



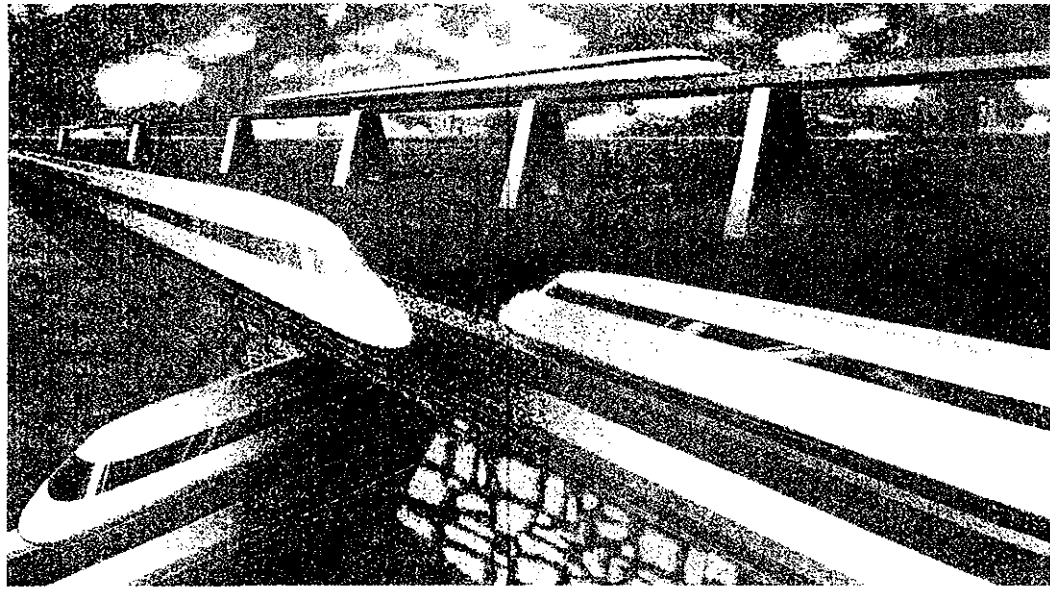
U S Department  
of Transportation  
**Federal Railroad  
Administration**

# Safety of High Speed Ground Transportation Systems

Office of Research  
and Development  
Washington, D.C. 20590

## Analytical Methodology for Safety Validation of Computer Controlled Subsystems

### Volume II: Development of a Safety Validation Methodology



DOT/FRA/ORD-95/10.2  
DOT-VNTSC-FRA-95-8.II

Final Report  
September 1995

This document is available to the  
public through the National Technical  
Information Service, Springfield, VA 22161

12-Safety

# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 1995		3. REPORT TYPE AND DATES COVERED Final - April 1994	
4. TITLE AND SUBTITLE Safety of High Speed Ground Transportation Systems: Analytical Methodology for Safety Validation of Computer Controlled Subsystems Volume II: Development of a Safety Validation Methodologies				5. FUNDING NUMBERS RR593/R5019	
6. AUTHOR(S) Jonathan F. Luedeke*					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Battelle 505 King Avenue Columbus, OH 43201-2693				8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-FRA-95-8.II	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Transportation Federal Railroad Administration Office of Research and Development Washington, DC 20590				10. SPONSORING/MONITORING AGENCY REPORT NUMBER DOT/FRA/ORD-95/10.2	
11. SUPPLEMENTARY NOTES *under contract to:		U.S. Department of Transportation Research and Special Programs Administration Volpe National Transportation Systems Center Kerdall Square, Cambridge, MA 02142			
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public through the National Technical Information Service, Springfield, VA 22161				12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words)  This report describes the development of a methodology designed to assure that a sufficiently high level of safety is achieved and maintained in computer-based systems which perform safety critical functions in high-speed rail or magnetic levitation transportation systems. This report consists of two volumes. The first presents a glossary of relevant computer technology terminology to assure consistency of use and understanding. A state-of-the-art review of safety verification and validation processes worldwide is presented. Following the review, these processes are assessed relative to their degree of assured safety as well as their potential applicability to safety critical systems in US rail transportation systems.  This, the second volume, builds upon the information developed in the first volume and describes a methodology which has been developed specifically for application to computer-controlled systems used in railroad applications in the United States.					
14. SUBJECT TERMS verification, validation, software, hardware, methodology, safety, safety standards, high-speed rail, magnetic levitation, high-speed guided ground transportation system				15. NUMBER OF PAGES 154	
				16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT		

## **PREFACE**

The Federal Railroad Administration (FRA) is responsible for assuring the safety of high-speed rail and magnetic levitation systems deployed in this country. A primary concern of FRA is the proper use of computer technology in the implementation of safety critical functions, such as signalling and train control, in newer high-speed systems as well as in conventional rail systems. This report describes the development of a methodology designed to assure that a sufficiently high level of safety is achieved and maintained in these computer-based systems. Adequate safety is necessary whether the systems are used in new applications or are used to replace or enhance existing equipment. This report comprises the second of two volumes relative to the development of this methodology.

The first report included a glossary of terms which was developed to ensure consistency and understanding. A description of the state-of-the-art in safety verification and validation methodologies worldwide was presented, as well as an assessment of these methodologies from the standpoint of their applicability and level of assured safety.

The second volume builds upon the information developed in the first volume and describes a methodology which has been developed specifically for application to computer-controlled systems used in railroad applications in the United States.

This report was prepared in support of the United States Department of Transportation, FRA, Office of Research and Development.

# METRIC/ENGLISH CONVERSION FACTORS

## ENGLISH TO METRIC

### LENGTH (APPROXIMATE)

1 inch (in) = **2.5** centimeters (cm)  
 1 foot (R) = **30** centimeters (cm)  
 1 yard (yd) = **0.9** meter (m)  
 1 mile (mi) = **1.6** kilometers (km)

## METRIC TO ENGLISH

### LENGTH (APPROXIMATE)

1 millimeter (mm) = **0.04** inch (in)  
 1 centimeter (cm) = **0.4** inch (in)  
 1 meter (m) = **3.3** feet (R)  
 1 meter (m) = **1.1** yards (yd)  
 1 kilometer (k) = **0.6** mile (mi)

### AREA (APPROXIMATE)

1 square inch (sq in, in<sup>2</sup>) = **6.5** square centimeters (cm<sup>2</sup>)  
 1 square foot (sq ft, ft<sup>2</sup>) = **0.09** square meter (m<sup>2</sup>)  
 1 square yard (sq yd, yd<sup>2</sup>) = **0.8** square meter (m<sup>2</sup>)  
 1 square mile (sq mi, mi<sup>2</sup>) = **2.6** square kilometers (km<sup>2</sup>)  
 1 acre = **0.4** hectare (he) = **4.000** square meters (m<sup>2</sup>)

### AREA (APPROXIMATE)

1 square centimeter (cm<sup>2</sup>) = **0.16** square inch (sq in, in<sup>2</sup>)  
 1 square meter (m<sup>2</sup>) = **1.2** square yards (sq yd, yd<sup>2</sup>)  
 1 square kilometer (km<sup>2</sup>) = **0.4** square mile (sq mi, mi<sup>2</sup>)  
 10,000 square meters (m<sup>2</sup>) = 1 hectare (he) = **2.5** acres

### MASS - WEIGHT (APPROXIMATE)

1 ounce (oz) = **28** grams (gm)  
 1 pound (lb) = **0.45** kilogram (kg)  
 1 short ton = **2.000** pounds (lb) = **0.9** tonne (t)

### MASS - WEIGHT (APPROXIMATE)

1 gram (gm) = **0.036** ounce (oz)  
 1 kilogram (kg) = **2.2** pounds (lb)  
 1 tonne (t) = **1,000** kilograms (kg) = **1.1** short tons

### VOLUME (APPROXIMATE)

1 teaspoon (tsp) = **5** milliliters (ml)  
 1 tablespoon (tbsp) = **15** milliliter; (ml)  
 1 fluid ounce (fl oz) = **30** milliliters (ml)  
 1 cup (c) = **0.24** liter (l)  
 1 pint (pt) = **0.47** liter (l)  
 1 quart (qt) = **0.96** liter (l)  
 1 gallon (gal) = **3.8** liters (l)  
 1 cubic foot (cu ft, ft<sup>3</sup>) = **0.03** cubic meter (m<sup>3</sup>)  
 1 cubic yard (cu yd, yd<sup>3</sup>) = **0.76** cubic meter (m<sup>3</sup>)

### VOLUME (APPROXIMATE)

1 milliliter (ml) = **0.03** fluid ounce (fl oz)  
 1 liter (l) = **2.1** pints (pt)  
 1 liter (l) = **1.06** quarts (qt)  
 1 liter (l) = **0.26** gallon (gal)  
 1 cubic meter (m<sup>3</sup>) = **36** cubic feet (cu ft, ft<sup>3</sup>)  
 1 cubic meter (m<sup>3</sup>) = **1.3** cubic yards (cu yd, yd<sup>3</sup>)

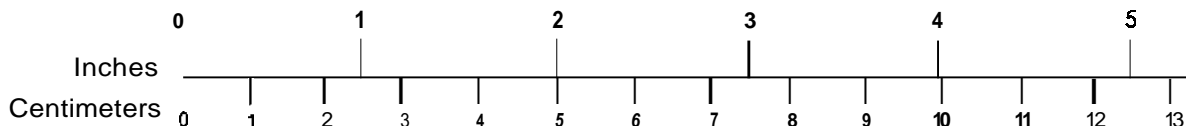
### TEMPERATURE (EXACT)

$$[(x-32)(5/9)]^{\circ}\text{F} = y^{\circ}\text{C}$$

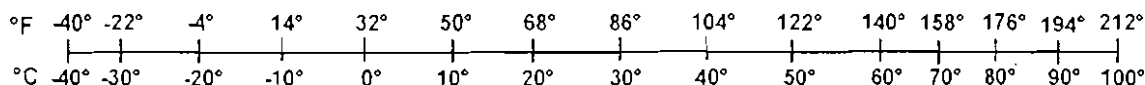
### TEMPERATURE (EXACT)

$$[(9/5)y + 32]^{\circ}\text{C} = x^{\circ}\text{F}$$

## QUICK INCH - CENTIMETER LENGTH CONVERSION



## QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSION



For more exact and or other conversion factors, see NBS Miscellaneous Publication 286. Units of Weights and Measures.  
 Price \$2.50 SD Catalog No. C13 10286

Updated 1/23/95

# TABLE OF CONTENTS

## Section

1. INTRODUCTION .....	1-1
1.1 Background .....	1-1
1.2 Objectives .....	1-2
2. APPROACH .....	2-1
2.1 Option Task Approach .....	2-1
2.1.1 Item 1 Approach - Safety Validation Methodology .....	2-1
2.1.2 Item 3 Approach - Training Program Plan .....	2-2
2.1.3 Item 4 Approach - Technical and Economic Feasibility .....	2-2
2.1.4 Item 5 Approach - Human Factors Aspects .....	2-3
3. BASE TASK OVERVIEW .....	3-1
3.1 Base Task Activities .....	3-1
3.1.1 Glossary of Terms .....	3-1
3.1.2 State-of-the-Art In Safety Verification/Validation Methodologies ..	3-1
3.1.3 Assessment of Safety Verification/Validation Methodologies ....	3-2
3.2 Safety Verification/Validation Assessment Summary .....	3-3
3.2.1 General Observations .....	3-3
3.2.2 Diversity .....	3-4
3.2.3 Single "Best" Existing Methodology .....	3-6
3.2.4 Trends .....	3-7
4. SAFETY VALIDATION METHODOLOGY DEVELOPMENT .....	4-1
4.1 Discussion of Issues .....	4-1
4.1.1 Safety Validation Methodology-What is it? .....	4-1
4.1.2 Role of Safety V&V in Overall Safety Assurance .....	4-2
4.1.3 FRA's Role and Intent of Methodology .....	4-3
4.1.4 Nature of the Methodology .....	4-4
4.1.5 Applicability of the Methodology .....	4-4
4.1.6 Safety Requirements .....	4-5
4.1.7 Safety V&V Vs. Hazard Analysis/Risk Assessment .....	4-7
4.1.8 Safety Integrity Levels .....	4-8
4.1.9 Hardware/Software Modifications .....	4-9
4.1.10 Independent Safety Assessment .....	4-9

## TABLE OF CONTENTS (cont.)

### Section

4.2 Overall Safety Assurance Methodology . . . . .	4-9
4.2.1 Quality Management . . . . .	4-10
4.2.2 Safety Management . . . . .	4-12
5. RECOMMENDED SAFETY VERIFICATION AND VALIDATION METHODOLOGY . . . . .	5-1
5.1 Introductory Comments . . . . .	5-1
5.2 General Safety Requirements . . . . .	5-2
5.3 Safety V&V Methodology . . . . .	5-4
5.3.1 Safety V&V Planning . . . . .	5-4
5.3.2 Software Safety V&V Activities . . . . .	5-6
5.3.3 Hardware Safety V&V Activities . . . . .	5-11
5.3.4 System Safety V&V Activities . . . . .	5-15
5.3.5 Safety V&V of Modifications . . . . .	5-19
5.4 Compliance Ensurance Process . . . . .	5-20
5.4.1 General Compliance Ensurance Process . . . . .	5-20
6. TECHNICAL AND ECONOMIC FEASIBILITY . . . . .	6-1
6.1 Overview of Safety Verification/Validation Methodologies . . . . .	6-1
6.1.1 Recommended Methodology . . . . .	6-2
6.1.2 Present U.S. Practice . . . . .	6-4
6.1.3 Present Foreign Practice . . . . .	6-7
6.2 Methodology Comparison . . . . .	6-10
6.2.1 Comparison with U.S. Practice . . . . .	6-11
6.2.2 Comparison with Foreign Practice . . . . .	6-12
6.3 Feasibility Review . . . . .	6-14
6.3.1 Technical Considerations . . . . .	6-15
6.3.2 Economic Considerations . . . . .	6-15
6.3.3 Technology Advancement Considerations . . . . .	6-17
6.4 Conclusions . . . . .	6-18

## TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
7. TRAINING PROGRAM PLAN .....	7-1
7.1 Introduction .....	7-1
7.2 Training Course Approach and Content .....	7-1
7.3 Presentation Techniques .....	7-1
7.3.1 Lectures .....	7-5
7.3.2 Discussion Sessions .....	7-6
7.3.3 Video Tapes .....	7-6
7.3.4 Demonstration of the Methodology .....	7-6
7.3.5 Practice of the Audit Process .....	7-6
7.4 Instructor Qualifications .....	7-6
7.5 Training Materials .....	7-7
7.5.1 Instructor Guide .....	7-7
7.5.2 Overheads/Slides .....	7-7
7.5.3 Student Workbook .....	7-7
7.5.4 Training Course Topic Outline and Time Schedule .....	7-8
7.5.5 Audit/Inspection Aid .....	7-8
7.5.6 Course Evaluation Form .....	7-8
7.5.7 Audit Exercise Materials .....	7-8
7.6 Examinations .....	7-9
7.6.1 Quizzes .....	7-9
7.6.2 Final Exam .....	7-9
7.6.3 Certificate of Achievement .....	7-9
7.7 Course Evaluation .....	7-9
7.8 Long-Term Training Needs and Requirements .....	7-10
8. HUMAN FACTORS ASPECTS .....	8-1
8.1 Introduction .....	8-1
8.1.1 Background .....	8-1
8.1.2 Purpose .....	8-2
8.2 Method .....	8-2
8.2.1 Operator Physiologically Related Elements Method .....	8-2
8.2.2 Automation Related Elements Method .....	8-3

## TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
8.3 Results .....	8-4
8.3.1 Physiological and Associated Aspects Related to Operator Performance .....	8-4
8.3.2 Implications of HSGT Speed .....	8-6
8.3.3 Implications of Increased Automation .....	8-9
8.4 Implications for HSGT Development .....	8-16
8.4.1 HSGT Development in the U.S. ....	8-16
8.4.2 HSGT Display and Control Guidelines .....	8-17
8.5 Summary of Findings and Conclusions .....	8-18
8.5.1 Summary of Human Factors Aspects Study Findings .....	8-18
8.5.2 Conclusions .....	8-22
Appendix A. Reference Sources .....	A-1
Appendix B. Information Sources .....	B-1
Appendix C. Individual Contacts .....	C-1
Appendix D. Responses from Industry Survey .....	D-1

## LIST OF FIGURES

Figure 5.1 Safety V&V Methodology Activities .....	5-5
--	-----

## LIST OF TABLES

Table 7.1 Training Course Topic Outline .....	7-2
---	-----



# 1. INTRODUCTION

The Federal Railroad Administration (FRA) is currently responsible for assuring the safety of conventional rail, high-speed rail and maglev systems deployed in this country. One of the FRA's primary concerns is the proper use of computer technology in the implementations of safety critical functions in newer high-speed systems as well as in conventional rail systems. Existing Federal Regulations governing signalling and train control systems may need to be revised to adequately address the various issues associated with the utilization of this new technology.

