CENELEC, 1999



translates to “All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system”.

### 3.5.3 MEM (Minimum Endogenous Mortality)

The calculation of a tolerable hazard rate is directly derived from a common independent safety target, typically the mortality rate for members of the national population. That is, the risk of a fatal accident to a person riding the high-speed train system should not be greater than the risk to that same person dying of other causes that day. EN 50126-2 describes the acceptance criteria for the MEM principle as “The individual risk (fatalities per person and time) caused by the system is lower than the tolerable risk derived from MEM”. The MEM principle is applied as risk acceptance criteria for the German railway systems.

## 4.0 SUMMARY AND RECOMMENDATIONS

### 4.1 SUMMARY

Risk-based hazard management allows an entity to make decisions according to the amount of risk involved with a particular situation or piece of infrastructure. Both the probability and consequences are considered when making a decision to manage a particular hazard, and the residual risk is assessed. Risk acceptance criteria describe the baseline by which the Authority can determine acceptance of residual risk, established so that the Authority can make a consistent, informed decision about how to accept that residual risk.

Risk-based hazard management is increasingly recognized as an appropriate strategy for managing risks, and soon will be a regulatory requirement of the Federal Railroad Administration. The European-based *Common Safety Method* represents an accepted process for risk-based hazard management in the railway sector. The ALARP principle is an internationally-accepted method for accepting residual risk for those hazards that must be estimated for their probability of occurrence and consequences. The *Common Safety Method*, combined with use of the ALARP principle where appropriate, represents an appropriate risk acceptance strategy for the California High-Speed Train System.

### 4.2 RECOMMENDATIONS

**Recommendation #1** - It is recommended that the *Common Safety Method* (CSM) be adopted as the method for assessing hazard risk and determining risk acceptability, as identified in Appendix A. Appendix A demonstrates the application of CSM to Sections 4.0, 4.1, and 4.2 of the *CHSTS Safety and Security Management Plan* (SSMP) and is meant as an in-kind replacement of those sections in the SSMP. The CSM is used as a reference process for the development of this Appendix A, but is modified to conform to the characteristics and requirements specific to the development of the California High-Speed Train System.

**Recommendation #2** - It is also recommended that the ALARP Principle be used as the method for determining acceptable risk in support of the Explicit Risk Estimation process of CSM, also as identified in Appendix A.



## 5.0 SOURCE INFORMATION AND REFERENCES

- *ANSI B11.0 Safety of Machinery: General Requirements and Risk Assessment*, American National Standards Institute, 2010
- *ANSI Z590.3 Prevention through Design*, American National Standards Institute, 2011
- *ANSI Z690.3 Risk Assessment Techniques*, American National Standards Institute, 2011
- *EN 50126-1 Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) Part 1: Basic requirements and generic process*, CENELEC, 1999
- Draft update to *EN 50126-1 Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) Part 1: Basic requirements and generic process*, CENELEC, 2012
- *EN 50126-2 Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) Part 2: Guide to the application of EN 50126-1 for safety*, CENELEC, 2007
- European Railway Agency *Common Safety Method on Risk Evaluation and Assessment*, Official Journal of the European Union, 29.4.2009, Regulation 352/2009/EC
- European Railway Agency *Guide for the Application of the CSM Regulation*, ERA/GUI/01-2008/SAF, Version 1.1, page 26
- Federal Railroad Administration 49 CFR Part 236, Appendix C, Rules for Signal and Train Control, Safety assurance Criteria and Processes
- Federal Railroad Administration Notice of Proposed Rulemaking, 49 CFR Part 270, Federal Register, Vol. 77, No. 177, 9/7/2012
- Federal Railroad Administration *Collision Hazard Analysis Guide: Commuter and Intercity Passenger Rail Service*, October 2007
- Federal Railroad Administration *Report to Congress: Positive Train Control – Implementation Status, Issues, and Impacts*, August 2012
- Federal Transit Administration *Hazard Analysis Guidelines for Transit Projects*, January 2000
- Federal Transit Administration manual *Transit Safety Management and Performance Measurement*, FTA Office of Safety and Security, 2011
- One Hundred Tenth Congress of the United States, H.R. 2095, *Rail Safety Improvement Act of 2008*, 2008
- *ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation*, U.K. Office of Rail Regulation, September 2010
- U.S. Coast Guard, *Risk-Based Decision Making Guidelines*, Volume 2, Chapter 3
- U.S. Dept. of Defense Military Standard 882E, *Standard Practice for System Safety*, 2012
- U.S. Dept. of Transportation Guidance *Treatment of the Value of Preventing Fatalities and Injuries in Preparing Economic Analyses*, 2013



## **4.0 HAZARD AND THREAT/VULNERABILITY MANAGEMENT**

### **4.1 Overview**

A hazard is a condition or circumstance that could lead to an unplanned or undesired event which, when it occurs, can cause injury, illness, death, damage or loss of equipment or property, or severe environmental damage.

Threats are specific intentional acts that will damage the system, its facilities, or its patrons. Threats include any intentional actions which detract from overall security. They range from the extreme of terrorist-initiated bombs or hostage-taking to more common events such as theft of services, pick pocketing, graffiti and vandalism. Vulnerability is defined as the susceptibility of the system to a particular type of security threat. Threat/vulnerability management is detailed in Section 4.3.