The Volpe National Transportation Systems Center (Volpe Center) is assisting the FRA in identifying and addressing many of the pertinent safety issues. The primary interest in this overall program, conducted for the Volpe Center in support of the FRA, is the development of a safety validation methodology to assure that a sufficiently high level of safety is achieved and maintained in these computer-based systems. Adequate safety is necessary whether the systems are used in new applications or are used to replace or enhance existing signalling/train control equipment.

This overall program to develop the methodology was separated into two major tasks (i.e., Base Task and Option Task) which were conducted sequentially. Work in the Base Task involved three activities: 1) the development of a glossary of relevant terminology and acronyms, 2) an investigation of the state-of-the-art in safety verification/validation methodologies and associated standards in computer-based systems worldwide, and 3) an assessment of the methodologies/standards from the standpoint of their applicability and level of assured safety. All results were documented in the report entitled "State-of-the-Art and Assessment of Safety Verification/Validation Methodologies," dated February 11, 1994.

This present document is the Final Report for the Option Task of the program relative to the development of this methodology. The report describes work performed and results obtained on four major activities or items of work. The first involved the development of the safety validation methodology being recommended to the FRA. The second involved the development of a training program plan that could form the basis for the education of appropriate FRA personnel on the nature and content of the methodology. The third involved the conduct of a technical/economic feasibility study of the recommended methodology, and the last activity involved an investigation into various human factor aspects associated with the man-machine interface in high-speed ground transportation systems.

## 1.1 BACKGROUND

The evolution in the implementations of safety critical systems in the railroad industry from simple vital relays to more complex computer-based configurations has raised many issues among users as well as the FRA. Foremost among these issues is the need to assure similar or improved levels of safety to those currently provided by conventional fail-safe technology. This concern is heightened in newer high-speed rail and maglev systems which operate or are

being designed to operate at considerably higher speeds and levels of automation than conventional rail systems. Computers are playing an increasing role in the safety critical functions in these newer systems such as in train location determination, switch/route control (interlocking), control of braking/propulsion to ensure safe speed and headway, and communications among the trains, wayside and central elements.

The use of computers has not only brought about an increase in the complexity of hardware and interest in its safe operation, but has also brought to the forefront the issue of safe execution of software and its safe interaction with the host hardware. A wide variety of design techniques are being used by manufacturers worldwide (in transportation as well as other industries) to help ensure a high level of safety in their systems and to provide a high level of fault tolerance and system availability. Those include the use of redundancy, diversity in hardware and/or software as well as extensive diagnostics and other special design techniques. Further, manufacturers are using different verification/validation practices (e.g., failure modes and effects analyses, hazard analyses, fault trees, testing) and are applying them at varying degrees and at different times throughout the system life cycle to help ensure safe operation of their systems. To date, there have been no widely accepted or mandated (by regulations) development or verification/validation practices for the railroad industry (including high-speed rail and maglev) in this country to address the safety concerns of computer-based systems.

## **1.2 OBJECTIVES**

The overall objective of this program was to develop a safety validation methodology that could be considered (by the FRA) for use as a standard for manufacturers and users to help ensure the safe operation of safety critical computer-based systems. Specific objectives of the two major tasks of this program were as follows:

Base Task - To identify, describe and assess existing safety verification/validation methodologies used by selected government and industry organizations worldwide, and to identify the "best" existing methodology for railroad (including high-speed rail and maglev) applications

Option Task - The primary objective was to utilize results of the Base Task in the development of an industry-approved methodology for ensuring the safe operation of safety critical computer-based systems from installation throughout post-installation modifications. This was to consist of two major aspects: 1) establishing standards that must be followed by manufacturers and/or end-users, and 2) establishing a means by which the FRA could ensure compliance with that standard. A secondary objective was to identify and assess human factor issues associated with computer automation and high-speed vehicle operation.

## 2. APPROACH

As indicated, this program was separated into two major tasks (i.e., Base Task and Option Task). An overview of the work performed and results obtained in the Base Task is provided in the next section (i.e., Section 3). The various activities that comprised the Option Task (to which this report is directed) including the general approaches used in those activities are described below.

### 2.1 OPTION TASK APPROACH

Work performed in the Option Task was separated into the following five items of work:

- Item 1 - Safety Validation Methodology--development of a safety validation methodology (based upon the results of the Base Task) and associated compliance ensurance process for FRA's consideration.

Item 2 - Solicitation from Industry (i.e., railroads, suppliers and other interested parties). Note: This item was eliminated as it was judged to be premature at this time. Further discussion on this is provided in Section 4.1.4 of this report.

Item 3 - Training--development of a training program plan (but not the training itself) for appropriate FRA personnel on ensuring compliance with the methodology.

Item 4 - Techno-Economic Feasibility Study--investigation into the technical and economic feasibility of the recommended methodology.

Item 5 - Human Factors Aspects Issues--investigation into human factors aspects issues relative to computer automation and operator interfaces in high-speed rail/maglev applications.

Results of all work conducted in the Option Task have been assimilated into this final report. The nature of the work performed on each of the Option Task activities is described below.

#### 2.1.1 Item 1 Approach - Safety Validation Methodology

The primary emphasis in Item 1 concerned the development of a safety validation methodology to help ensure the safety of computer-based system/equipment used in safety critical applications. The intent here was to draw from the findings of the Base Task, and in particular, the attributes of existing/draft safety verification and validation methodologies and associated standards worldwide. As will be discussed later, the methodology presented in this report is referred to as a safety verification and validation (safety V&V) methodology since it

incorporates both verification and validation aspects. The methodology describes a process, associated activities, and general documentation requirements for demonstrating the safety of computer-based systems/equipment.

There were several important aspects to developing and presenting the recommended methodology. First, it was necessary to determine and investigate various issues associated with the nature, applicability and utilization of the methodology. Section 4 of this report presents and discusses these various issues, many of which will require further consideration before a final methodology can be developed. Second, it was necessary to determine and describe the relationship of the safety V&V methodology within the context of overall safety assurance. Lastly, it was necessary to determine and describe an appropriate safety V&V process including all activities to be associated with the process. This was conducted by reviewing results of the methodology assessment that was performed in the Base Task as well as the existing methodologies/standards themselves.

Other emphasis in this item of work was directed to the development of a process for ensuring compliance with the safety V & V methodology. The process was structured such that it could be applied by the FRA (if desired) or a third party organization.

### **2.1.2 Item 3 Approach - Training Program Plan**

The development of the Training Program Plan was based on the training industry's accepted Instructional System Design approach. The recommended safety verification and validation methodology was examined to determine the knowledge required to understand all aspects of the methodology and how it is to be implemented. In addition, the suggested approach to auditing the implementation of the methodology was examined to determine its knowledge requirements. Knowledge requirements were then examined to determine what the trainee should know or be able to do at the end of the course. The knowledge requirements were then sequenced to provide a topic outline of the training course itself. Sequencing of the topics was based on teaching simple material before the complex, and teaching certain key topics before others.

To assist in the course design, discussions were held with the FRA to determine general trainee characteristics such as educational background, experience with computers and software, experience with FRA training, etc. Using this information, additional course contents were determined, and the training program plan was prepared. The plan includes the training course contents, presentation techniques, instructor qualifications, instructor and student training materials, student examination requirements, and an approach to course evaluation. Long term training needs were also identified in the plan.

### **2.1.3 Item 4 Approach - Technical and Economic Feasibility**

Item 4 involved a review of the recommended safety verification and validation methodology from the point of view of techno-economic feasibility. Three primary feasibility issues were considered:

Will compliance with the proposed standards require excessive expense of technical effort on the part of both the manufacturer and the end-user?

Will compliance with the proposed standards pose undue financial burden on the pan of both the manufacturer and end-user?

Will the requirements imposed by the standards serve to impede rather than promote the advance of new technology?

The feasibility review was carried out in three basic steps. First, several summary overviews of safety verification and validation methodologies were developed to provide a database. These covered the proposed methodology, present U.S. practice (a composite based on practices by three U.S. railway equipment suppliers, plus the methodology proposed for use by the AAR/RAC ATCS program), and present foreign practice (a composite based on practices by three Western European organizations, and the methodology being developed by EC/CENELEC as a European standard). Next, comparisons were made between the recommended methodology and each of the others previously summarized. This was done to highlight similarities and differences, so as to provide a basis for assessing the potential impact of employing this new methodology. Finally, the primary feasibility issues were addressed in terms of associated considerations. Conclusions, based on the preceding materials, were then developed.

#### **2.1.4 Item 5 Approach - Human Factors Aspects**

Item 5 involved the analysis of human factors aspects of computer-controlled subsystems use in high-speed ground transportation (HSGT) systems. HSGT operator physiologically-related and automation-related elements were separately addressed using a common review-and-analysis strategy designed to comprehensively identify elements and their implications. Based upon preliminary results, automation-related elements were organized into two areas related to different speeds and levels of automation. For each area, review efforts involved a three-step approach: 1) pertinent literature was identified that contained related reviews or incident analyses concerned with area elements, 2) "informal" discussions were held with cognizant individuals aimed at identification of related issues in the HSGT context, and 3) literature and informal review elements were put into a common set of salient elements.

Common elements in each of the reviewed areas were separately analyzed for implications and the results were summarized in three sections. Developed in turn were results pertaining to: 1) physiological and other elements related to operator performance, 2) different speeds, and 3) different levels of automation. These results are followed by considerations of some overall implications for HSGT design, and a summary of findings and conclusions regarding human factors aspects.

### **3. BASE TASK OVERVIEW**

This section provides an overview of the work performed and results obtained in the first task of this program (i.e., Base Task). This is considered appropriate here since the results of the Base Task effort formed the basis for the recommended methodology presented later in this report. Following brief descriptions of the three major activities performed in the Base Task, there is an overall summary of the assessment which was performed on all safety verification/validation methodologies and associated standards.

#### **3.1 BASE TASK ACTIVITIES**

##### **3.1.1 Glossary of Terms**

The first activity in the Base Task involved the development of a glossary of terms pertaining to the safety verification and validation of computer-controlled subsystems used in railroad and fixed guideway applications. Work was initiated by establishing a list of relevant and appropriate terms and acronyms pertaining to several topic areas. Areas of interest included safety, computer systems, software and software engineering, verification and validation, signalling and train control, and implementations of systems/equipment to which the methodology would be applied.

Over 25 documents containing definitions of terms in the above areas were identified and obtained. This included documents from the Institute of Electrical and Electronics Engineers (IEEE), the National Computer Systems Laboratory (NCSL), the Association of American Railroads (AAR), the American Public Transit Association (APTA), the Department of Defense (DOD), the Volpe Center and others.

Definitions considered to be the most relevant for this program were extracted from the literature. Although multiple definitions were found for numerous terms, every attempt was made to select the most clear, concise and appropriate definitions given the nature of this program and the fact that the glossary may be used by a variety of personnel with different skills and backgrounds. The glossary itself was provided as part of the final report for the Base Task.

##### **3.1.2 State-of-the-Art In Safety Verification/Validation Methodologies**

The second activity of the Base Task involved the identification and description of safety verification and validation (V&V) methodologies being utilized by various railway, regulatory bodies and other organizations worldwide to assess the safety of computer-based systems/equipment. This work included the identification and description of various safety related standards/guidelines which were required either in part or in full by the methodologies themselves.

A list of 22 organizations to be addressed in the program was established and jointly agreed upon by the Volpe Center and Battelle at the project's initiation. Included were railway suppliers and authorities, regulatory bodies and other organizations from North America, Europe and Japan. As the study progressed and further information was obtained, (six) additional organizations were added to this list due to their unique safety V&V processes/standards.

In order to obtain information on the various safety V&V methodologies/standards used, appropriate personnel involved with each organization were identified and contacted, after which follow-up letters were sent to outline the information of interest. It was quickly observed that, in most instances, a single document which described the safety V&V process used by a specific firm did not exist. Rather, the process typically involved multiple internal documents (some of which were proprietary) and/or existing/draft safety standards and other nonmandatory guidelines. Thus, it was usually necessary to obtain multiple documents for each organization from (usually) several different sources both within and external to the organization.

Following numerous discussions and a review of all literature received, summary descriptions were prepared of the safety V&V methodologies/standards used or developed by the different organizations. The intent in each of these descriptions was to summarize the following: 1) the role of the organization in setting standards, conducting safety V&V and/or obtaining approval/certification of systems/equipment, 2) the identification of existing standard/methodology documentation utilized or developed, and 3) the nature/content of the safety V&V process itself--what activities are performed, why they are performed, when in the product development or actual usage they are applied, and who performs them.

### **3.1.3 Assessment of Safety Verification/Validation Methodologies**

The final activity in the Base Task involved an assessment of the safety verification and validation (V&V) methodologies and associated standards addressed by the previous activity. The assessment was conducted in two parts from two major standpoints: 1) applicability to railroad and other fixed guideway equipment, and 2) level of assured safety. First, an initial assessment was performed in order to select a lesser number of the most promising methodologies for further and more detailed review. Criteria used in this initial assessment were directed to some general aspects as well as the potential applicability of the methodologies. Second, a more detailed assessment was conducted in which the selected methodologies were subjected to other criteria which were heavily directed to the level of assured safety if the methodologies were to be applied. Attributes and limitations of each methodology were identified, and all results (including overviews of all methodologies/standards assessed) were documented in the comprehensive final report for the Base Task.

## 3.2 SAFETY VERIFICATION/VALIDATION ASSESSMENT SUMMARY

This section provides a summary of the methodology assessment conducted in the Base Task. Following some general observations, a discussion on the diversity of the methodologies assessed, and some comments on the identification of a single "best" methodology, a number of trends are identified which represent the general direction being taken by safety verification and validation methodologies worldwide.

### 3.2.1 General Observations

A total of almost 60 major standards or guideline documents which contained safety related verification/validation methodologies utilized and/or developed by a wide variety of industries worldwide were subjected to an initial assessment. Approximately one-half of these were then subjected to the detailed assessment from the standpoint of applicability and level of assured safety.

It was found that the North American railway suppliers have and utilize (almost exclusively) their own internal standards and processes relative to safety verifications and validations. On the other hand, most European railway suppliers and authorities typically use one or more national standards plus their own internal standards/guidelines, many of which have been created to implement the intent of the national standards. There are certainly exceptions. In Sweden, for example, there are no national or other relevant standards in this area. In Germany, one of the primary standards for the German Federal Railway (DB) is the document Mü 8004, which was developed by the DB. Although British Rail tends to generally follow the RIA Tech Spec No. 23, they have their own internal standards for verification and validation.

Interest is certainly great worldwide by all industries in this topic area as reflected by the numerous documents that exist or are in various stages of development. Some examples of draft standards that address safety verification/validations are as follows:

CENELEC CLC/TC9X/SC9XA/WGA1 - "Railway Applications: Software for Railway Control and Protection Systems"

CENELEC CLC/TC9X/SC9XA/WGA2 - "Railway Applications: Safety Related Electronic Control and Protection Systems"

IEC 65A (Sec) 122 - "Software for Computers in the Application of Industrial Safety Related Systems"

IEC 65A (Sec) 123 - "Generic Aspects: Functional Safety of Electrical/Electronic/Programmable Safety Related Systems: Part 1, General Requirements"

IEEE P1228 - "Standard for Software Safety Plans"



ANSYANS 7-4.3.2 - "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

SAE ARP 4761 - "Safety Assessment Guidelines for Civil Airborne Systems and Equipment"

NASA - "Software Safety Standard"

IEC 62 (Sec) 69 - "Electrical Equipment in Medical Practice"

UL 1998 - "Standard for Safety Related Software"

NATO STANAG 4452 - "Safety Assessment of Munition Related Computing Systems."

It should also be noted that Europe and the international community is well ahead of the U.S. in creating standards/guidelines for safety critical computer-based systems, particularly in the railway industry. This is apparent in several ways, perhaps most obviously in the UIC/ORE design and assessment recommendations for computer-based systems. The UIC and ORE (now ERRI) have been working in this area since the 70's. Another example is the current work being conducted by CENELEC for the railway industry within the European Community. Two standards are being developed (one directed to software and the other to system/hardware aspects). This work has been underway for several years by a working group of individuals from all over Europe.

Another observation is that terminology in the area of safety verifications and validations varies greatly among industries, organizations and individuals. In some instances the term safety verification was used to denote all activities that are performed to demonstrate the safety of a system. In other instances a safety verification was used to denote the activities performed at the end of each development phase to demonstrate compliance with the requirements of that phase--this is more consistent with the term **verification** in this country. A similar variation was found in the usage of the term safety validation. In at least one instance, safety validation was referred to as a type of audit in which someone or a group of individuals independently reviews the safety activities' assessments performed by others.