A risk assessment process for the management of safety hazards and security threats/vulnerabilities will be used for the CHSTS. The purpose of the process is as follows:

- Identify and evaluate the effects of hazardous conditions and security threats/vulnerabilities on passengers, CHSTS personnel, CHSTS infrastructure and equipment in order to apply mitigation measures that allow the Authority to achieve an acceptable level of risk;
- Define and evaluate mitigation measures to eliminate or control the identified hazards and security threats/vulnerabilities;
- Document the development and incorporation of safety and security mitigation measures on a Certifiable Elements and Hazards Log (CEHL) during System development and implementation, demonstrating how an acceptable level of safety and security is to be achieved.

The development of the safety hazard analyses and threat/vulnerability assessments will be coordinated with the appropriate engineering disciplines for the identification of applicable hazards/security threat issues and recommended control measures. Supporting documentation will be submitted to the SSPC for review. The SSPC will elevate the reports to the Authority, through the SSEC, as appropriate to the processes described in Section 3.3.2.

Hazard and threat/vulnerability management processes will be applied to the development of the System throughout the entire System life cycle. As the System enters Final Design, the design/build contractors will review and update the CEHL for the geographic section under consideration, and work with the Authority to perform or support other analyses as warranted by local or site-specific conditions or designs. Any deviations to the Design Criteria will follow the procedures outlined in section 5.4. Other hazards or threats/vulnerabilities may be identified during the normal course of work on the development of the CHSTS, including such activities as design reviews, construction inspection and testing, and start-up and integrated testing. Additional hazards or threats/vulnerabilities identified during these activities will also require a hazard analysis or threat/vulnerability assessment to be performed.

The SSPC will be responsible for reviewing and approving all hazard analyses and threat/vulnerability assessments to ensure that significant safety hazards and security threats/vulnerabilities are identified and that the proposed mitigations allow the Authority to achieve an acceptable level of risk. The SSPC will monitor the status of the identified hazards and threats/vulnerabilities from initial identification through final resolution and closure in conformance with the V&V process and by utilizing reports from the V&V Requirements Management Tool database. Sensitive security issues will be tracked on a separate log per the CHSTS SSI Program.

## 4.2 Risk-Based Hazard Management

Risk-based hazard management addresses hazards to the system based upon the amount of risk, both the severity and frequency, posed by the hazard. Hazards that represent higher levels of risk will receive higher levels of resources and analysis.

The risk-based hazard management process is the overall iterative process that comprises:

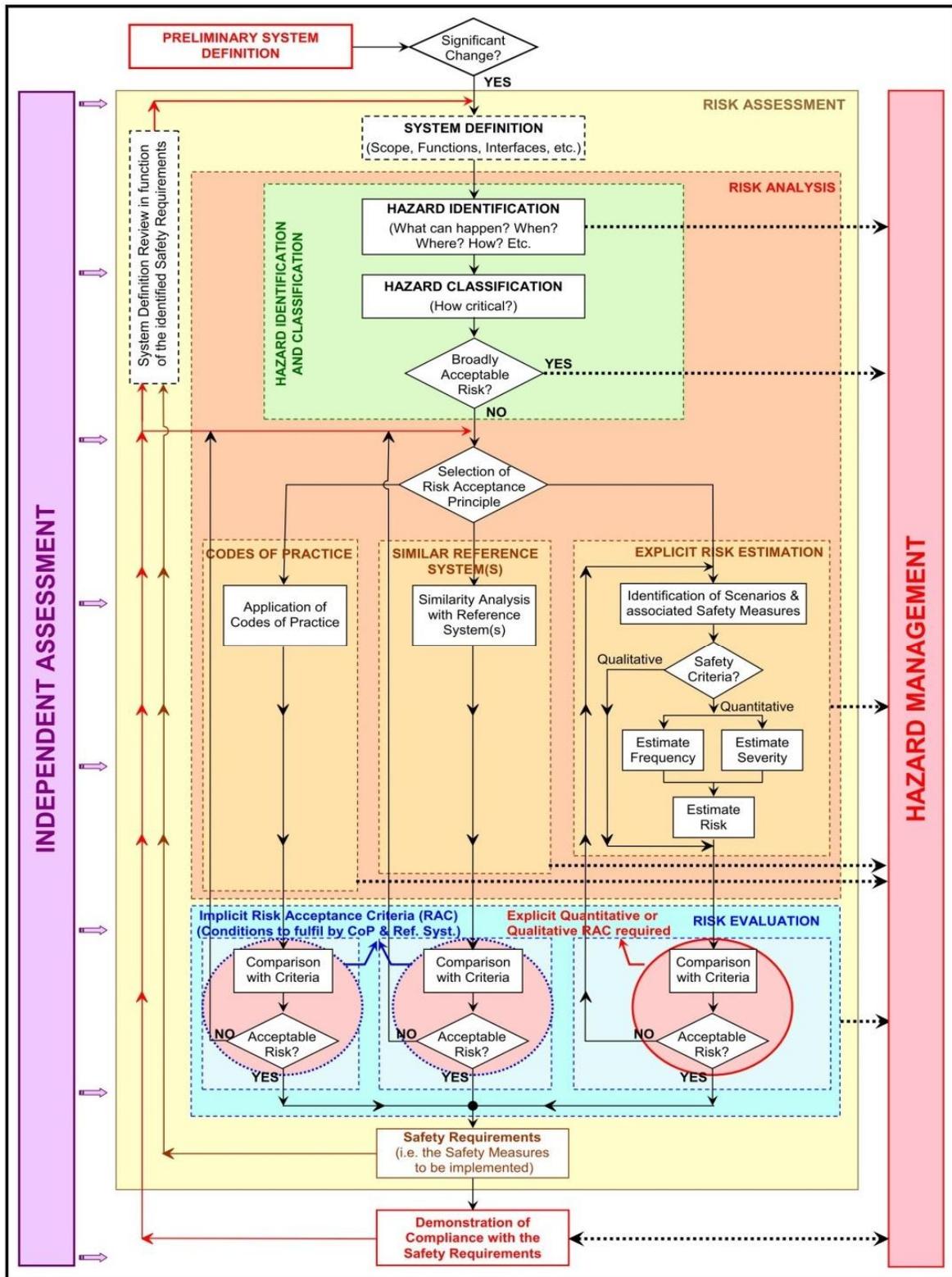
- System definition;
- Hazard identification;
- Risk analysis;
- Accepting residual risk after the application of measures of mitigation; and
- Verification and validation of implemented hazard management elements.