Perhaps the most significant observation concerns the diversity found in the various methodologies. This is addressed in more detail below.

### **3.2.2 Diversity**

A great deal of diversity exists in the methodologies/standards reviewed in this program. To begin with, the methodologies were developed (often within working groups) by personnel from diverse backgrounds and organizations (e.g., regulatory agencies, research firms, equipment suppliers and users) for different industries (e.g., rail, avionics, aerospace, military, nuclear, medical and consumer products). This in itself tends to diversify the methodologies

since the objectives, ways that safety is viewed and means of achieving safety differ from individual to individual, organization to organization and industry to industry.

The system coverage (or the portions or aspects of a system to which a given methodology applies) varies greatly. For example, some methodologies apply only to high level system aspects (e.g., conduct of system risk assessment) and do not directly address assessment of hardware or software. Two such methodologies are MOD 00-56 and DIN V 19250. Other methodologies (i.e., DO 178B, ANSI/IEEE 1012) apply only to software (development and assessment), while others address software and hardware or a combination of software, hardware and system aspects in varying degrees.

Further, the nature of the methodologies themselves varies tremendously. They range from requirements (either high or low level), guidelines and recommendations to menus of activities and techniques. Further, most methodologies specify "what is to be done" as opposed to "how to do it." Below are examples of the diversity that exists in the methodologies assessed:

- General system design and assessment guidelines (UIC 738R)
- Detailed design and assessment guidelines that describe means for detecting, avoiding and controlling errors and failures (DIN V VDE 0801)
- Software development requirements that include verification and validation aspects (DO 178B)
- Software verification and validation plan requirements (IEEE 1012)
- Software safety plan requirements (IEEE P1228)

System safety program plan requirements for developing and implementing a system safety program (MIL-STD-882C, ATCS Spec 140)

- System installation requirements (DIN 0831)--little safety verification and validation content

System risk assessment requirements/guidelines for determining safety integrity levels (DIN V 19250, MOD 00-56)

System/hardware proof-of-safety requirements addressing technical and management issues (CENELEC)

Independent verification and validation (IV&V) guidelines (JPL D-576, AFSC 800-5)

- Transmission system proof-of-safety recommendations (ORE A155.1/RP8)

Product investigation requirements that include system, hardware and software analyses (UL 1998)

Software development requirements that include formal methods with assessments (MOD 00-55)

Software engineering requirements that include verification and validation aspects (982 C-H69002-0001).

There is also diversity in the activities and the specific assessment techniques required or recommended by the different methodologies.

### **3.2.3 Single "Best" Existing Methodology**

The initial objective of the Base Task was to assess selected methodologies from the standpoint of their applicability and level of assured safety, and then to select the "best" existing methodology that would serve as a basis for developing a specific methodology for FRA's consideration.

Although the majority of the methodologies assessed were found to be generally applicable to equipment of interest and different design philosophies, each was found to "fall short" in some aspect(s) relative to assuring the safety of a computer-based system. For example, some methodologies apply to software only as opposed to an entire computer system. Others were found to not fully cover or address certain types of hardware and/or software concerns. For these reasons, a single "best" existing methodology was not identified following the Base Task.

However, at that time, several methodologies that were found to have significant attributes or qualities from, especially, a system safety verification/validation standpoint were identified. Those are as follows (in no particular order of importance):

ATCS Spec 140  
UIC/ORE A155/RP11 and A155.A/RP8  
Mü 8004  
MOD 00-55 and 00-56  
IEC 65 A (Sec.) 122 and 123  
MIL-STD-882C  
CENELEC CLC/TC9X/SC9XA/WGA1 and WGA2.

Two others with particularly good attributes from just a software safety verification/validation standpoint are RIA Tech Spec No. 23 and DO 178B. Several other software related standards (e.g., IEEE 1012) were found to be quite extensive from a verification and validation standpoint, but not exceptionally strong in or particularly directed to safety issues.

All of the methodologies and associated standards reviewed in the Base Task were considered when developing and recommending a reasonable, comprehensive and effective methodology for FRA's consideration.

### 3.2.4 Trends

As a result of reviewing the various existing methodologies and those in different stages of development across a number of industries worldwide (e.g., railroad, avionics, nuclear, military, medical, consumer product), a number of trends were observed. Several of those are described below:

- 1) Safety related assessments are being required/recommended throughout the development cycle of a computer-based system, from conceptual design through final development stages. Most include safety related verifications following each major design phase of the system, and software and safety validations at the end of development.
- 2) Hazard analyses and risk assessments are being required/recommended in early design stages to help identify and eliminate (or reduce the risk associated with) potential system hazards and assign safety integrity levels to entire systems and/or specific functions.
- 3) A wide mix of analysis and testing techniques are being required/ recommended -- no clear choices are dominating.
- 4) (A "non-trend") - There is actually no clear trend toward either requiring or just recommending/suggesting possible verification/validation techniques. Some methodologies require specific techniques while others provide menus of techniques.
- 5) Emphasis has been on software, but is now becoming more comprehensive from a system standpoint as groups and organizations realize the importance of safety in a system context.
- 6) Formal methods for software development are gaining acceptance and are being recognized as useful techniques. To date, most methodologies do not require their use.
- 7) Methodologies are requiring/recommending separate safety-related development and assessment processes/activities for software (in addition to those for an overall system).
- 8) Methodologies are requiring/recommending independent safety assessments (to assess safety of equipment) and/or safety audits (to review safety activities and associated outputs conducted by others).

- 9) Methodologies are requiring/recommending the establishment and implementation of quality assurance plans (e.g., those associated with ISO 9000 series standards) in addition to safety plans. The proper implementation of quality assurance plans is expected to minimize the existence of both hardware failures and software errors.
  
- 10) Emphasis appears to be placed on proof-of-safety requirements--what process, activities and documentation has to be performed/submitted to adequately demonstrate the safety of a system.

It should be noted that most methodologies and associated standards reviewed in the Base Task are directed to both development and assessment aspects. Safety V&V is more of an assessment, and represents only one part of the overall safety assurance process that is being followed by most organizations. More discussion on this matter is provided in Section 4.1.2.

## 4. SAFETY VALIDATION METHODOLOGY DEVELOPMENT

The objective of this program was to develop an (analytical) safety validation methodology to help ensure and demonstrate the safety of computer-based systems, subsystems and equipment. Earlier activities (in the Base Task) and results obtained greatly facilitated this development effort. These earlier activities included the investigation of existing system level as well as hardware and software safety verification and validation processes and activities developed and/or utilized by others. It also included investigating when in system, hardware and/or software development these safety activities are performed. This was important since activities to ensure and demonstrate safety are typically performed throughout system development (as opposed to just at the end of development).

This section provides some background information on the development of the safety validation methodology for this program. It begins with a discussion of various issues regarding the nature of the methodology, its applicability and usage by the FRA. Following this, there is a discussion on how the methodology being developed in this program fits into the overall scheme of safety assurance in computer-based systems. The recommended methodology itself is described in Section 5.

### 4.1 DISCUSSION OF ISSUES

#### 4.1.1 Safety Validation Methodology-What is it?

As was observed earlier in this program, there is a lack of common usage in the various other methodologies and standards addressed relative to the terms "verification" and "validation" as well as "safety verification" and "safety validation." In many of the methodologies/standards reviewed, the terms verification and validation are used in a similar manner to that conveyed in the Institute of Electrical and Electronics Engineers (IEEE) document "Standard Glossary of Software Engineering Terminology," IEEE Std. 610.12-1990. In that document, which pertains specifically to software, the terms verification and validation are defined as follows:

- Verification--The process of determining whether or not the products of a given phase of the (software) development life cycle fulfill the requirements established during the previous phase.
- Validation--The process of evaluating (software) at the end of the software development process to ensure compliance with software requirements.

It should be noted that the above definitions are not specifically directed to safety or safety requirements. Rather, they apply to software requirements in general. Many of the methodologies reviewed in this program use similar definitions when dealing with demonstrating compliance with safety requirements for software, and also extend these definitions to address system and even hardware safety requirements. In these instances, the methodologies use terms such as safety verification, safety validation, system validation and

even software and hardware verification and validation. Terms/phrases such as proof-of-safety and technical proof-of-safety are also used. Overall, many different terms relating to safety verifications/validations are used in other methodologies, and the terms have a multitude of different meanings.

It is believed that, in this program, the desired (safety validation) methodology is one that describes a process and associated activities which are conducted to demonstrate or "prove" the safety of a computer-based system, subsystem or item of equipment. It is also believed that a process of this nature does not rely solely on activities conducted at the end of system development. Rather, the most effective (validation) process to demonstrate safety is based on a collection of activities which are integrated into the system, hardware and software development processes. Further, such activities to demonstrate safety which are conducted at the end of specific system, hardware and software development phases can be referred to as (safety) verifications, while those conducted at the end of hardware, software and system development, respectively, can be referred to as (safety) validations. This is consistent with the traditional (software) definitions of verification and validation as described above. However, the definitions have been extended to apply to hardware as well as an entire system, and have been limited to apply to safety aspects only.

In light of the above, the safety validation methodology addressed in this program is actually a safety verification and validation (V&V) methodology that is comprised of a collection of analyses, tests, calculations, etc., performed at different stages in system (as well as hardware and software) development to demonstrate compliance with all safety requirements. This includes demonstrating with a high degree of confidence that potentially unsafe hardware failures, software errors and other hazards have been eliminated or, where appropriate, showing that hazards do not present unacceptable risks. The resulting documentation from applying this process provides evidence as to the safety of the system/subsystem/equipment design. This methodology could also be referred to as a technical proof-of-safety process, with the resulting documentation comprising a technical proof-of-safety.

#### **4.1.2 Role of Safety V&V in Overall Safety Assurance**

The utilization of a safety V&V methodology (such as the one described in this report) is certainly a key aspect in helping to ensure a safe system. However, it is believed that there are other aspects which, when combined with a safety V&V methodology, provide an even higher level of confidence in the safety of a system. These other aspects pertain more to designing safety into a system (and are basically preventive in nature) as opposed to safety V&V which pertains more to demonstrating or proving the actual safety of the design.

These other aspects can be generally categorized into two major areas: Safety Management and Quality Management. Safety Management includes activities such as developing/implementing a system safety program plan (which defines all safety related activities to be performed during system development), establishing a safety organization and holding periodic design reviews. Quality Management includes a wide range of activities, one of which involves the establishment/implementation of well-structured system, hardware and software development processes. The actual system, hardware and software development

processes will most likely be accompanied by various hazard analyses and risk assessments to help identify potential hazards (and means of eliminating/resolving them) as the design progresses. Thus, safety and quality management activities help to minimize hazards in the design (including potentially unsafe hardware failures and software errors) while the safety V&V activity helps to show that the hazards have been eliminated or the associated risks reduced to acceptable levels and all safety requirements have been met.

Safety Management, Quality Management and safety V&V processes and associated activities, together, could comprise an overall safety assurance process. Further, evidence that these three aspects have been applied in a system's development (including results of applying them) could comprise an overall proof-of-safety for the design. Evidence of applying a safety V&V process (as well as results) could be, and is, considered in this program as a (technical) proof-of-safety of the design--just one part of the overall safety assurance process.

Section 4.2 of this report describes some key elements/activities of the safety and quality management aspects within an overall safety assurance process. Then, Section 5.0 describes the safety V&V methodology itself, which is the primary focus of this program.

It is very important to note that most railway and other organizations reviewed in this study have developed standards/guidelines that address both development and assessment aspects, including various safety and quality management issues. Safety V&V is essentially an assessment of safety, and, while important, is not believed by most organizations to be sufficient by itself to ensure safety. Thus, the content of most standards is not limited to safety V&V activities, but rather, is directed to the "bigger picture" of development and assessment and the overall safety assurance issue. Therefore, it is recommended that the FRA consider going beyond safety V&V, and consider addressing the "bigger picture" of overall system safety assurance.

It should also be noted that safety assurance is just one aspect of overall system assurance, which could include (among others) reliability, maintainability, availability, security, and others. The whole of system assurance aspects is sometimes referred to as dependability. However, as noted, this program deals with the safety assurance part of system assurance, and more specifically, with the safety V&V aspect of safety assurance.

#### **4.1.3 FRA's Role and Intent of Methodology**

At the present time, it is understood that the FRA wants any (safety V&V) methodology that results from this program to serve as a "recommended practice" for suppliers rather than a strict requirement. However, even in this manner, a resulting methodology could serve as a standard in the industry. This goes along with the FRA's currently desired role in enforcing or ensuring compliance with the methodology. More specifically, at the present time, the FRA does not want to undertake a certification or approval role for all new or existing computer-based systems (such as is done by other organizations such as the Federal Aviation Administration—FAA). Rather, the FRA wants to have the methodology in place in order to establish a more consistent basis for the industry relative to demonstrating safety and to improve/maintain existing levels of safety.



However, there may be a desire under certain circumstances (e.g., following an accident or at random on new systems) for the FRA to have an audit conducted in order to determine compliance with the methodology. An audit of this nature could be conducted directly by the FRA, or via a third party organization. A general process for ensuring compliance with the methodology is outlined in Section 5.4 of this report.

#### **4.1.4 Nature of the Methodology**

The safety V&V methodology presented later in this report is preliminary in nature and is at a relatively high level for two main reasons. First, before a "final" methodology can be established, it is necessary to discuss and resolve many of the issues presented in this report. This includes the intended use of the methodology, FRA's role in compliance assurance, the extent to which the methodology describes "how to do it" versus "what to do." and the expansion of the methodology to include the bigger picture (i.e., overall safety assurance--with safety and quality management issues). Second, any methodology of this nature which is used as a recommended practice or requirement for the railway industry should include industry input. An industry input task was originally intended for this program, but was subsequently eliminated (following the Base Task effort) as it was considered premature primarily because of the following:

- The extensive effort required to identify, obtain, review and assess existing safety V&V methodologies for numerous organizations
- The results of the methodology assessment (conducted in the Base Task)--extreme diversity in existing methodologies and no single methodology that was found to serve as a good basis for a railway-specific methodology, and
- The need to discuss and resolve numerous issues (such as those discussed in this section).

However, an industry input cycle is still considered important before any final methodology is presented to the industry as a standard.

In addition to being preliminary in nature, the recommended safety V&V methodology emphasizes "what to do" as opposed to "how to do it." In other words, various activities that comprise the methodology are identified along with their intent (why they should be performed) and when during system, hardware and/or software development they should be conducted. This is consistent with the current trend in existing and draft safety V&V methodologies worldwide. and would probably be more desirable to suppliers as well.

#### **4.1.5 Applicability of the Methodology**

The safety V&V methodology herein is applicable to computer-based systems, subsystems or equipment which perform safety critical functions in the railway industry. This includes signalling/train control, communications and other systems (e.g., grade crossing systems) that

could involve wayside, on-board and even centrally located equipment in conventional as well as high-speed rail applications. Examples include interlockings, track circuits and other train detection equipment. speed measurement/control subsystems affecting propulsion and/or braking and enforcing speed limits: and data communications equipment responsible for transmitting, receiving, encoding and decoding safety critical data. Also included is safety critical equipment used in other fixed guideway applications such as maglev. Examples here include equipment pertaining to the control of vehicle speed and guideway power, vehicle separation, levitation, guidance, switching and safety related communications.

The methodology is also applicable to systems with different design philosophies including different hardware and software configurations. Limiting the methodology to a single design philosophy/configuration would greatly limit its usefulness (and place significant design restrictions on a supplier) unless a decision is made at a later time to require or prohibit certain philosophies/configurations. Some of the design philosophies/configurations currently being used in computer-based safety critical systems are as follows:

Single channel systems (essentially one microprocessor performing any given function in a single data path) with extensive embedded diagnostics

Single channel systems based upon special embedded software coding and signature techniques

Single channel systems with multiple diverse software programs

Dual channel redundant (hardware) systems with hardware and/or software comparators

Triple channel systems with voting schemes.

As indicated earlier, the recommended methodology consists of a set of activities that are integrated into the development process of a system. It addresses both hardware and software safety issues as well as system safety aspects such as hazards associated with a human operator interface. The methodology is primarily directed to new systems as opposed to existing systems. Further, it is structured to be performed primarily during the system development process itself. It is believed that this is the most efficient manner to conduct safety V&V, and results in the safest system. However, it is possible to conduct the methodology post-development, provided all activities are conducted and there is access to all applicable design information from the different phases of development.

#### **4.1.6 Safety Requirements**

Since the main purpose of safety V&V is to demonstrate compliance of a system (including hardware and software) with safety requirements, it is necessary to establish proper and complete safety requirements before any verifications/validations are performed. While the FRA may (in the future) establish some safety-related requirements and recommended practices for the verification/validation and/or design of computer-based systems in general, it

will be up to the user to establish certain other specific safety requirements relative to their application such as safety functions to be performed and perhaps even a quantitative level of safety. The safety V&V methodology in this report focuses on the method or process to be used to demonstrate or prove safety (demonstrate compliance with safety requirements), rather than on safety requirements in general. However, certain safety requirements are inherent in the methodology presented. For example, some requirements pertaining to demonstrating safety under conditions of normal operation, hardware failure, systematic failure and external influences are given (in Section 5.2).