Risk-based hazard management shall be the responsibility of the Authority or its designated representative, but subject to review by an Independent Safety Assessment body (ISA). Risk-based hazard management will begin at the system level and flow-down to sub-system or site-specific levels as appropriate to capture relevant information and sufficient detail to provide appropriate input to the hazard analysis process.

### 4.2.1 Application of Risk-Based Hazard Management – The Common Safety Method

Risk-based hazard management shall be applied to a new system or sub-system and to significant safety-related technical, operational, or organizational changes to the CHSTS using a process called Common Safety Method (CSM). The CSM applied to the CHSTS is based upon the process identified in the European Commission Regulation No. 352/2009 and described in the UK Office of Rail Regulation's (ORR) *Guidance on the Application of the Common Safety Method (CSM) on Risk Evaluation and Assessment*, December 2012. The main phases of the CSM process are illustrated in Figure 4-1. Note – the significant change referenced in the flow-chart also implies application to new systems or sub-systems.

Figure 4-1 – The Common Safety Method Process



To determine the significance of a new system sub-system, or change the following six criteria should be examined:

- Failure consequence: most reasonable credible mishap scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;
- Novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organization implementing the change;
- Complexity of the change;
- Monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;
- Reversibility: the inability to revert to the system before the change; and
- Additionality: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

Guidance on determining significance can be found in SSMP Appendix G *ORR Guidance on the Application of the CSM, Annex 1, December 2012*.

Technical changes are changes to structural and functional railway sub-systems. Technical changes should also be reviewed to determine whether they introduce changes to the operation of the railway sub-system under consideration.

Operational changes are:

- Changes to the operation of the CHSTS as a whole;
- Changes to the operation of a structural CHSTS sub-system; or
- Changes to the operating rules of the CHSTS.

Changes to the operation of a CHSTS sub-system may be caused by technical changes to that sub-system. In this case, the technical change and its effect on the operation of the CHSTS sub-system, and any changes to the operation or operating rules of the CHSTS system, should be assessed together. For example a change in the wayside signaling may result in increased line capacity. The technical change (new wayside signals) should be assessed together with the operational change (added trains to the line). However, changes to the operation or operating rules of the CHSTS system can be introduced without a related technical change. The CSM should be used to assess whether these changes, if they are safety-related, are significant or not. If they are significant, the CSM should be applied to these changes.

Technical changes to a sub-system can also introduce changes to the operating rules of the railway system. Changes to the operating rules of the CHSTS should be considered together with the technical change, the change to the operation of the affected CHSTS sub-system, and any change to the operation of the CHSTS as a whole.

Organizational changes are changes to the organization of an actor or entity within the CHSTS which could impact on the safety of the CHSTS. The “actor” could be any organization (Authority, contractor, sub-contractor, etc) that directly affects the safety of the CHSTS. Guidance on organizational changes can be found in SSMP Appendix H *ORR Guidance on the Application of the CSM, Annex 4, December 2012*.

#### 4.2.2 System Definition

The CSM process starts with the system definition. This provides the key details of the new system or the system that is being changed - its purpose, functions, interfaces and the existing safety measures that apply to it. In most cases, the hazards which need to be analyzed will exist at the boundary of the system with its environment. The definition is not static and during iterations of the risk management process, it should be reviewed and updated with the additional safety requirements that are identified by the risk analysis. It, therefore, describes the condition (or expected condition) of the system before the change, during the change and after the change.

The system definition shall address at least the following issues:

- System objective, e.g. intended purpose;
- System functions and elements, where relevant (including e.g. human, technical and operational elements);
- System boundary including other interacting systems;
- Physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;
- System environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);
- Existing mitigation measures and definition of the safety requirements identified by the hazard risk assessment process;
- Assumptions which shall determine the limits for the hazard risk assessment.

The system definition needs to cover not only normal mode of operations but also degraded or emergency mode.

Consideration of interfaces should not be restricted to physical parameters, such as interfaces between wheel and rail. It should include human interfaces, for example the user-machine interface between the locomotive engineer and displays in the cabs of rail vehicles. It should also include interfaces with non-railway installations and organizations, for example, the interface with underground utilities.