Also, as discussed earlier, V&V traditionally includes determining compliance with all (software) requirements, including those pertaining to safety. The recommended safety V&V methodology refers to system, hardware and software safety related requirements only. The determination of compliance with other non-safety related requirements is certainly important from a functional, performance and overall system assurance standpoint, but it is not considered as part of the safety V&V methodology covered by this program.

**4.1.6.1 Level of Safety** - One of the safety issues relative to computer systems that has been under investigation by many organizations worldwide for quite some time centers around the quantification of computer system safety. One primary concern involves a meaningful quantification of software safety and its relationship/contribution to overall system safety. Another concern involves establishing how safe (in quantified terms) an overall system should be.

Safety critical systems in the railway industry have traditionally been designed to be "fail-safe," being based on "vital relays" and other discrete components with well-defined failure modes. However, even in these vital relay based systems, safety is not absolute. Rather, it is probabilistic in nature since there is still a finite, but extremely low, probability that an unsafe failure could occur.

Software, on the other hand, does not "fail" in the same sense as hardware, but contains errors that could be unwantingly inserted into the software at different phases in the development process. Although some means exist (e.g., metrics) for estimating software reliability/safety (existence of errors) in a quantitative manner, there is currently no widely accepted practice that gives meaningful results. Further, it is generally accepted throughout different industries that it is virtually impossible to identify and remove all errors from software of any significant complexity.

Suppliers have been using special design techniques and philosophies including different hardware and/or software configurations (e.g., redundancy) to help minimize the existence of software errors, to detect potentially unsafe hardware failures/conditions and to ensure that safe states are achieved. The goal of these design techniques is to effectively provide a relatively low probability of unsafe system failure.

Of the safety assurance methodologies reviewed and assessed earlier in this program, the majority do not require a specific quantified level of safety for computer systems. Some of these methodologies indicate that a computer system should be as safe as existing fail-safe

systems (implemented with vital relays and other discrete components with well-defined failure modes) that perform the same functions. A few others briefly address the quantification issue, but make the determination of a mean-time-between-unsafe-failure (MTBUF) or mean-time-between-wrong-side-failure (MTBWSF) value for a system as optional. The CENELEC organization (establishing safety standards for the railway industry in the European Community) requires that a quantitative level of safety be demonstrated, but still places emphasis on a qualitative demonstration of safety. This whole matter of a quantified level of safety is certainly an issue for FRA's consideration--whether or not to establish a quantitative safety requirement or goal for computer-based systems, and what an appropriate value would be.

Another related matter must be discussed here. This concerns the existence of criteria or a benchmark for determining that a given system is adequately safe. There is, at the present time, no simple meaningful criteria or simple test that can be used to determine that an adequate level of safety has been achieved. Rather, the "criteria" is based upon the proper conduct of a well-structured/managed development and safety V&V process, including showing that all applicable safety requirements are met. This same concept applies to the safety V&V methodology recommended in this program. However, as discussed earlier, the methodology is directed to safety V&V and not the entire development/management issue (due to the scope of work of this program). The means of determining that an adequate level of safety has been achieved in a given system is by determining/assessing how closely a supplier followed the recommended process. This is the primary reason why the European railway organizations require an independent assessment/audit to approve new systems--to assess whether or not the required (development and safety V&V) methodology has been properly followed.

One alternative is to have a meaningful quantitative level of safety for the system. However, as discussed above, neither has an adequate and meaningful quantitative level of safety been established for railway systems, nor has an acceptable and meaningful means of establishing such a level been developed.

As will be observed later in this report, the recommended methodology includes a requirement for demonstrating that a system meets a quantified safety target or goal--but only if a quantified goal is identified by the user. Further, the quantified level of safety is treated as a goal only--the primary emphasis still being qualitative. It should also be noted that no specific quantitative value/number is cited by the subject methodology.

#### **4.1.7 Safety V&V Vs. Hazard Analysis/Risk Assessment**

There appears to be two major philosophies in existing safety assurance methodologies relative to demonstrating the safety of system design. One is heavily based on the conduct of different hazard analyses and risk assessments throughout the system development process in order to identify potential hazards, determine associated severities and probabilities of those hazards, determine associated risks, and determine means of eliminating/resolving the hazards. These analyses are then often updated when the design is complete, and supplemented by what is usually referred to as verification testing, to demonstrate compliance with safety

requirements and overall system safety. One example of a methodology of this nature is MIL-STD-882B/C. In these instances, there are usually separate methodologies directed more to the development and general V&V of software. The safety standards developed and utilized by the Ministry of Defence (i.e., MOD 00-55 and 00-56) follow a similar philosophy. but are based on the utilization of formal methods including mathematical proofs to help demonstrate the safety of software.

Another slightly different safety philosophy is utilized by various railway suppliers. authorities (e.g., German Federal Railway) and other railway organizations (e.g., Railway Industry Association) in the U.S. and Europe. This philosophy is based more on the use of hazard analyses in the early stages of system development to identify potential hazards and associated risks--the intent being to help establish safety requirements and impact the design early. Then, safety verification and/or validation activities (comprised of analyses, testing, calculations, etc.) are performed on hardware. software and the overall system to ensure safety requirements are met and that no unsafe conditions (e.g., unsafe hardware failures, software errors or other unacceptable system hazards) are present in the system. One could argue that there is not a great deal of difference between the two philosophies described here. Both are usually qualitative in nature and both involve activities to demonstrate safety. However, the primary difference is that the latter one does not rely as much on the use of risk assessments to demonstrate safety of the system (particularly where hardware failures and software errors are concerned)--the emphasis is on showing (via what is referred to as safety verifications and validations--safety analyses and testing) with a high degree of confidence that safety requirements are met and no potentially unsafe hardware failures or software errors are present in the system. This latter philosophy, in some instances, does involve a very limited risk assessment (for the demonstration of safety) that is directed to certain system level aspects.

As will be observed, the methodology recommended in this report is actually based upon a combination of the above two philosophies, with more emphasis on the latter.

#### **4.1.8 Safety Integrity Levels**

Several European organizations (e.g., IEC, RIA, CENELEC) utilize a concept in their computer system safety standards referred to as safety integrity levels. This essentially involves categorizing either an overall system or the software into different levels of safety depending upon the criticality or degree of risk that could be afforded by the system/software. For example, an interlocking system and certain software portions thereof would be assigned the highest safety integrity level, while a train identification (but not detection) system may be assigned a lower level. These integrity levels are determined via the conduct of a hazard analysis and risk assessment in the early development phases of system development. Then, various safety verification and validation techniques as well as certain safety requirements are suggested/defined for the different integrity levels. This is done to not only relate the most stringent safety requirements to systems with the greatest risk potential. but also to allow the greatest development (including safety V&V) effort to be directed to these systems and certain key software portions.

The recommended methodology, at this time, is not based on the concept of safety integrity levels (i.e., it does not define different activities or techniques for different systems). Rather, it is intended to be applicable to all safety critical computer-based systems including those that present the highest level of risk. It may be desired in the future to further investigate the benefits of safety integrity levels as a part of an overall safety assurance methodology.

#### **4.1.9 Hardware/Software Modifications**

Most of the safety methodologies/standards reviewed in this program discuss (to varying degrees) hardware/software modifications and the need to conduct associated reverifications/revalidations. However, none of them identify specific detailed processes for conducting these reverifications/revalidations. Rather, they generally indicate that the impact of the modifications need to be assessed and safety must be ensured. Most seem to agree that, in most cases, a complete system reverification/revalidation is not needed--only the affected portions.

The safety methodology in this report does include a recommended, but relatively high level, process for ensuring safety following modifications. The determination of a more detailed process for ensuring safety following hardware/software modifications would require a more thorough investigation beyond this program.

#### **4.1.10 Independent Safety Assessment**

Practically every European safety assurance methodology/standard reviewed in this program as well as some in the U.S. requires an independent assessment of some nature to be conducted on safety critical computer-based systems. These assessments vary some in nature, but generally are of two types. One (and the most common) type resembles an audit in which an independent organization reviews the safety development (including safety V&V) process and activities performed by the developer as well as all results to ensure compliance with the requirements of a given standard that was established as a basis for acceptance of a system. As mentioned earlier, this is done to give the approval organization the confidence that the required processes/activities have been properly carried out. The approval organization then bases acceptance of the system on results of the assessment/audit. Another type is more of an independent safety V&V activity in which an independent organization conducts analysis and testing activities totally separate from the developer in order to determine compliance with safety requirements. In some cases this is required for an independent verification and validation (IV&V) of the software in general. Consideration should be given to requiring an independent assessment of some nature for the safety V&V methodology as well as for an overall safety assurance methodology (at some time in the future).

## **4.2 OVERALL SAFETY ASSURANCE METHODOLOGY**

As discussed above, a safety V&V methodology as is being developed within this program is considered to be only one aspect of an overall safety assurance methodology, the others being

related to Safety Management and Quality Management. Safety Management and Quality Management are preventive measures to impact the design while safety V&V demonstrates the safety of the design itself.

It was also suggested that all evidence associated with applying these three aspects (i.e., Safety Management, Quality Management and safety V&V) in the development of a system comprises an overall proof-of-safety. Evidence of applying safety V&V, by itself, could be considered as a technical proof-of-safety.

Although this program is directed to the development of a safety (verification and) validation methodology, and addresses only one part of an overall system safety assurance methodology, it is considered important to discuss what other safety aspects are associated with Safety and Quality Management. This will help put the safety V&V methodology in context of overall system safety assurance.

Therefore, this section discusses the nature and purpose of Safety and Quality Management and focuses on some of the associated key aspects. It does not address these in a comprehensive manner--this would require additional efforts beyond the scope of this program. The recommended safety V&V methodology itself is addressed in Section 5.

Although there is not universal agreement on the relationship between quality (assurance) and safety, this report treats Quality and Safety Management as separate aspects which, together (with safety V&V), help to ensure overall system safety.

#### **4.2.1 Quality Management**

The overall quality of a system, subsystem or piece of equipment should be controlled/managed through the establishment and implementation of a quality system. This quality system can be defined in a quality plan which describes all quality procedures and associated documentation utilized to ensure overall system quality and to demonstrate all relevant design and manufacturing procedures have been correctly followed throughout the system life cycle. Guidance on the establishment of a quality system can be obtained in the ISO 9000 series of quality assurance standards, and in particular, ISO 9001. The implementation of a complete and well-defined quality system can help minimize potentially unsafe conditions in the design, since it can reduce the incidence of human error that could occur at various development life cycle phases. It is also possible for a supplier to obtain ISO 9001 certification--this is highly recommended.

It is also suggested that software quality aspects be addressed separately in a software quality assurance plan such as one that is compliant with the ISO 9001-3 or other appropriate standard. It may also be desired to establish a separate hardware quality assurance plan.

Some of the system aspects which could be controlled by the quality system are as follows:

- Design reviews
- Verification and validation
- Manufacturing
- Product identification/traceability
- Configuration management and document control
- Packaging/delivery
- Installation
- Operation and maintenance
- Organizational structure, personnel qualifications and training
- Quality audits.

Several key areas are addressed in more detail below.

**4.2.1.1 System Development Process** - There should be a well-structured overall system development process which identifies all major phases and activities of system development from concept through operation and maintenance. Again, ISO 9001 provides guidance on developing such a process. There is no one single universally accepted process, but typical phases/activities are as follows:

- Concept
- System definition
- Requirements definition
- System design
- Detailed design of hardware and software
- Implementation
- Integration and testing
- Installation
- System acceptance
- Operation and maintenance.

**4.2.1.2 Software Development Process** - There should also be a well-structured software development process/life cycle (such as that suggested in ISO 9001-3) which defines all software development phases and activities. As stated earlier, this can be described in a software quality assurance plan. Again, there is no single universally accepted development life cycle, but several good examples are found in the IEC, CENELEC, RIA and IEEE software standards described earlier in this program. Some typical activities that should be addressed by this software development process are as follows:

- Software Requirements Specification development
- Software Architecture Specification development
- Software architecture design
- Software Design Specification development
- Software design
- Software Module Design Specification development
- Software module design
- Software module coding



Software integration testing  
Software/hardware integration testing.

Verifications and validations for functional as well as safety aspects should be integrated into this development process.

Other key aspects that could be covered by a software quality assurance plan include a detailed description of all life cycle phases (e.g., tasks to be performed, inputs and outputs of each phase, and entry and exit criteria), a requirements traceability matrix, definition of all documentation to be produced, configuration management procedures, system/hardware integration procedures, and coding standards. It should be emphasized that these are just examples, and do not totally define the contents of a software quality assurance plan. As noted above for the overall quality plan, the development and implementation of a software quality assurance plan helps to minimize human error and resulting unsafe conditions in the software. This is due to the utilization of a logical, well-structured, and closely monitored software development process.

**4.2.1.3 Quality Audit** - The conduct of quality audits is a key management activity in the overall quality system since they are used to determine and ensure compliance with all quality related procedures and documentation.

## **4.2.2 Safety Management**

Another extremely important aspect of overall safety assurance pertains to the establishment and control of an overall safety process via safety management activities. This helps to even further minimize the incidence of potentially unsafe conditions in a system. Just as a quality plan can be prepared to address quality aspects, a safety plan can be utilized to describe all safety activities including the management structure. More on the safety plan is provided later in this section. Some of the key aspects of Safety Management (as it is defined in this report) are discussed below.

**4.2.2.1 Integrated Safety Process** - There needs to be a managed safety process or safety life cycle which defines all safety related activities that should be performed as part of the system development life cycle including hardware and software development. The process should also define when in the respective development processes specific activities are to be performed. It is possible that the safety activities could be defined along with the system, hardware and software development processes discussed in the quality management sections of this report. However, it is necessary to define all activities in some manner.

Some of the key safety related activities which would be expected to comprise the safety process are as follows:

Preliminary Hazard Analysis (PHA)--performance of a hazard analysis and associated risk assessment on the conceptual system in the early stages of system development; performed to identify potential hazards and associated risks in the system so that safety concerns can be addressed early and the design can be appropriately directed: preparation of a Preliminary Hazard List (PHL) that identifies types of hazards to be aware of may be helpful

Safety Requirements Specification--identification of overall safety requirements for the system in a Safety Requirements Specification; based upon overall system/user requirements (including safety related functions to be performed), the PHA and safety concerns of computer-based systems in general

Safety requirements allocation--allocation of safety requirements to hardware and software; based upon a Safety Requirements Specification and architectural design decisions including the overall design philosophy

Other hazard analyses--conduct of other hazard analyses and risk assessments (if desired) as design progresses to help identify hazards and their associated risks, and to identify possible means of eliminating hazards or reducing their risks to acceptable levels: possible examples include those identified in MIL-STD-882B/C and/or the Advanced Train Control System (ATCS) Specification 140: System Hazard Analysis (SHA); Subsystem Hazard Analysis (SSHA); Operating and Support Analysis (O&SHA); Failure Modes, Effects and Criticality Analysis (FMECA); and other hazard analyses directed to the design and coding of software; the conduct of analyses of this nature will help ensure the success of the (safety) verification and validation effort

Safety verification and validation--conduct of various analyses and tests at the conclusion of certain system, hardware and software development phases to demonstrate compliance with safety requirements; as will be discussed more later, the safety V&V activities can, in some instances, draw from and rely on some of the hazard analyses conducted as preventive measures to impact the design; thus, as can be observed, safety V&V is just one of several design-related safety activities which help to ensure a safe design

Reverification/reevaluation of modifications--conduct of safety verifications/validations as appropriate to demonstrate safety following hardware, software and other system related modifications.

It should be emphasized that the above activities do not represent a comprehensive set of all safety related activities that should be part of a safety process or life cycle, but do outline some of the key elements of a typical safety process.

**4.2.2.2 Safety Organization** - Another key element of Safety Management is the establishment and control of an appropriate safety organization. This includes the identification of an overall safety management structure and the identification of groups that

have specific safety responsibilities. It also includes the identification of personnel qualifications, roles and responsibilities.

**4.2.2.3 Safety Reviews** - It is considered very important to hold periodic design reviews throughout system development. These not only help ensure that key safety activities are carried out at their appropriate times, but also help ensure that safety issues are addressed and resolved in a timely manner. Reviews of this nature are in addition to quality audits which, as indicated earlier, should also be conducted throughout system development.

**4.2.2.4 Hazard Tracking** - A hazard tracking mechanism/process should be established to record and track the identification and resolution of hazards identified in the PHA, subsequent hazard analyses and during other system development activities.

**4.2.2.5 Safety Plan** - Perhaps one of the most important activities of Safety Management is the development (and implementation) of a safety plan, often referred to as a System Safety Program Plan. This document describes the various activities and requirements for conducting and managing the entire system safety effort. It can include descriptions of the various elements discussed above such as the overall safety process or life cycle and associated activities, the safety organizational structure, safety reviews, schedule and milestones, safety related documentation, and even safety verification and validation plans (to be addressed later in this report).

## 5. RECOMMENDED SAFETY VERIFICATION AND VALIDATION METHODOLOGY

This section discusses and describes the safety verification and validation (safety V&V) methodology being recommended in this program. There are first some introductory comments, followed by a discussion of general safety requirements for computer-based systems, and then a description of the methodology itself. The methodology is directed to computer-based systems including subsystems and equipment which may comprise a part of an overall system. Many of the issues pertaining to the development and presentation of this methodology were discussed earlier in Section 4.1.

### 5.1 INTRODUCTORY COMMENTS

For reasons discussed earlier, the methodology is considered preliminary, and is at relatively high level--describing activities that should be conducted and general safety requirements pertaining to the conduct of those activities. It also describes the purpose of the various activities, their interrelationships (i.e., how they, together, help to demonstrate safety), and at what point in the system development process they should be performed.

Although emphasis is on what needs to be done relative to safety V&V, rather than how to do it, some example techniques (e.g., Failure Modes and Effects Analysis, Fault Tree Analysis) are cited in certain instances. It is believed that suppliers should have some freedom, not only in designing their system. but also in demonstrating its safety.

Safety V&V activities are best and most efficiently conducted if they can be integrated into, and conducted in parallel with, the system development process. Therefore, the methodology is structured in this manner. However, as discussed earlier, it is possible to apply this methodology post-development as long as appropriate design information/ documentation for different design phases is available and utilized.

To summarize earlier discussions as to the nature and purpose of safety V&V, safety V&V demonstrates or "proves" the safety of the implemented design--that it meets all safety requirements. It should be noted that safety V&V also can, and usually does, impact the design since the verification and validation activity will often result in a revision (to the design or other aspect) and may require a repeat of all or a portion of the verification/validation activities to check the revision. However, the primary purpose is to demonstrate safety.

It should also be noted that, in many instances, special design techniques (e.g., software diversity--two or more different programs to perform a given function) are used to help ensure safety. If this is the case, safety V&V documentation should include the identification/description of these, how they help to ensure safety, and justification for why certain safety V&V activities were not considered necessary.

Safety V&V activities performed at intermediate stages in the development of the overall system as well as hardware and software are referred to as safety verifications, while activities performed on the final integrated system including the final hardware and software are referred to as safety validations. Also, as discussed earlier, V&V traditionally refers to the determination of compliance with all functional and performance requirements, including those pertaining to safety. However, this safety V&V methodology refers only to safety related requirements.

Documentation that plays a key part of the safety V&V process (either as inputs or outputs) is identified as appropriate within the various activities. These include planning-related as well as results-related documentation. It should be noted, however, that although certain documents are cited, they represent only a small number of the documents that would normally be generated in system development. Further, the documentation cited is for purposes of example only, and is not intended to be viewed as strict requirements relative to their titles or specific content.

It was briefly discussed earlier that all evidence relative to the planning, conduct and results of safety V&V could be viewed as a technical proof-of-safety for the design, depending on whether the documentation applies to a basic system or a given application. Further, this evidence plus other evidence relative to the areas of Quality Management and Safety Management including associated processes could comprise an overall proof-of-safety for a system. It is understood that in many instances a generic system may be developed and then revised accordingly (in hardware, software or other means) to meet the requirements and functions of a given application. If this is done, it is necessary that the safety V&V conducted show compliance with the safety requirements for the specific application. This could be done by having a generic technical proof-of-safety for a basic system and a revised technical proof-of-safety (or safety case) for a given application. This could also apply to the overall proof-of-safety for the system--there could be a generic proof-of-safety and then a revised application-specific safety case.

## **5.2 GENERAL SAFETY REQUIREMENTS**

There are a number of safety requirements that should be addressed when demonstrating the safety of computer-based systems. These can generally be categorized into the following areas:

Normal operation -- The system (including all hardware and software) must be shown to operate safely under normal anticipated operating conditions with no hardware failures, proper inputs and in the expected range of environmental conditions. All safety critical functions must be performed properly under these normal conditions.

Systematic failure -- The system must be shown to be free of unsafe systematic failure--those conditions which can be attributed to human error that could occur at various stages throughout system development. This includes unsafe errors in the software due to human error in the software specification, design

and/or coding phases: human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed man-machine interface: installation and maintenance errors: and errors associated with making modifications.

Hardware failure – The system must be shown to operate properly under conditions of random hardware failure. This includes single as well as multiple hardware failures, particularly in instances where one or more failures could occur, remain undetected (latent) and react in combination with a subsequent failure at a later time to cause an unsafe operating situation. In instances involving a latent failure, a subsequent failure is similar to their being a single failure. Another concern of multiple failure involves common mode failures which could compensate one another and result in unsafe conditions. This is of particular concern in instances in which two or more elements (hardware and/or software) are used in combination to ensure safety. One example involves the use of redundancy in which two or more elements perform a given function in parallel. Another example is when one (hardware and/or software) element checks/monitors another element (of hardware or software) to help ensure its safe operation. Common mode failure relates to independence, which must be ensured in these instances.

When dealing with the effects of hardware failure, it is necessary to address the effects of the failure not only on other hardware, but also on the execution of the software (since hardware failures can greatly affect how the software operates).

External influences – The system must be shown to operate safely when subjected to different external influences such as:

Electrical influences – e.g., power supply anomalies/transients, abnormal/ improper input conditions (e.g., outside of normal range inputs relative to amplitude and frequency, unusual combinations of inputs) including those related to a human operator, and others such as electromagnetic interference and/or electrostatic discharges

- Mechanical influences – e.g., vibration, shock
- Climatic conditions – e.g., temperature, humidity.

Modifications – Safety must be ensured following modifications to the hardware and/or software. All or some of the concerns identified above may be applicable depending upon the nature and extent of the modifications.

These general requirements are addressed and discussed as appropriate within the specific safety V&V activities in the next section.

### 5.3 SAFETY V&V METHODOLOGY

The safety V&V methodology as presented in this section has been structured to address the safety concerns identified above. These same concerns formed the basis for the criteria which were used to assess the existing safety methodologies/standards earlier in this program. The methodology itself consists of a set of activities which can be separated into the following general areas:

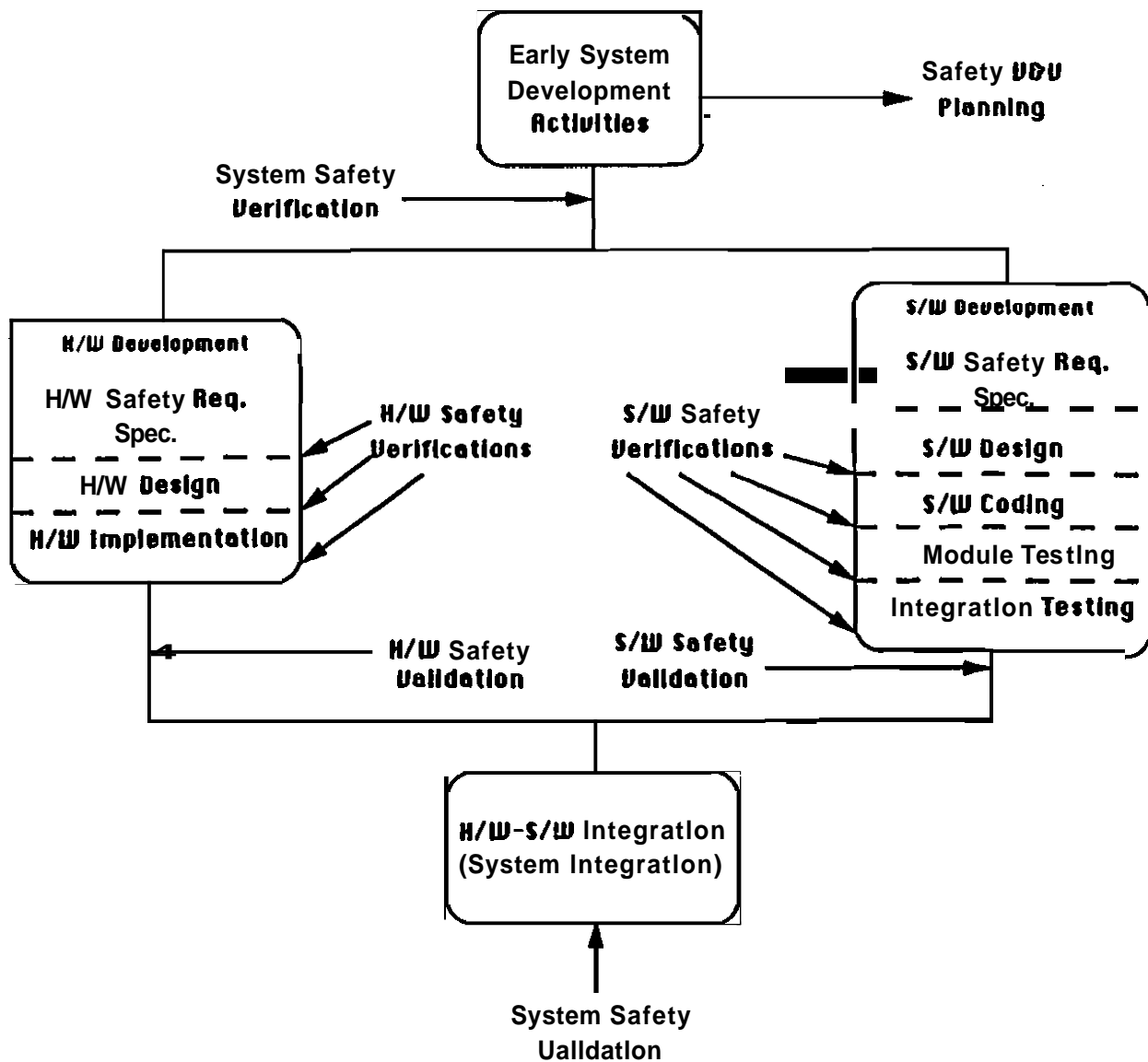
- Safety V&V planning
- Software safety V&V activities
- Hardware safety V&V activities
- System safety V&V activities
- Safety V&V of modifications.

The various activities of the methodology and their relationship to a typical system development cycle are shown in Figure 1. As can be observed from the figure, various safety verifications and validations are integrated throughout the development process.

#### 5.3.1 Safety V&V Planning

Before V&V is initiated, and typically in the early stages of system development, various activities should be performed to prepare initial plans for the conduct of all safety V&V activities. Some suggested plans which may be in separate documents or combined in some appropriate manner are as follows:

- System (Safety) Verification Plan
- System (Safety) Validation Plan
- System Test Plan
- Software (Safety) Verification Plan
- Software (Safety) Validation Plan
- Software Safety Plan — not always utilized, but could describe all activities, including safety V&V, that are planned to ensure the safety of the software; if used, it could incorporate the Software (Safety) Verification and Validation Plans
- Hardware (Safety) Verification and Validation Plans.



**FIGURE 5-1. SAFETY V&V METHODOLOGY ACTIVITIES**

These represent only the major, high-level safety-related V&V planning documents that should be generated. They could actually be part of broader verification and validation planning documents which address other aspects in addition to safety (e.g., reliability, performance). There could also be separate verification plan documents for each verification activity pertaining to the software and/or hardware. In addition, there could also be software and hardware test specifications for different development phases. There are, of course, many other system, hardware and software development related documents which are not addressed here because they do not directly impact safety V&V.



Although the actual verification and validation planning documents prepared could vary, they should cover the associated activities to be performed, the strategies and techniques (analyses, testing) to be used, test cases where applicable, test equipment, documentation to be produced, and responsible parties for the conduct of the various activities.

One of the key documents that should be used as input to this planning activity is a System Safety Requirements Specification, which may be a part of an overall System Requirements Specification. The System Safety Requirements Specification is usually developed following the conduct of a Preliminary Hazard Analysis (PHA) and associated risk assessment, which is based upon an early system definition. Safety functions are typically allocated to the hardware and software based upon the System Safety Requirements Specification, the overall design philosophy and the anticipated architecture. Then, Hardware and Software Requirements Specifications, including specific safety requirements for the hardware and software, are typically generated in preparation for the hardware and software development cycles.

Hazards identified in the PHA and other design related analyses help direct the emphasis in the various V&V plans including test plans. It may be necessary to revise the planning documents as development continues and various safety issues/concerns arise.

### **5.3.2 Software Safety V&V Activities**

As discussed earlier, software contains errors that are due primarily to human errors that could occur in the different development phases (i.e., from developing specifications to actual coding). One of the ways of demonstrating that unsafe software errors have been eliminated and safety requirements are met is by conducting software safety verifications and validations at different stages in software development. As noted earlier, it is generally accepted that it is virtually impossible to develop totally error-free software and/or demonstrate that all errors have been eliminated. However, the utilization of appropriate safety V&V activities together with other development related practices (e.g., well-structured software development process, modularity, production of clear and auditable documentation) can help ensure and demonstrate with a high degree of confidence that unsafe errors have been eliminated.

As software V&V implies, there are two major activities that should be conducted: software safety verifications and an overall software safety validation--both are an integral part of software development. Safety verifications should be conducted at the end of various software development phases to demonstrate that safety requirements imposed by the previous phase are met. Each verification activity should be successful (i.e., all safety requirements met including no unsafe errors found) before the next development phase is initiated. A safety validation should be performed at the end of the software development process, and acts as a final check on the software prior to system integration.

Safety V&V, as described here, involves a combination of software related analyses, testing and perhaps simulations and modeling. It is the combination of the various safety V&V activities which demonstrate that the software operates safely under normal operating conditions as well as under certain abnormal input conditions. Potential unsafe operation of

the software due to hardware failures is addressed during the system (**hardware/software**) integration phase of system development--this is described in the System Safety Validation section.

**5.3.2.1 Software Safety Verification** - As described, software safety verifications should be conducted following various development phases (in accordance with a Software Safety Verification Plan) to ensure and demonstrate compliance with software safety related requirements. These should demonstrate that all safety related functions (and not other spurious functions) are correctly and safely performed and demonstrate with a high degree of confidence that unsafe software errors have been eliminated.

Software verifications may be considered as an incremental confidence building activity in ensuring and demonstrating the safety of the software. However, they are considered more than that--they are considered to be a necessary part of ensuring software safety since certain human errors that could result in unsafe software errors may not be found via a check on a final software product. One example is the preparation of an unsafe software requirements specification. This can best be protected against by conducting an intermediate software verification directed **specifically** to ensuring the safety of this specification.

The various software verification activities described below consist of both analyses and testing. Verifications conducted following the requirements specification, design and coding phases are primarily analytical in nature (except for the coding phase which could involve some testing). The module and integration testing activities are also considered to be verification activities, and are described separately following the coding verification activity.

The safety verification activities described in this section are structured around a typical software development process with the following elements:

Software Requirements Specification development – this or a separate specification would typically contain the top-level safety requirements for the software

Software design – could include architectural, high level and low level (module) design

Software coding – development of actual code

Software module testing – testing of individual modules

Software integration testing – testing of integrated modules

**Hardware/Software** integration testing – testing of the software with the actual hardware.

Results of conducting the various software verifications described below should be clearly and accurately documented. The preparation of separate reports for each verification activity is recommended.

It should be noted that software safety may be ensured, in part, by the design philosophy itself (e.g., use of software redundancy--two or more programs written to perform a given function and executed either in parallel or at different times, and/or software diversity--two or more programs intentionally designed to be different in some manner such as by using different algorithms and/or code). If this is the case, safety V&V documentation should include appropriate descriptions of the design philosophy and justifications for why certain verifications are considered unnecessary.

Recommended software safety verifications are described below.

**5.3.2.1.1 Software Safety Requirements Specification Verification** • This activity should be performed to demonstrate that the Software (Safety) Requirements Specification accurately reflects the safety related software requirements in the System Safety Requirements Specification and that human error has not occurred during this translation process. This activity is important because the creation of an unsafe specification (e.g., wrong safety related function to be performed, failure to identify a safety function that should be performed) could adversely affect all remaining software design activities.

In conducting this verification, the Software Safety Requirements Specification (or safety requirements in a Software Requirements Specification) should be reviewed and checked for correctness, completeness, consistency, unambiguity, and proper mapping to the System Safety Requirements Specification. It is recommended that this be done via manual analytical/inspection techniques. Many existing software safety standards provide guidance on conducting a verification of this nature. One example is the RTCA/DO 178B document pertaining to software considerations in airborne systems.