Operational procedures and rules, and staff competence should be considered as part of the system environment in addition to the more usual issues such as weather, electromagnetic interference, local conditions such as lighting levels, etc. The system definition is complete and sufficient if it describes the system elements, boundaries and interfaces, as well as what the system does.

The description can effectively serve as a model of the system and should cover structural issues (how the system is constructed or made up) and operational issues (what it does, and how it behaves normally and in failure modes). The existing safety measures, which may change as the risk assessment process progresses, can be added after the structural and operational parts of the model are complete.

The hazard assessor may not know all the environmental or operational conditions in which the altered or new system will operate. In these circumstances, they should make assumptions on the basis of the intended or most likely environment. These assumptions will determine the initial limits of use of the system and should be recorded. When the system is put into use, the hazard assessor (who may be different to the original proposer) should review the assumptions and analyze any differences with the intended environmental and operational conditions.

#### 4.2.3 Hazard Identification and Classification

The Authority shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate, and its interfaces. Scope of hazards shall be limited to those hazards that directly or indirectly affect the

safety of passengers, employees, rolling stock, and facilities of the CHSTS. All identified hazards shall be registered in the CEHL.

The purpose of the hazard identification is to identify all reasonably foreseeable hazards which are then analyzed further in the next steps.

The hazard identification should be systematic and structured, which means taking into account factors such as:

- The boundary of the system and its interactions with the environment
- The system's modes of operation (i.e. normal/degraded/emergency)
- The system life cycle including maintenance
- The circumstances of operation (e.g. proximity to freight-only line, tunnel, bridge, etc.)
- Human factors
- Environmental Conditions
- Relevant and foreseeable system failure modes

Relevant tools for hazard identification include structured brainstorming, checklists, task analysis, operations analysis, preliminary hazard analysis, and failure modes and effects analysis. Whichever technique is used, it is important to have the right mixture of experience and competence while maintaining impartiality and objectivity. Correct hazard identification will underpin the whole risk assessment process and give assurance that the risks will be managed in the project.

Preliminary Hazard Analysis (PHA) shall be performed in order to identify an initial risk index for hazard classification and to form a basis for risk acceptance. Development of the PHA involves identifying the severity of consequence and frequency of occurrence before the application of mitigation measures, using the risk estimation process and risk acceptance criteria identified in Section 4.2.5. The PHA form shall be completed in accordance with the PHA process identified in SSMP Appendix I.

Development of the PHA will allow classification of the hazard as broadly acceptable or not. Based on expert judgment, hazards associated with a broadly acceptable risk need not be analyzed further but shall be registered in the CEHL. In this context, 'broadly acceptable' applies to those hazards where the risk is, to all intents and purposes, insignificant or negligible. Their acceptable classification shall be justified in order to allow acceptance by the Authority.

The level of detail of the hazard identification depends on the system that is being assessed and needs to be sufficient to ensure that relevant safety measures can be identified. If it can be successfully demonstrated that a hazard can be controlled by application of one of the three risk assessment principles identified in the CSM, following high-level hazard identification, then no further hazard identification is necessary. If it is not possible to have sufficient confidence at this stage, then further analysis of the causes of these high level hazards is undertaken to identify relevant measures to control the risks arising. The risk assessment process continues until it can be shown that the overall system risk is controlled by one or more of the risk assessment principles.

Hazard identification is still necessary for those systems/sub-systems/changes where the hazards are controlled by the application of codes of practice or by comparison to reference systems. Hazard identification in these cases will serve to check that all the identified hazards are being controlled by relevant codes of practice or by adopting the safety measures for an appropriate in-use system. This will also support mutual recognition and transparency. The hazard identification can then be limited to verification of the relevance of the codes of practice or reference systems, if these completely control the hazards, and identification of any deviations from them. If there are no deviations, the hazard identification may be considered complete.

During the hazard identification, mitigation measures may be identified as well. Potential mitigation measures shall be registered in the CEHL.

The hazard identification only needs to be carried out at a level of detail necessary to identify frequency and severity of the hazard, plus potential mitigations. Development of sub-system analysis may be necessary until a sufficient level of detail is reached for the identification of hazards.

#### 4.2.4 Risk Analysis

The risk acceptability of the system under analysis shall be established by following this hierarchy of CSM Risk Acceptance Principles:

1. The application of codes of practice (Section 4.2.4.1)
2. A comparison with reference systems (Section 4.2.4.2)
3. Explicit risk estimation (Section 4.2.4.3)

More than one of these risk acceptance principles may be applied in concert. The hazard assessor shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The hazard assessor shall also ensure that the selected risk acceptance principles are used consistently. The Authority is ultimately responsible for approving the risk evaluation efforts of the risk assessor and accepting the residual risk associated with the identified hazard or vulnerability.

Whenever a code of practice or a reference system is used to control the risk, the hazard identification must also include:

- (a) The verification of the relevance of the code of practices or of the reference system;
- (b) The identification of the deviations from the code of practices or from the reference system.

The application of CSM Risk Acceptance Principles shall identify possible mitigation measures which make the risk(s) of the system under assessment acceptable. Among these mitigation measures, the ones selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Compliance with these safety requirements shall be demonstrated in accordance with the Verification and Validation and Safety and Security Certification Program requirements identified in Chapter 7.