Formal methods, being investigated by numerous organizations worldwide and utilized by some, involve mathematical proofs to demonstrate that errors have been eliminated during the software development process, including the requirements, design and coding phases. This is a relatively new technique, and is not being recommended at this time as the sole technique for this or other verification activities. However, it certainly could supplement other verification efforts conducted on this and further activities. If used, its nature, intent and process should be described and justified.

**5.3.2.1.2 Software Design Verification** - A software design verification should be performed to demonstrate that the design (and design specifications) correctly reflects the safety requirements in the higher-level design related specifications (i.e., Software Safety Requirements Specification) and that human error has not occurred during the design process. This should address the architectural and high level software design as well as the design of the more detailed and lower level software modules. As in the previous activity, concerns

include the design of a incorrect safety related function, failing to design a safety function and/or designing a safety function incorrectly.

The verification is expected to be primarily analytical in nature, and should be directed to such design aspects as logic (e.g., algorithms, control logic, equations), use of data and variables, interfaces between modules and with other system components, real-world constraints (e.g., human interface, timing, throughput) and others. Additional guidance on a verification of this nature can be found in many of the documents reviewed earlier in this program (e.g., RTCA/DO 178B, CENELEC WG A1, and the IEEE V&V and Software Safety Standard).

**5.3.2.1.3 Software Code Verification** - This activity should be performed to demonstrate that the code accurately and safely reflects the design (and design related specifications such as a Software Design Specification) and that human error has not occurred during the actual coding. Again, concerns include coding the wrong safety function, failing to code a safety function and coding a function incorrectly. The code should be demonstrated to be complete, accurate and correct from a safety standpoint.

It is expected that analytical techniques will be the primary method used here. One such method can be referred to as a static code/path analysis. This often involves a control flow analysis (i.e., checking for poor program structure such as having unintended loops), data flow analysis (i.e., deals with the improper use of program data and variables) and boundary value analysis (i.e., checking for errors at parameter limits). Automated tools exist which assist in this type of analysis. Other aspects to check, among others, include timing, interrupts, constants and stack usage. Additional guidance on a verification activity of this nature can be found in many documents, one of which is the RIA Technical Specification No. 23. Table A11 in Tech Spec No. 23 cites some other possible analytical techniques which could be used.

**5.3.2.1.4 Software Module Testing** - Testing should be conducted on each software module to demonstrate that it correctly performs the intended safety functions (and not any unintended functions) and does not operate in an unsafe manner. The testing should be based upon a System Test Plan or even more detailed Software Module Test Specification generated prior to the conduct of V&V. The testing should generally complement the analyses (and especially the code verification analyses) conducted earlier.

Many different testing techniques are possible here. Examples include load testing (i.e., exercising the software via test cases under various load and throughput conditions) and boundary value testing (i.e., checking execution at parameter limits). It is recommended to exercise all safety functions and, if possible, to cover all statements, all branches and loops, timing constraints, numerical accuracy and other safety matters. The use of a testing checklist is highly recommended. A good checklist of this nature is found in Table A12 of the RIA Tech Spec No. 23 document.

Modules can be tested on a simulator or the target machine itself. It should be noted that only software is being tested in this activity--and not the effects of hardware failure on the software.

**5.3.2.1.5 Software Integration Testing** - This testing activity should be conducted to demonstrate that the software modules are integrated properly. It does not involve integration of the software with the hardware--this is done later. The intent here is to progressively combine modules into a composite whole and to ensure a safe interaction between modules. The actual integration procedure may be defined in a Software Integration Plan, prepared as part of normal system development.

Testing of this nature is sometimes referred to as interface testing--described in more detail in the IEC 65A 122 draft software standard. Interfaces should be checked over the expected range of input conditions. Again, the use of a checklist is highly recommended. Table A12 in the RIA Tech Spec document described above provides some additional guidance.

**5.3.2.1.6 Software/Hardware Integration Verification** - The integration of hardware and software, and related verification/validation, is addressed in the System Safety Validation activity.

**5.3.2.2 Software Safety Validation** - An overall software (safety) validation should be performed on the complete software product (in accordance with a Software Safety Validation Plan) to demonstrate compliance with the System Safety Requirements Specification. The main intent of the validation is to demonstrate that the software is "fit for its purpose" from a safety standpoint.

It should be comprised of two main aspects. One is a review of previous software verification activities and results--not necessarily from a management standpoint to see if they were done as planned, but rather, from a technical standpoint to review what was done and what was found. This may have some impact on the validation effort. Another, and the most significant, aspect of software validation is the conduct of testing, and perhaps additional analyses as deemed necessary. However, it is expected that the primary activity is based on testing.

Functional and "black box" testing techniques are recommended here. There should be coverage via test cases of items such as each safety related function with the expected input domain (including boundary values) as well as with abnormal/out-of-range input conditions. The states of the various software outputs should also be exercised. Other safety related aspects related to the System Safety Requirements Specification such as timing and throughput constraints should also be tested. All results should be documented in a Software Safety Validation Report.

**5.3.2.2.1 Compiler Validation** - Any compiler that is used in the software development/V&V process should also be validated (if it has not already been subjected to a validation)--that is, to show that it performs its functions in a safe manner. One possible technique that is sometimes used can be referred to as "reverse translation" or "de-compiling." The technique involves (usually via the use of an automated tool) the conversion/translation of the developed object code back into source code and then a comparison between it and the original source code. This technique is described in more detail in an appendix to the RIA Tech Spec No. 23 document. If the compiler cannot be validated with any high degree of confidence, more emphasis is needed on analyzing and testing the object code itself. Documentation is needed to identify any compiler used and any associated validation information/activities.

### **5.3.3 Hardware Safety V&V Activities**

This section presents the hardware related verification and validation activities to be conducted. However, before describing the specific activities, it is necessary to discuss the different types of hardware that may be utilized in computer-based systems and some specific associated safety requirements that are a part of this safety V&V methodology.

The following general types of hardware are possible in computer systems to help ensure safety:

Hardware circuits designed to be inherently "fail-safe" – have an extremely low (and acceptable) probability of unsafe failure

Hardware circuits based on hardware redundancy and hardware checkers (e.g., comparators, voters) – used to lower (improve) the overall unsafe failure rate of hardware (to an acceptable value) if the failure rates of individual components are unacceptably high; these circuits rely on other hardware to detect unsafe operation and ensure safe states

Hardware circuits that rely, in part, on software to detect unsafe failures and ensure safe states.

It is very likely that any computer-based safety critical system will utilize two or more of the above types of hardware. As will be discussed later, there are general and slightly different safety concerns when dealing with different hardware implementations.

The hardware safety V&V activities described herein are separated, as with software, into two major aspects: safety verifications and a safety validation. The purpose of the safety verifications is to demonstrate that the output of each hardware development phase meets the safety requirements imposed by the previous phase. Safety validation is to demonstrate that the completed hardware (or portions thereof) meets all safety requirements imposed by the System Safety Requirements Specification. Safety requirements will be based, in part, on demonstrating safe normal operation as well as safe operation under conditions of random hardware failure.

All safety critical computer systems rely on the interaction between hardware and software for the implementation of at least some safety critical functions. Also, computer hardware including integrated circuits and microprocessors have unacceptable failure rates from a safety standpoint. Thus, it is usually not possible to demonstrate the safety of all hardware in isolation of the software. Conversely, it is not possible to demonstrate the safety of the software in isolation of the hardware (because the impact of hardware failures on software execution must be determined). For this reason, the hardware verifications and validation described in this section are primarily directed to only a portion of the hardware--hardware that does not rely on software to help ensure safety. Hardware of this nature includes those circuits that have been designed to have an extremely low probability of unsafe failure. It includes circuits that have been designed to be inherently "fail-safe" as well as circuits that utilize hardware redundancy (but which do not rely on software for detection of unsafe failures). The other type of hardware (i.e., that associated with the use of software elements to detect unsafe operation) is addressed in the System Safety Validation activity--which applies after hardware and software are integrated.

As with the software safety V&V activities, the hardware activities discussed in this report pertain to safety related aspects only, and not to overall functionality and performance.

**5.3.3.1 Specific Safety Requirements -** Safety requirements for hardware should include demonstrating safe operation of the hardware under a variety of conditions including 1) normal operation with normal input signals and no hardware failures, 2) random hardware failures with normal input conditions, and 3) external influences including abnormal input conditions, and others as identified earlier in this report (Section 5.2).

The safety requirements relative to random hardware failures can be categorized into two areas: single failures and multiple failures. These are addressed separately below.

**5.3.3.1.1 Single Failures -** The system should be shown to operate safely under conditions of random single component failure. This can be demonstrated in one of two ways using either items 1) and 3), or items 2) and 3) below:

- 1) It must be shown that the unsafe failure rate of the hardware for the system, subsystem or equipment is "extremely low"--i.e., that the hardware is designed in a traditional fail-safe manner (like many discrete hardware circuits have traditionally been designed in the railway industry for many years).
- 2) It must be shown that all potentially unsafe random single hardware component failures are detected "promptly" and the system "promptly" goes to, or remains in, a safe state.
- 3) It "should" be shown that a quantified safety target or goal is achieved. This safety target may be a combination of the unsafe failure rates of associated hardware **and/or** one or more time intervals that relate to the time to detect potentially unsafe failures and ensure safe states. This target helps to quantify

the term "promptly" in item 2) above and "extremely low" in item 1). A safety target could be required by the user, or as discussed earlier, by the FRA. In any case, the safety target should be viewed as a goal--the primary means of demonstrating safety should still be based on qualitative techniques.

It should be noted that the safety target should apply to hardware as well as the combination of hardware and software (in instances where the software helps ensure the safety of the hardware).

**5.3.3.1.2 Multiple Failures** - There are two key requirements for demonstrating safety relative to the occurrence of multiple random hardware failures. One pertains to latent failures and the other to simultaneous failures as follows:

Latent failures – It must be shown that any single hardware failure, which by itself is not unsafe, but which could react in combination with a subsequent failure to cause an unsafe condition, is detected "promptly" and a safe state ensured "promptly." The quantified safety target should also be met in this instance, but should be considered as a goal.

Multiple simultaneous failures – It must be shown that no mechanism exists which could cause simultaneous potentially unsafe hardware failures in two or more system elements in systems in which simultaneous failures could be unsafe. This relates to the need to show independence between these elements as discussed earlier. Internal as well as external influences need to be addressed.

**5.3.3.2 Hardware Safety Verifications** - Hardware safety verifications should be performed at the end of various hardware development phases (in accordance with a Hardware Safety Verification Plan) to demonstrate compliance with hardware safety requirements which served as input to those phases. These requirements relate to the safety functions to be performed including operation of the hardware under different conditions (e.g., single and multiple random hardware failures as described above, and certain external influences).

Hardware V&V activities described below are based upon analyses, testing, and where appropriate, calculations. The activities are structured around a typical hardware development process with the following phases: hardware safety requirements specification development, hardware design and hardware implementation.

Results of the verification activities should be clearly and accurately documented in verification reports.



**5.3.3.2.1 Hardware Safety Requirements Specification Verification** - This activity should be performed to demonstrate that the Hardware (Safety) Requirements Specification accurately reflects the safety related hardware requirements in the System Safety Requirements Specification and that human error has not occurred. The creation of an unsafe hardware safety specification (e.g., wrong safety related function to be performed, failure to identify a safety function that should be performed) could adversely affect all remaining hardware design activities. This activity parallels a similar activity conducted for the software.

In conducting this verification, the safety requirements in the Hardware Safety Requirements Specification (or other appropriate document) should be reviewed and checked for correctness, completeness, consistency, unambiguity, and proper mapping to the System Safety Requirements Specification. It is recommended that this be done via manual analytical/inspection techniques.

**5.3.3.2.2 Hardware Design Verification** - This verification should be performed to demonstrate that the hardware design complies with the safety requirements in the Hardware Safety Requirements Specification. This includes demonstrating safe normal operation (without hardware failures and with normal inputs) via the analyses of hardware electrical schematics, demonstrating safe operation under conditions of random hardware failure as discussed earlier, and under conditions of abnormal inputs.

It should be emphasized that this verification is directed to hardware circuits that do not rely on software to help ensure safety (i.e., to detect unsafe failures). Hardware circuits based on the use of software to help detect unsafe operation and ensure safe states is addressed later in the System Safety Validation activity--after hardware and software have been integrated.

A Failure Modes and Effects Analysis (FMEA) is one technique recommended here to address the effects of single failures. A Fault Tree Analysis (FTA) is another possible technique which is also good for investigating the effects of multiple hardware failures. The analyses should be done on individual circuit boards, where appropriate, as well as on integrated boards to address some interface concerns. The analyses should demonstrate that the safety requirements for hardware failures described earlier are met. This should include demonstrating that no potentially unsafe hardware failures exist in the design, or the unsafe failure rate is "extremely low," or all potentially unsafe failures are "promptly" detected and a safe state ensured. It is highly recommended that a failure mode list be prepared and utilized in this analysis of random hardware failures to identify all failure modes to be considered.

These analyses could expand upon other analyses (e.g., hazard analyses and risk assessments) that may have been conducted to help in making design decisions. These analyses may very likely have included FMEAs as well as an FTA. This verification activity should be performed on the appropriate final hardware design to demonstrate its safety.

There should also be analyses to demonstrate safe operation of this hardware under conditions of various external influences such as abnormal inputs and power supply anomalies.

**5.3.3.2.3 Hardware Implementation Verification** - There should be a hardware implementation verification to demonstrate that the hardware implementation correctly and accurately reflects the hardware design. This activity, done primarily via inspections, should address all system hardware. One could argue that this is more of a quality control matter. However, it is being recommended in this methodology since there are safety implications, and since subsequent **analyses/testing** in the system validation activity may not detect all potentially unsafe implementation errors.

**5.3.3.3 Hardware Validation** - A hardware validation activity should be performed on the hardware that does not rely on software for its safe operation in order to demonstrate compliance with the safety requirements of the System Safety Requirements Specification. This should be done in accordance with a **Hardware Safety Validation Plan**.

The activity should be based primarily on testing, and should have the following objectives:

- To demonstrate proper and normal safe operation--that safety functions are performed correctly
- To supplement earlier analyses of the design as needed (e.g., effect of certain hardware failures)
- To demonstrate safe operation of the subject hardware under expected environmental conditions--most of this testing could be delayed until later (in the system validation activity).

It should be emphasized that this validation activity applies only to the hardware that does not rely on software for its safe operation. This other hardware is addressed in the System Safety Validation activity, after hardware and software have been integrated.

#### **5.3.4 System Safety V&V Activities**

System safety **V&V** activities to be performed are separated into two main parts: system safety verification and system safety validation. The system safety verification activity should be conducted in the early development phases, while system validation should be performed on the integrated system (all hardware and software) after all other activities previously described in this methodology have been conducted.

As with the other **V&V** activities, results of the following activities should be appropriately documented. In addition, all documentation (e.g., plans, processes, results) related to all safety **V&V** activities **conducted** as part of this methodology should be contained in, or referenced by, a single report which provides evidence as to the safety **V&V** effort conducted, results obtained, and the overall safety of the design. A recommended title for this document is "Technical Safety Report."

**5.3.4.1 System Safety Verification** - This verification should be performed very early in system development to demonstrate that the System Safety Requirements Specification accurately reflects the system safety requirements as dictated by the user and intended application of the system. It is done to demonstrate that no human error has occurred during translation of the actual safety requirements into the specification document. Concerns include the specification of incorrect safety requirements **and/or** omission of safety requirements. The specification should be reviewed for **correctness**, completeness, unambiguity, consistency, etc., and should be done according to a System Safety Verification Plan.

**5.3.4.2 System Safety Validation** - An overall system safety validation should be conducted following the integration of all hardware and software, and after all **separate** hardware and software **V&V** activities have been performed. The purpose is to demonstrate that the overall system complies with system safety requirements and is "fit for purpose" from a safety standpoint. The validation should be done in accordance with a System Safety Validation Plan.

The validation activity generally involves 1) a description of how the design ensures safety, 2) a brief review of previous hardware and software safety **V&V activities/results**, and, primarily 3) the conduct of additional analyses, testing and calculations as appropriate. This latter aspect includes an investigation into special systematic safety issues (**e.g.**, other safety concerns not previously addressed by the hardware and software **V&V** activities). The various recommended activities are described below.

It should be noted that the system validation described here is intended to **be** performed on an integrated system (of hardware and software) at the supplier's facility and prior to installation. It is acknowledged that further validation (testing) including on-site customer acceptance testing will also most likely be needed following installation. Such testing would be performed to help demonstrate to the user that the system operates safely and as intended in its operating environment. This "further validation" is not addressed by this safety **V&V** methodology, which is directed primarily to system development activities. However, safety **V&V** activities associated with post-installation modifications of hardware **and/or** software are addressed in a general manner in this methodology (**i.e.**, Section 5.3.5).