Mitigation measures shall be applied in accordance with the *Prevention through Design* principle as detailed in Section 5.1. The *Prevention through Design* principle includes the following order of precedence:

1. Avoidance
2. Elimination
3. Substitution
4. Engineering controls
5. Warnings
6. Administrative controls such as Operations & Maintenance procedures
7. Personal protective equipment and guards

Unacceptable risk will be reduced to an acceptable level before design acceptance. Undesirable risk must be reduced where reasonably practicable, and an Authority decision is required to accept the residual risk of the hazard or dispose of the system. The hazards will be reviewed by the SSPC, with recommendation made to the SSEC for decision. Acceptance of the level of risk or disposal of the system will be provided by the Authority through the SSEC. Tolerable risk can be tolerated and accepted with adequate controls, although risk-reducing mitigations must be applied where reasonably practicable. The iterative risk assessment process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.

As a criterion, risks resulting from hazards may be classified as acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgment shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

Individual hazards can be closed out by the application of one of the three principles but it is likely that, for most major projects, a combination of the three principles will be used. Any risk assessment conducted under the CSM should always be proportionate to the extent of the risk being assessed. The CSM has been introduced to ensure that levels of safety are maintained or improved when and where necessary and reasonably practicable. Applying one or more of the three risk acceptance principles correctly for all identified hazards means that the risk has been reduced to an acceptable level. No further evidence is required to show that the residual risk is acceptable.

#### **4.2.4.1 Application of Codes of Practice**

The Authority shall analyze whether one or several hazards are appropriately covered by the application of relevant codes of practice.

The codes of practice shall satisfy at least the following requirements:

- (a) Be widely acknowledged in the passenger rail industry. If this is not the case, the codes of practice will have to be justified and be acceptable to the Authority;
- (b) Be relevant for the control of the considered hazards in the system under assessment; and
- (c) Be publicly available.

If one or more hazards are controlled by codes of practice fulfilling the requirements of points (a), (b), and (c) above then the risks associated with these hazards shall be considered as acceptable. This means that:

- These risks need not be analyzed further; and
- The use of the codes of practice shall be registered in the CEHL as safety requirements for the relevant hazards.

The PHA form developed during the hazard identification phase shall be completed with the term “acceptable” in the Resolution column. It will not be necessary to identify a final risk index.

Standards and rules that are widely accepted in the passenger rail sector include:

- Federal Railroad Administration regulations found in 49 CFR, Parts 200-299
- Federal Transit Administration regulations found in
- AREMA Standards for track
- California Public Utilities Commission General Orders
- TSIs or other mandatory European standards and norms
- Standards issued by the American National Standards Institute (ANSI)

This list is not exhaustive. It is also possible to use standards or codes of practice from other sectors (for example aviation, maritime, etc) but these have to be justified and be acceptable to the ISA.

Deviations from codes of practice are possible where the hazard assessor can demonstrate that at least the same level of safety will be achieved. Mandatory standards such as FRA regulations often include a process for deviating from them. Most non-mandatory standards do not have a process for deviating from them. If one or more conditions of the code of practice are not fulfilled, the hazard assessor may have to conduct explicit risk estimation on those hazards where the code of practice is not relevant for the control of the hazards in the system under assessment. Alternatively, other codes of practice or reference systems could be used. Where an alternative approach is not fully compliant with a code of

practice, the hazard assessor shall demonstrate that the alternative approach taken leads to at least the same level of safety.

If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional mitigation measures shall be identified applying one of the two other risk acceptance principles.

When all hazards are controlled by codes of practice, the hazard management process may be limited to:

- The hazard identification and classification in accordance with section 4.2.3;
- The registration of the use of the codes of practice in the CEHL; and
- The documentation of the hazard management process in accordance with Section 4.2.7.

#### **4.2.4.2 Use of a Reference System**

The Authority, with the support of other involved actors, shall analyze whether one or more hazards are covered by a similar system that could be taken as a reference system. Reference systems can be used to derive the safety requirements for the new or changed system.

A reference system shall satisfy at least the following requirements:

- (a) It has already been proven in-use to have an acceptable safety level and would still qualify for approval by the regulatory body having jurisdiction;
- (b) It is accepted by the body having regulatory authority over its application to CHSTS (e.g. FRA, CPUC, Office of State Fire Marshal, etc)
- (c) It is used under similar functional, operational, and environmental conditions and has similar interfaces as the system under consideration for CHSTS.

For technical changes, it is unlikely that evidence of in-service history alone can prove that a high integrity system has an acceptable safety level, given the low failure rates required of such systems. Evidence that sufficient safety engineering principles have been applied in the development of the reference system will need to be confirmed for each application of it.

If a reference system fulfils the requirements listed in points (a), (b), and (c), above, then for the system under assessment the risks associated with the hazards covered by the reference system shall be considered as acceptable.

If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.

If the same safety level as the reference system cannot be demonstrated, additional mitigation measures shall be identified for the deviations, applying one of the two other risk acceptance principles.

The safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system. These safety requirements shall be registered in the CEHL as safety requirements for the relevant hazards.

The PHA form developed during the hazard identification phase shall be completed with the term "acceptable" in the Resolution column. It will not be necessary to identify a final risk index.

When hazards are accepted by use of a reference system, the hazard management process may be limited to:

- The hazard identification and classification in accordance with section 4.2.3;
- The registration of the use of the reference system in the CEHL; and
- The documentation of the hazard management process in accordance with Section 4.2.7.

#### 4.2.4.3 Explicit Risk Estimation

Explicit risk estimation is an assessment of the risks associated with hazard(s), where risk is defined as a combination of the likelihood (or frequency of occurrence) and the consequence (or severity) of a hazard. Explicit risk estimation can be used where:

- The Authority is unable to address the hazards identified in the hazard identification stage of the CSM via a code of practice or comparison with a reference system;
- Deviations are necessary from codes of practice or reference systems; or
- The Authority needs to analyze the hazards and evaluate design principles or safety measures.

The estimation can be qualitative, semi-quantitative, or quantitative. The choice will be determined by factors such as availability of, and confidence in, quantitative data and the depth of analyses should be proportionate to the potential risks. Any risk assessment should follow a systematic and structured process. Qualitative hazard assessment shall be performed by technical experts with sufficient experience and qualifications relevant to the hazard under consideration.

The acceptability of the estimated risks shall be evaluated using the risk acceptance criteria identified in Section 4.2.5. The acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.

If the estimated risk is not acceptable, additional mitigation measures shall be identified and implemented in order to reduce the residual risk to an acceptable level. The ALARP Principle (As Low as Reasonably Practicable) shall be applied to compare the cost and feasibility of applying additional mitigation measures against the benefit gained from reduced residual risk.

When hazards are accepted by use of explicit risk estimation, the hazard management process may be limited to:

- The hazard identification and classification in accordance with section 4.2.3;
- Completion of the PHA process by registering the risk index in the Residual Risk Index (Projected) column of the PHA form;
- The registration of the use of the explicit risk estimation and the mitigation measures in the CEHL; and
- The documentation of the hazard management process in accordance with Section 4.2.7.

When the risk associated with one or a combination of several hazards is considered as acceptable, the identified mitigation measures shall be registered in the CEHL.

Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:

- For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the failure rate of that system is less than or equal to  $10^{-9}$  failures per operating hour.

The explicit risk estimation and evaluation shall satisfy at least the following requirements:

- The methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes); and
- The results shall be sufficiently accurate to serve as robust decision support, i.e. minor changes in input assumptions or prerequisites shall not result in significantly different requirements.

#### 4.2.5 Risk Estimation Process and Risk Acceptance Criteria

The risk assessment process for significant hazards is as follows:

1. Identify the hazardous event(s) which have the potential to cause injury or death to passengers, employees, or members of the public who are directly or indirectly exposed to the technical, operational, or organizational change being considered.
2. Identify the precursors (i.e. the component, sub-system or system failures, physical effects, human error failures or operational conditions) which can result in the occurrence of each hazardous event.
3. Identify the control measures that are in place to control or limit the occurrence of each precursor that cannot be eliminated.
4. Estimate the frequency at which each hazardous event can occur.
5. Estimate the consequences (most reasonable credible mishap) in terms of injuries and fatalities, environmental impact, monetary loss, or reputational damage that could occur for the different outcomes that may follow the occurrence of a hazardous event.
6. Estimate the overall risk associated with the hazardous event.
7. Identify additional mitigations or control measures that, if applied, would ensure that residual risk is reduced so far as is reasonably practicable.
8. Provide clear and comprehensive documentary evidence of the methodologies, assumptions, data, judgments, and interpretations used in the development of the risk assessment and the analysis of its results. Particularly where the assessment is quantitative and where different safety measures need to be assessed, the results may also need to be accompanied by sensitivity and uncertainty analysis.

The severity category and frequency of occurrence of the potential mishap(s) for each hazard across all system modes are estimated using the definitions in Tables 4-1 and 4-2 respectively.

**Table 4-1 Hazard Severity Categories**

<b>Hazard Category</b>	<b>Definition</b>
<p style="text-align: center;"><b>1</b> <b>Catastrophic</b></p>	<p>Could result in one or more of the following:</p> <ul style="list-style-type: none"> <li>• Multiple fatalities or equivalent fatalities</li> <li>• Irreversible significant environmental impact</li> <li>• Monetary loss equal to or exceeding \$10M                             <ul style="list-style-type: none"> <li>○ Severe damage or total loss of rolling stock</li> <li>○ Severe damage to infrastructure or other severe system loss causing all or a significant portion of the system to be unavailable for normal service for more than 72 hours</li> </ul> </li> <li>• Reputational damage of national impact</li> </ul>
<p style="text-align: center;"><b>2</b> <b>Critical</b></p>	<p>Could result in one or more of the following:</p> <ul style="list-style-type: none"> <li>• A single fatality or multiple major injuries or occupational illnesses</li> <li>• Reversible significant environmental impact</li> <li>• Monetary loss equal to or exceeding \$1M but less than \$10M                             <ul style="list-style-type: none"> <li>○ Major but repairable damage to rolling stock</li> <li>○ Major damage to infrastructure or other major system loss, repairable within 72 hours to allow normal service</li> </ul> </li> <li>• Reputational damage of statewide impact</li> </ul>
<p style="text-align: center;"><b>3</b> <b>Marginal</b></p>	<p>Could result in one or more of the following:</p> <ul style="list-style-type: none"> <li>• A major injury or occupational illness, or multiple minor injuries</li> <li>• Reversible moderate environmental impact</li> <li>• Monetary loss equal to or exceeding \$100K but less than \$1M                             <ul style="list-style-type: none"> <li>○ Minor repairable damage to railcars</li> <li>○ Minor damage to infrastructure or other minor system loss, repairable within 24 hours to allow normal service</li> </ul> </li> <li>• Reputational damage of local area impact</li> </ul>
<p style="text-align: center;"><b>4</b> <b>Negligible</b></p>	<p>Could result in one or more of the following:</p> <ul style="list-style-type: none"> <li>• A minor injury or occupational illness</li> <li>• Minimal environmental impact</li> <li>• Monetary loss less than \$100K                             <ul style="list-style-type: none"> <li>○ Minimal infrastructure damage or system loss affecting normal service for less than 12 hours</li> </ul> </li> <li>• Reputational damage of limited or little impact</li> </ul>