**5.3.4.2.1 System Safety Description** - The system validation documentation should include a clear and accurate description of the overall system with emphasis on how and why the design ensures safety. There should be a description of the overall design philosophy, the **hardware/software** architecture, **hardware/software** interactions, safety critical **internal** and **external** interfaces (including any operator interface), and other special features utilized to help ensure safety (**e.g.**, redundancy in hardware **and/or** software, self check features and diagnostics, special **encoding/decoding** techniques). This activity is important since, in many instances, special design techniques are utilized to help ensure **safety**, and they may impact the **verification/validation** efforts carried out. Justification must be provided for any instances in which verification or validation activities were not conducted because of the utilization of special design techniques.

**5.3.4.2.2 V&V Review** - An activity should be performed that involves a review of all safety V&V activities previously conducted and results obtained. The purpose is not to necessarily ensure that all safety V&V activities have been performed (as this is more safety management related), but rather to obtain a clear understanding of what was done and what was found (from a technical standpoint) before additional validation activities are conducted. Earlier results obtained may direct focus to certain portions of the system and may impact additional analyses and tests that are conducted.

**5.3.4.2.3 Hardware/Software Integration Validation** - This activity should be performed to demonstrate the safety of the integrated hardware and software. There are two primary aspects to this effort. One involves **demonstrating** the safety of the hardware portions that were not addressed by the earlier hardware safety V&V activities. This includes the hardware that relies, at least in part, on software to **ensure** safe operation (i.e., detect potentially unsafe failures and ensure safe states are achieved). The other aspect involves demonstrating safe operation of the software (and overall system) under conditions of hardware failure (i.e., impact of hardware failures on software execution). As a reminder, hardware that does not rely on software for safety is addressed in the hardware safety V&V activities discussed earlier.

One portion of this validation activity should be to demonstrate (via analyses and **inspection**) safe operation of the integrated **hardware/software** under normal operating conditions (i.e., proper inputs and no hardware failures).

Another activity should involve the demonstration of safe operation under conditions of random single hardware failure. It should be shown that the applicable safety requirements pertaining to single hardware failure (discussed earlier in **Section 5.3.3.1**) are met. These include the prompt detection of potentially unsafe failures, the prompt ensurance of a safe state following detection, and compliance with a quantified safety target. An FMEA, Software Failures Modes and Effects Analysis (SFMEA) **and/or** other analysis technique should be used to demonstrate the effects of single hardware failures on **other** hardware and on the software. The technique used should also identify the means of detection of the potentially unsafe failure and the means of ensuring a safe state.

There should also be a demonstration of safe operation of the integrated hardware and software under conditions of multiple hardware failures. Again, there are two main areas of concern here: latent and subsequent failures, and simultaneous failures. It should be shown through appropriate analyses that the applicable safety requirements pertaining to multiple hardware failures (described earlier in **Section 5.3.3.1**) are met. In other words, any single failure, which by itself is not unsafe, but could react with a subsequent failure and cause an unsafe condition, must be detected promptly and a safe state promptly ensured. Further, it should be shown that the quantified safety target is met for the system. Similar analysis techniques as described above such as a Fault Tree Analysis or similar technique should be used.

It is also necessary to demonstrate independence **between** two or more system elements (hardware **and/or** software) in which simultaneous failures could be unsafe. Both internal and external influences should be addressed. A common mode failure analysis is one possible technique here.

It should also be demonstrated analytically that the system operates safely (meets all safety requirements) under appropriate conditions of external influence (e.g., **abnormal/** improper inputs, power anomalies). These were described earlier in Section 5.2.

**5.3.4.2.4 Overall System Hazard Analysis.** An analysis should be conducted on the overall system to **demonstrate** that other hazards (in addition to those imposed by hardware **failures** and software errors) do not present unacceptable levels of risk. Hazards of primary interest here are those of a systematic nature – dealing with human error (that have not already been addressed). One example is a possible unsafe condition because of improper human response during operation.

This activity should be based upon a Fault Tree Analysis or similar technique, and could be an expansion of, or revision to, one or more **analyses** that were conducted with the express purpose of impacting the design and making design decisions.

**5.3.4.2.5 Testing -** System testing (under different conditions) is another key activity of system (safety) validation to further demonstrate compliance of the integrated system with safety requirements. Testing should be conducted on the integrated system, and should generally confirm **and/or** supplement earlier analyses and testing activities. Particular areas of interest are as follows:

Normal operation – Demonstrate that safety related system functions are correctly performed and safety requirements met under conditions of normal operation and over the expected range of input conditions.

External influences – Demonstrate that safety related system functions are correctly performed and other safety requirements met under all applicable electrical, **mechanical** and climatic conditions as described earlier and as dictated by the user.

Hardware failure – Demonstrate that safety related system functions are correctly performed and other safety requirements met under conditions of hardware failure. This should generally be conducted in accordance with a System Test Plan and System (Safety) Validation Plan. Certainly, all plausible hardware failures need not be verified by testing. However, the testing should focus on particularly critical portions of the system hardware, and should generally **supplement/confirm** earlier analyses (including the **hardware/software** analyses conducted earlier in this system validation activity). Special attention should be given to failure detection mechanisms. Results of hazard

analyses/risk assessments that were previously conducted to impact design decisions could help direct the testing activity.

### **5.3.5 Safety V&V of Modifications**

Post development modifications are often made to hardware *and/or* software for the purpose of corrections, enhancements or adaptations. Such modifications could be at the requirements, design, or implementation level of hardware or software. It is not only important that a process be in place for **carrying** out the modification, but also that there is a safety V&V process for demonstrating that safety requirements are still met (and safety has not been compromised) following the implementation of the modification.

A safety V&V process should generally be comprised of the following activities:

Determine, justify and describe the impact of the modification on the system, hardware, and/or software operation--This should include determining the nature and extent of the impact including the identification of all affected portions of the system. Consideration should be given to the impact on hardware, software, hardware/software interaction, human interaction, and environmental conditions.

Determine, justify and describe needed safety V&V activities--This should include the identification of what V&V activities are needed (e.g., analyses, regression testing) and to what system portions they should be directed. Needed activities should be related to the activities in the original safety V&V process, since it may be necessary to perform many of the same activities originally conducted. Depending upon the nature and extent of the **modification**, activities may be needed on the entire system or just selected portions. Whatever is determined to be needed must be justified.

Conduct safety reverifications/revalidations--Safety V&V should be conducted on the affected portions as determined above. It should be conducted with the same rigor as the safety V&V conducted during the initial development of the system (assuming that a proper safety V&V effort was performed) relative to such topics as level of expertise, planning, documentation control, independence from the design team and others.

Document approach and results--The approach to conducting the **reverifications/** revalidations should be documented along with all justifications and results.

A process of this nature should be documented, and could be part of a software and hardware maintenance plan. The overall modification process should, of course, be done in accordance with an appropriate quality plan such as the one described earlier in the discussion of Quality Management.

## 5.4 COMPLIANCE ENSURANCE PROCESS

As discussed earlier, it is understood that the FRA is not currently interested in a certification or formal approval process for all new or existing computer-based systems utilized in safety critical applications. Rather, it is understood that the FRA views the safety V&V methodology as a recommended practice which would help establish commonality in the process used to demonstrate safety of such systems and would help to improve existing levels of safety. Further, it is understood that the FRA may wish to **determine/assess** a supplier's compliance with the methodology under certain circumstances such as following an accident or at random on new systems. In such instances, the FRA may wish to determine compliance themselves or with the assistance of a third party organization.

Since the scope of this work pertains to a safety V&V methodology (as opposed to an overall safety assurance process that may include safety and quality development processes and management), the compliance ensurance process described below is directed to safety V&V aspects. Also, the process presented is somewhat general in nature since the safety V&V methodology itself is preliminary at this time and a number of issues need to be resolved before the compliance ensurance process can be finalized. These include the level of detail desired in the methodology itself, the extent to which recommended safety practices are desired beyond safety V&V, and FRA's desired role in the compliance ensurance process.

### 5.4.1 General Compliance **Ensurance** Process

The compliance ensurance process presented here is in the nature of an audit. It outlines a general procedure to follow to determine a supplier's compliance with the safety V&V methodology. It is expected that the process would be comprised of the five activities described below.

**5.4.1.1** Audit Notification - A supplier should be notified of an impending audit, and the following information should be provided in that notification:

What is being conducted, to what system or equipment it is being **directed** to and why (for what purpose)

When and over what period it is being conducted

- Who will conduct it, including roles and responsibilities of parties involved (i.e., FRA, supplier, third party)
- Where it will be conducted (e.g., in-house, elsewhere)

How it will be conducted (i.e., review evidence requested and submitted by supplier and determine compliance with methodology).

**5.4.1.2 Evidence to be Provided** - The type of evidence to be provided by the supplier should be identified. It should generally identify and describe all documentation associated with conducting safety V&V activities on the subject system or equipment. It is expected to include documentation addressing the following:

Design materials and descriptions of how safety is ensured in the design (e.g., design philosophy, hardware/software configuration and interaction, special safety features)

Safety V&V plans describing the overall safety V&V process utilized including activities performed and analysis/testing techniques applied; should include all planning documents related to the system, hardware and software

Results of all safety V&V activities--should show detailed results (e.g., FMEA tables) of analyses, testing and calculations plus summary documents if they exist

All applicable safety requirements for the system, hardware and software.

If the interest goes beyond safety V&V, other evidence could include documentation pertaining to an overall quality process and management (e.g., quality system and plan, structured system, hardware and software development processes), a safety process and management (e.g., safety organization, safety plan, safety reviews), and description/results of other safety related activities (e.g., PHA, other hazard analyses and risk assessments conducted to impact design decisions).

**5.4.1.3 Conduct of Audit** - This includes a review of the evidence/documentation provided (e.g., items listed above). The reviewer should look for deficiencies and areas of noncompliance (e.g., failure to conduct a certain activity, incomplete/improper conduct of an activity, improper safety requirement/criteria utilized, lack of sufficient documentation). This is generally directed to the activities performed, techniques used and results obtained. It is recommended that an audit checklist be utilized during this review--this could be included as part of a more detailed audit process.

**5.4.1.4 Document Findings** - All audit findings should be documented, including what approach was used and what was found. All areas of noncompliance should be identified. Recommendations should be made on how the safety V&V process could be revised/improved in order to better demonstrate safety. These recommendations could be independent of the reason for conducting the audit.

**5.4.1.5 Follow-up Activities** - Follow-up activities to be performed may be dependent, in part, upon the reason for conducting the audit. If a random audit is being conducted on a new system and deficiencies have been identified, a follow-up audit may be desired. If an audit is conducted following an accident, a follow-up audit or other action may still be appropriate.



## 6. TECHNICAL AND ECONOMIC FEASIBILITY

This activity (a combination of Item 4 of the Base and Option Tasks) was directed to the examination and evaluation of the recommended methodology from the point of view of techno-economic feasibility. Three primary feasibility issues were considered:

Will compliance with the proposed standards (methodology) require excessive expense of technical effort on the part of both the manufacturer and the end-user?

- Will compliance with the proposed standards pose undue financial burden on the part of both the manufacturer and end-user?
- Will the requirements imposed by the standards serve to impede rather than promote the advance of new technology?

It must be recognized that the methodology for safety validation under consideration here is preliminary and general in nature. Therefore, the findings resulting from any feasibility review will likewise be general and preliminary. Nevertheless, they can provide insight into the feasibility of imposing and utilizing this methodology, and can serve as a basis for an in-depth examination of the methodology when it is fully developed in the future.

In conducting this activity, the proposed methodology was examined from two basic viewpoints. First, it was examined in terms of its inherent activities and requirements and their potential impact upon the development process for vital railroad equipment and systems. Second, it was examined in terms of the relationship between the activities and process called for, and those presently existing within the railroad industries in both the U.S. and abroad. This was necessary in order to contrast/compare what would be required under the proposed methodology with existing safety assurance processes and practices. or any lack thereof. Following this review and comparison, the feasibility issues are examined and discussed. This is followed by summary and conclusion commentary.

### 6.1 OVERVIEW OF SAFETY VERIFICATION/VALIDATION METHODOLOGIES

The following overviews characterize the basic nature, activities, and requirements of, first, the recommended methodology and, then, U.S. and foreign methodologies as presently utilized for railway related signalling and control systems and equipment. Because of the lack of uniformity in the standards and approaches utilized for safety assurance throughout the world, a single "methodology" is not presently employed either in the U.S. or abroad. Therefore, it is necessary to base the characteristics of the U.S. and foreign methodologies on typical **and/or** composite safety verification/validation activities as currently practiced.

The following description of the recommended methodology (in Section 6.1.1) provides an overview of the methodology presented in Section 5.0, and serves as a major basis for the feasibility review.

### **6.1.1 Recommended Methodology**

The safety validation methodology presented earlier in this report is directed to providing a means by which a technical proof-of-safety can be established for vital computer-based systems and equipment. This methodology is to be applied during, and as an integral part of, the **system/product** development process. Here, technical proof-of-safety denotes validation of the safety of the fully implemented physical system. Since the methodology encompasses the conduct of both verification and validation (**V&V**) activities, it has been denoted as a "safety **V&V** methodology." The **V&V** activities to be performed under this methodology are directed to determining whether or not the resulting equipment complies with associated safety-related requirements. Such compliance is the primary basis for obtaining assurance that a safe design has been realized. While these **V&V** activities, and their results, can provide guidance to the design process, such is not their intended purpose. Rather, they are specifically directed to establishing whether or not the resulting "equipment" will **perform "safely"** when utilized for its intended applications.

The subject safety **V&V** methodology is but one of three interrelated aspects of an overall safety assurance process directed to realizing the development of a safe system and establishing an overall proof that such has been achieved. The other two aspects are denoted as Quality Management and Safety Management. These "management" functions provide the basis for the control and conduct of the various activities essential for the proper design, development, and application of vital railroad systems. It can be expected that, in turn, the overall safety assurance process will be incorporated into a larger system assurance activity that will also address other product assurance issues such as reliability and maintainability.

Quality Management is concerned with ensuring overall product quality via the application of quality-related procedures throughout the development process. A "quality system" is to be established and delineated in a "quality plan;" this plan is to define and **direct** the associated procedures and activities. Several key aspects of Quality Management are: system development process, **software/hardware** development processes, quality audits, configuration management and document control. **V&V** activities, addressing functional as well as safety aspects of the product, are to be integrated into both the system development and **software/hardware** development processes. Activities conducted via quality audits include auditing/confirming that the overall quality procedures, as well as the individual **V&V** activities, have been properly applied throughout the development process.

Safety Management is specifically directed to the elimination and control of hazards resulting from all sources--hardware failures, software errors, operating environment, human errors, etc. It comprises the systematic application of a system safety effort that is to be carried out throughout the system life-cycle. Safety Management as described herein incorporates all safety related activities, including those directed to assisting the design process, as well as those concerned with verifying and validating that safety requirements have been met. Key aspects of Safety Management are: an integrated safety process, safety organization, safety

reviews, hazard tracking, and a definitive safety plan. Safety V&V activities are to be an integral part of the overall safety process and a general description of safety V&V plans and activities are to be included in the safety plan.

The recommended safety V&V methodology defines the general nature, purpose, and activities of a formal process for establishing a technical proof-of-safety for vital computer-based systems and equipment. The basic activities consist of various reviews, analyses, simulations and tests directed to determining whether or not the system meets the associated safety requirements, and, therefore, whether or not it is "safe." These activities are keyed to specific phases and/or milestones within the overall development process. In most instances, the favorable outcome of the conduct of these activities, especially those directed to verification, can be considered as prerequisite to initiation of a subsequent design/development phase.

The proposed methodology entails the conduct of prescribed V&V activities to be conducted throughout the product design/development process, and is structured around five areas of activity: safety V&V planning, software safety V&V, hardware safety V&V, system safety V&V, and hardware/software modification safety V&V. Planning is to be initiated early in the development process and delineates all safety V&V activities to follow; it is keyed to the specific system/product and its associated safety requirements. The results of this activity is to be a set of safety V&V plans which then define and govern the nature and conduct of the remaining areas of activity.

Software safety V&V comprises a series of verification activities conducted throughout the software development process, and a validation activity applied to the complete software product. The safety verification activities are associated with individual phases of the development process and include requirements verification, design verification, code verification, module testing and integration testing. Requirements associated with, and possible approaches to the conduct of, these activities are presented. Software safety validation consists of two aspects--a review of the previously conducted software verification/testing activities and results and, especially, testing and, as appropriate, analysis of the overall software. Validation is directed to ensuring overall compliance with safety requirements. The validation of any compiler used in the software development, or associated V&V activities, is also required. Reports documenting the safety verification and validation process, activities, and results, are required.