To determine the appropriate severity category as defined in Table 4-1 for a given hazard at a given point in time, identify the potential for death or injury, environmental impact, monetary loss, or reputational damage in a most reasonable credible mishap scenario. A given hazard may have the potential to affect one or all of these areas. An equivalent fatality may be expressed as 10 major injuries (those requiring hospitalization) or 100 minor injuries (those not requiring hospitalization).

Hazard frequency is defined as the likelihood that a specific hazard will occur during the planned life-cycle of the system element, subsystem, or component, recognizing that these life-cycles will vary depending upon the item under consideration. Hazard frequency can be described subjectively in potential occurrences per unit of time (Mean Time to Hazardous Event – MTTHE), events, population, items, or activity, and shall be ranked as shown in Figure 4-2.

**Table 4-2 Hazard Frequency Categories**

Description	Level	Qualitative Definition	Qualitative Description for the System	Quantitative Context (Probability of Occurrence)
Frequent	A	Likely to occur frequently in an individual item or the System; may be continuously experienced in fleet/inventory.	MTTHE < 2 mos	$p > 10^{-1}$
Probable	B	Likely to occur several times in the life of an individual item or the System; will occur frequently in fleet/inventory.	2 mos < MTTHE < 1 yr	$10^{-1} > p > 10^{-2}$
Occasional	C	Likely to occur sometime in the life of an individual item or the System; will occur several times in fleet/inventory.	1 yr < MTTHE < 10 yrs	$10^{-2} > p > 10^{-3}$
Remote	D	Unlikely but possible to occur in the life of an individual item or the System; unlikely but can be expected to occur in fleet/inventory.	10 yrs < MTTHE < 100 yrs	$10^{-3} > p > 10^{-6}$
Highly Unlikely	E	So unlikely that it can be assumed occurrence may not be experienced in the life of an individual item or the System; unlikely but possible to occur in fleet/inventory.	MTTHE > 100 yrs	$10^{-6} > p$
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.	n/a	$p = 0$

Note - Frequency level F is used to document cases where the hazard is no longer present. No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap frequency to level F.

The frequency of the hazard can be determined qualitatively based on the relative frequency of expected occurrence, or quantitatively (using failure rates or accident/incident statistical data). Quantitative determination is generally preferable, but in the absence of applicable quantitative data the use of qualitative estimation is necessary and appropriate. Table 4-2 identifies both a qualitative definition and a qualitative description of the system using MTTHE, based upon a railway operation 20 hours per day, 7 days per week.

Hazard severity categories (1 through 4) and hazard frequency categories (A through E) are combined in the Risk Assessment Matrix (Table 4-3) to produce a risk index for each identified hazard. The Risk Acceptance Matrix (Table 4-4) identifies required actions to reduce risk based on the risk rating. The Authority will accept the residual risk through the Safety and Security Executive Committee process where appropriate through direct approval of individual risk acceptance decisions for hazard risks categorized as *Undesirable*. Hazard risks categorized as *Acceptable* do not require direct SSEC approval, however review of the risk assessment process will fulfill the Authority’s responsibility to accept the residual risk.

**Table 4-3 Risk Assessment Matrix**

Frequency \ Severity	1 Catastrophic	2 Critical	3 Marginal	4 Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Highly unlikely	1E	2E	3E	4E
(F) Eliminated				

**Table 4-4 Risk Acceptance Matrix**

Hazard Risk Index	Risk Rating	Action Required
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable	Risk must be reduced and managed
1D, 2C, 3B, 4A	Undesirable	Risk is acceptable only where further risk reduction is impracticable. Authority decision required to accept residual risk
1E, 2D, 2E, 3C, 3D, 4B, 4C	Tolerable	Apply mitigations where reasonably practicable. Risk can be tolerated and accepted with adequate controls. Authority review required to accept residual risk.
3E, 4D, 4E	Acceptable	No further risk reduction required
	Eliminated	None

#### 4.2.6 As Low as Reasonably Practicable (ALARP Principle)

The ALARP Principle shall be applied where necessary to assess the cost/benefit of applying additional measures of mitigation in order to achieve residual risk that is as low as reasonably practicable. ALARP calculations can be qualitative, semi-quantitative, or quantitative depending on the level of risk and the amount of data available to the assessor. Qualitative analysis is entirely appropriate for assessment of risks that are found in standard industry practice or common experiences. Hazards deemed appropriate for more quantitative analysis will require development of more comprehensive analysis to provide the required level of data. Criteria for applying a detailed, quantitative cost/benefit analysis includes high risks that must be mitigated and accepted, highly-controversial risks, risks with a potentially high impact to the System or project under consideration.

The ALARP principle arises from the fact that infinite time, effort and money could be spent on the attempt of reducing a risk to zero, but that this is usually not practical. It should not be understood as simply a quantitative measure of benefit against detriment; it is more a best common practice of judgment of the balance of risk and societal benefit. ALARP does not represent zero risk.

For a risk to be ALARP it must be possible to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained; that is the greater the risk, the more resources that should be spent in reducing it, and the greater the bias on the side of safety. The costs could outweigh the benefits and the measure could still be reasonably practicable to introduce.

The disproportion factors (DF) in Table 4-5 shall be applied to the ALARP process according to the amount of risk. DFs that may be considered gross vary from upwards of 1 depending on a number of factors including the magnitude of the consequences and the frequency of realizing those consequences, i.e. the greater the risk, the greater the DF.

**Table 4-5**

<u>Risk Rating</u>	<u>DF</u>
Unacceptable	10
Undesirable	8
Tolerable	5
Acceptable	1

When using a cost/benefit analysis, convert both the additional mitigation(s) and the risk (so far as it is being reduced) to a common set of units – dollars – for the purpose of making a comparison. A hazard is considered ALARP using a cost/benefit analysis when cost divided by the benefit is greater than the DF.

Other issues to consider when performing a cost/benefit analysis include the sensitivity of key inputs (frequency/severity of the hazardous event), animalization (average costs and average benefits), and discounting the value of future benefits.

#### 4.2.7 Hazard Analysis Processes and Documentation, Verification and Validation

A variety of hazard analysis processes are available for proper risk estimation and mitigation development, based upon the characteristics of the system or subsystem under consideration. The types of analyses which may be required for the development of the CHSTS are described below.

- Preliminary Hazard Analysis (PHA) is typically the initial hazard analysis technique used during the system or subsystem design phase. PHA is used to identify safety critical areas within the system and roughly evaluate hazards. PHA establishes the basis for the safety criteria in design, equipment, and performance specifications.
- Site-Specific Hazard Analysis (SiSHA) is an expansion of the PHA, conducted as the general design criteria and system requirements are applied to specific system and subsystem elements. An

example would be a SiSHA for an elevated structure spanning the SR-99 highway in Fresno, applying the safety-critical criteria found in the Design Criteria to the specific characteristics and site conditions of this structure. SiSHA is generally performed during the Final Design, Construction, and Testing/Startup Phases. The primary output of the SiSHA is the identification and evaluation of hazards and mitigations that are specific to the system element under consideration.

- Failure Modes and Effects Analysis (FMEA) is an inductive analysis used to identify equipment failures. It evaluates a system or subsystem to identify possible failures of each individual component in the system. The results or effects of the subsystem and component failures are then classified according to severity.
- Fault Tree Analysis (FTAn) is representative of the deductive process. The purpose of the Fault Tree Analysis is to provide a concise and orderly description of the various combinations of possible occurrences within the system that can result in an undesired event. This is the most rigorous of the hazard identification process and analyses and is typically performed for the most complex systems.
- Interface Hazard Analysis (IHA) is performed to identify design hazards in components and subsystems of a major system. IHA determines the functional relationships between the systems, subsystems, processes, components and equipment based solely on safety considerations and also identifies all elements in which a functional failure could result in a hazardous condition or accidental loss.
- Operating Hazard Analysis (OHA) is performed to determine all applicable operational safety requirements for personnel, procedures, and equipment throughout all phases of the system life cycle. Engineering data, procedures, and instructions developed from other safety analyses, the engineering design, and initial test programs are used to support this analysis.
- Software Hazard Analysis (SHA) will be used to evaluate software design, and related software and hardware documentation will be reviewed for safety-critical software-controlled functions. The analysis will review software and hardware failures that could cause the system to operate in a hazardous manner.
- Adjacent Railroad Hazard Risk Assessment Model (ARHRAM) will be used to assess the hazards associated with freight railroad right-of-ways directly adjacent to the CHSTS trackway. This is a semi-quantitative assessment process that relies on input from technical experts to assess site-specific characteristics of the adjacent railway.

The detailed process for completing each of these analysis types, including the appropriate forms, is identified in SSMP Appendix I. Appropriate support documentation used in the development of risk assessment will be identified or referenced in detail as part of each analysis process, including, but not limited to, the following:

- a) System description including modes of operation and tasks
- b) Schematics, drawing, block diagrams, lists of assemblies, parts and components addressed within each subsystem and system
- c) Documented reliability and safety data including failure rate data obtained from service use in identical or manifestly similar equipment in similar environment
- d) Documented reliability and safety data obtained from formal test results, conducted in similar applications
- e) Documented reliability and safety data obtained from formal analyses, conducted for equipment in similar applications

Hazard management requires monitoring and documentation throughout the project life cycle. Verification and validation activities shall fulfill the requirements of the Safety and Security Certification Program, as described in Chapter 7.