As with software safety V&V, hardware safety V&V consists of both verification activities associated with the development process, and a validation activity applied to the resulting hardware. The verification activities relate to the hardware design/development process phases and include safety requirements verification, design verification, and implementation verification. Again, direction is provided relative to related requirements and possible techniques for carrying out verification activities. Hardware safety validation includes a brief review of the verification activities and results, but primarily consists of testing and other analyses. Primary attention is to be directed to hardware circuits that do not interact with, or rely upon, software to perform safety-critical functions. It is noted that this process only "validates" the safety of a portion of the hardware; the part which interacts with the software

is then validated during the subsequent system validation activity. Again, reports documenting the activities and findings are required.

System safety V&V is the final step in the overall safety V&V process for vital computer-based systems under development. It is directed to the complete hardware-software product. System safety V&V comprises a verification activity and a validation activity. The former is to be accomplished in the early stages of the overall system development process and is directed to ensuring that the System Safety Requirements Specification correctly reflects all safety requirements related to the product. Validation of system safety is initiated following integration of the hardware and software. It is directed to demonstrating that the operating system complies with applicable system safety requirements. Validation entails the conduct of a prescribed set of activities. These consist of: generation of a definitive system description (including all safety-related functions and features); conduct of a review of all prior safety V&V activities; conduct of hardware-software integration validation (primarily directed to those portions of the hardware not previously validated); conduct of an overall system hazard analysis (directed to the overall system in the context of its operational environment); conduct of system testing (to confirm safe operation under both normal and abnormal operating conditions). The nature and results of these activities are to be fully documented.

The methodology also addresses safety V&V requirements associated with subsequent modifications to the hardware and/or software of already fully validated products. The specific V&V activities are to be keyed to the specific nature and extent of the subject modifications, and are to relate to the process under which they are developed. Activities should include a determination of impact of the modification on system operation and safety requirements, a V&V plan and justification of the approach selected (to be related to existing V&V materials), and the conduct of specific V&V activities (e.g., analysis) as appropriate to validate the safety of the resulting modified product. All activities are to be fully documented.

In addition to validating the safety of the basic product, an additional V&V process may be required relative to each of its specific applications. Such will occur when an application necessitates reconfiguration or tailoring of the hardware, or the development of application specific software. This can be considered as the development of a "safety case" in support of the basic technical proof-of-safety originally developed. The associated V&V process is to be of the nature described above for product modifications.

### **6.1.2 Present U.S. Practice**

Safety assurance and verification/validation methodologies presently employed in the U.S. are essentially dictated by the railroad equipment and system manufacturers themselves. However, these methodologies also reflect the need for adequate levels of safety and associated proofs-of-safety expressed by the end-users and the railroad industry at large. The following overview of present U.S. practice is based upon the methodologies employed by three major U.S. suppliers--General Railway Signal, Harmon Electronics, and Union Switch

and Signal. Following this, the safety-related practices recommended for use by the AAR/RAC Advanced Train Control System (ATCS) development program are cited.

U.S. suppliers of computer-based vital railroad signaling and control equipment and systems apply an overall system assurance approach to their product design and development process. This approach provides for safety assurance as a distinct, but integral part of the development process. While the specifics of the process employed, and its application, vary from supplier to supplier, there is general consistency among the approaches and activities utilized to realize a safe product; and, to **verify/validate** that such has been achieved.

Product development plans are used to define and govern the development process throughout the life cycle of the product and are directed to providing overall product/system assurance. These plans contain direction as to the **means** to be utilized to assure product safety. Such may be contained in a "product safety program plan" that forms an integral part of the overall development plan. Commonly, specific safety activities (e.g., reviews, analyses, tests) are keyed to specific phases and activities within the development life cycle. The results of these safety activities are used to both assist the design process and to provide a basis for **assuring/verifying** the safeness of the system. Accordingly, product **design/** development and safety assurance progress step-by-step throughout a product's life cycle. Such may continue after a product has been placed in service via the monitoring of system performance **and/or** the in-field modification of equipment. Product modifications, either to the basic product or its in-service applications, are subject to safety review (**analysis/test**) and reverification.

In some instances, safety assurance is partially based upon the use of established design guidelines and techniques that have been developed specifically for vital systems. This approach is commonly directed to the configuration and application of software involved in performing vital functions **and/or** assuring safe operation. However, such usage does not preclude the conduct of specific safety verification and validation activities.

Once product requirements and specifications are established and subjected to preliminary safety review and analysis, the system design is undertaken in accordance with supplier established procedures. As the design progresses it becomes increasingly more detailed as do the associated safety assurance activities. For the most part, these activities are directed to the identification, assessment, and control of hazards associated with both the normally operating system and its failure modes.

It is common practice to develop system hardware and software under concurrent, but mostly separate design efforts. During this process, the **hardware/system** design is generally subjected to formal safety analysis and verification, while the software design is subjected to a review process primarily directed to the elimination of software errors.

In general, safety verification takes place on a design phase basis and serves as one criteria for progressing to the next phase. Validation, which may be referred to as system verification, safety validation, or system validation is applied to prototype or pre-production **equipment/systems** and involves inspection, analysis, **and/or** testing. Safety documentation requirements vary with supplier, but generally consist of the results of those safety specific activities that took place throughout the development process. At least one supplier has

specific proof-of-safety documentation requirements for its software design. This entails a checklist of possible failure types, design techniques and guidelines, and an analyses of how the various techniques were applied so as to safely combat the possible failures associated with the product.

U.S. suppliers all have safety assurance programs consisting of various activities (e.g., reviews, analyses) which are closely integrated with the product design/development process. However, there is a lack of uniformity in the definition and usage of the terms "verification" and "validation." Differences also exist in what is used as documentation constituting overall evidence as proof-of-safety for a product. Nevertheless, each has a defined approach to the process of product safety assurance, and utilize formal techniques and activities to achieve safe products.

**6.1.2.1 ATCS Safety Assurance Methodology** - The safety assurance methodology developed under the ATCS program for the railroad industry's use in designing and developing ATCS equipment is contained in two main specifications. ATCS Specifications 140 and 130 address recommended practices for safety and system assurance and for software quality assurance, respectively. The practices and activities described in the latter, while separate, also support those cited in the former. These specifications support an underlying ATCS program premise that each supplier would ensure and demonstrate the safety of its own equipment including any associated software.

Suppliers' safety assurance activities associated with the design, development, and implementation of ATCS systems and equipment are to be defined and directed by a System Safety Program Plan (SSPP). In turn, this plan is one element of a Systems and Safety Assurance Program Plan (SSAPP) that is to direct the overall product development program. Specification 140 provides guidance as to the nature and content of the SSAPP as well as the SSPP. Materials relative to the SSPP portion discuss safety analysis/testing/activities/techniques that a supplier could apply throughout an ATCS product life cycle to help ensure safety. These are heavily based on those described in MIL-STD-882B, and the supplier is encouraged to select appropriate activities/techniques based upon the specific product and associated railroad safety requirements. These are divided into two main categories: Design and Evaluation Tasks, and Verification and Testing. The former is to be employed concurrently with the product design/development process and includes analyses related to the overall product and its hardware and software. The latter addresses testing/ demonstrations directed to verifying compliance with safety requirements. Testing is also to be used where analysis or inspection cannot show that risk is acceptable.

There are two major testing activities associated with verification: Safety Evaluation and Test and Software Safety Testing. Safety verification testing is to be carried out as part of the design, production, and operation and maintenance life cycle phases. Hardware and software prototypes are to be tested in both laboratory and field environments. Software testing is to focus on testing the lower level units of software, and also includes any software not specifically developed for ATCS usage.

The requirements and process of achieving software quality assurance, as described in ATCS Specification 130, cover the entire software life cycle. A cited goal is to help ensure safety of operations of ATCS computer-based equipment. Therefore, the activities conducted here support the basic safety program thrust of detecting and controlling potentially unsafe conditions by eliminating software defects. The process described in Specification 130 is a tailored version of that contained in DOD-STD-2167A, and suggests activities, products/ documentation, and milestones for various software life cycle phases.

In summary, the concept for system safety assurance put forth by the developers of the ATCS concept essentially parallels that expressed by the U.S. Department of Defense for use by its procurement agencies and their contractors. It is based on the use of a SSPP which defines and directs a safety assurance program and calls for such safety analyses and tests as are considered appropriate for the subject product design/development program. Where software is involved, a separate, but integrated software quality assurance activity is required. This activity is primarily directed to assuring that the software is suitable for the purpose intended and free from errors. The identification and control of product hazards is accomplished via a series of safety analyses conducted throughout the design/development process. Further assurance of safety is then provided by verification and testing activities which take place as a part of specific phases of the product development process. Such activities are applied to both the hardware/system and the software.

### **6.1.3 Present Foreign Practice**

The following overview of safety assurance and validation methodologies presently employed within the foreign railroad industry is based on practices in Western Europe. The methodologies employed by Matra Transport (a French supplier), British Rail (BR) and the German Federal Railway (DB) provide the basis for the overview. Following this, the work in the area of railway signaling verification and validation in progress by CENELEC, an organization associated with the European Community (EC), is cited. The resulting final documents from CENELEC are expected to be released in 1994. In the meanwhile, CENELEC has adopted the existing International Union of Railways (UIC) recommendations regarding safety assessment practices.

As in the U.S., European railway industries apply a broad system assurance approach to the design and development of vital computer-based systems. Likewise, safety assurance is treated as a significant and distinct, but integral, part of the overall product development process. However, there is greater use of a final safety review and approval process prior to the acceptance of such products into operational service. Again, as in the U.S., there is general consistency relative to the approaches, and associated activities, utilized in Europe to realize a safe product. This includes the means employed specifically for safety verification and validation purposes. Because of the political structure, and the major roles played by national railroads, differences in European safety assurance processes primarily occur on a per country basis rather than among individual suppliers or end-users. However, organizations in all countries make some use of safety-related standards developed by international organizations such as UIC and IEC. Such standards are used for providing guidance to safety assurance programs or as a basis for developing their own requirements and standards.

Formal procedures are in place which define the process by which safety verification and validation is to be conducted during a product's development life cycle. Included is the responsibilities/roles of various parties which can include the supplier, the end-user and, possibly, a governmental agency. The activities and resulting documentation associated with verification and validation, as well as overall safety assurance, are generally definitive. However, some of the materials directed to the process are in the nature of guidelines and/or menus permitting selections according to the safety criticality and/or needs of the product.

Commonly, the product design/development process is separated according to hardware and software development, although variations exist. Matra also has a specific set of system/subsystem directed activities which are of an overall and, mostly, preliminary design nature; all direct specific attention to software development. BR utilizes, in part, a Railway Industry Association document (Technical Specification No. 23--"Safety Related Software for Railway Signalling"). The DB utilizes an internal document (Mu 8004--"Principles of Technical Approval for Signalling and Communications"). Mu 8004 provides both general guidelines for designing vital circuits and the application and testing of hardware and software. Maaa employs an internal policy which relies heavily on a proprietary "coded mono-processor" design technique, but also utilizes a formal software development approach along with analysis/testing directed to ensuring error-free software.

Generally, software is subjected to review, analysis, and/or test at various stages of its development, and such constitutes a verification process. In part, software validation relies on the activities and findings associated with verification. However, it also entails additional analysis and testing related to performance and operation in the context of the overall system and its application. Specific levels of validation may be employed and relate to the integrity level (i.e., degree of safety criticality) associated with the product's intended usage.

The design and development of the system concept and associated hardware are usually carried out together, at least initially. Early-on safety reviews and analyses are primarily directed to the identification and correction of hazards. In this regard, they are an aid to the development process. However, these may also serve as a basis for, and as preliminary versions of, verification activities which occur later in the process. As with software, hardware verification occurs primarily on a phase-by-phase basis as the design develops. Hardware validation activities include reviews and both analyses and testing which may be applied to both the hardware alone and in the context of the integrated hardware-software system. Interaction between hardware and software is commonly checked by means of fault insertion techniques. Overall system validation is therefore achieved through verification and validation processes and activities applied to the hardware and software both separately and in combination.

Responsibility for conducting verification and/or validation activities varies according to the individual organization. BR, which both develops its own products and buys from external suppliers, utilizes BR Research (BRR) for this purpose. In the former case, BRR conducts safety verification and validation activities; in the latter, it conducts a review/audit of a fully supported "safety case" provided by the manufacturer. The U.K.'s Railway Inspectorate also audits proofs-of-safety/safety cases presented by manufacturers and end-users. The Bundesbahn Zentralamt (BZA) within the DB interacts with the suppliers during the system



development process. It also performs safety verifications and validations (including some proof-of-safety testing), and approves the equipment for use on the DB. Suppliers must demonstrate compliance with all safety requirements. **Matra** employs a safety plan for each project and this delineates the activities to be performed internally to ensure the safety of the system under development; it also imposes applicable requirements and standards.

Verification and validation activities are conducted throughout the development cycle. These are performed by **Matra's** Hardware and Software **Development** Groups which are supported by the Reliability, Availability, Maintainability, Safety and Security Division. Further, transit projects in France are subjected to review and approval by a Safety Committee composed of representatives of the client, governmental agency and, possibly, independent organizations. The safety of the system is then "defended" by its supplier.

**6.1.3.1 CENELEC Railway Safety Methodology** - There are various organizations based in Europe that provide technical direction to European railway equipment/system suppliers and end-users. These exist at both national and, increasingly, international levels. The latter impacts the railway industry throughout Europe. The European Community (EC) is now actively establishing safety standards (that include verification and validation) for safety related railway equipment and systems utilizing computers. An EC associate organization, CENELEC, is presently developing common safety standards which are reflected in two related documents.

1. WGA1 — 'Railway Application: Software for Railway Control and Railway Protection Systems'
2. WGA2 — "Railway Application: Safety Related Electronic Railway Control and Railway Protection Systems"

The former addresses software, while the latter covers system/hardware related issues. These are to be utilized in combination to provide the basis for system acceptance for use on European railways. Various existing materials were utilized as inputs to CENELEC's work; included were DB's **Mü** 8004 and IEC standards.

It is expected that WGA1 will be similar in content to the IEC software document IEC 65A (Secretariat) 122--"Software for Computers in the Application of Industrial Safety Related Systems." Note that this IEC document is not specific to railroad applications whereas WGA1 is so directed. WGA1 contains requirements for achieving safety integrity of software in computer-based systems. It applies to the development and assessment of software (including safety V&V), and the activities cited therein support some of those cited in companion document WGA2.

Standard WGA1 describes a general process to achieve software integrity that ranges from requirements definition, to development, to validation. Specific attention is directed to the areas of verification, validation, assessment, and quality assurance. Descriptions of various design/assessment techniques are provided as guidance.

Verification is to be carried out, by an independent organization, at various phases of the software development process. It is directed to ensuring correctness and consistency. Validation is utilized (by an independent assessor) to test the integrated system to assure compliance with software requirements. Applicable validation techniques such as simulation/modeling are cited. Software assessment is directed to evaluation of the life cycle processes and products to determine that the software has the proper integrity level for its intended application. This is done via review of all safety related activities and results. The purpose of quality assurance is to identify, monitor, and control all technical and managerial activities necessary to ensure software safety.

Standard WGA2 defines the requirements and conditions which must be satisfied in order for railway control and protection systems to be accepted as "adequately safe" for their intended applications. It applies to the entire life cycle of complete systems as well as individual subsystems. Requirements are levied relative to both the utilization of suitable quality and safety management structures and activities, and to the demonstration of a safe design. Documentation evidence in these areas is to be furnished as a "proof-of-safety" for generic systems and equipment, and as a "safety case" for specific applications thereof.

The overall system quality is to be controlled via an appropriate management process that is to comply with established standards. The quality management organization is to be certified as well. Likewise, a formal safety management process is to be utilized throughout the life cycle. This is to consist of several specific items and activities including a safety organization, formal safety plan, hazard log, safety requirements specification, safety review plan, and a safety verification and validation plan. The latter is directed to ensuring that each life cycle phase satisfies safety requirements established in the previous phase (i.e., verification), and that the resulting system satisfies the original basic safety requirements (i.e., validation).

Considerable attention is directed to defining the evidence required to demonstrate that a safe design has, in fact, been achieved. This evidence is to be provided in a "safety assurance report" containing results of all activities that contribute to showing the design is safe.

In addition to the above activities which are primarily supplier directed and performed, specification WGA2 also requires that an independent "safety assessment" be carried out on the system to provide additional assurance of safety. This may involve conducting additional verification and validation activities. Guidance as to the nature of this assessment is provided. Ultimate acceptance of the subject equipment or system by the end-user (e.g., railway authority) will be based on the supplier's proof-of-safety and/or safety case plus the independent safety assessment.

## **6.2 METHODOLOGY COMPARISON**

The following is directed to a general comparison of the recommended safety V&V methodology with present and proposed safety assurance/validation practices used by U.S. and Western European railroad industries. Its purpose is to highlight principal similarities and differences so as to obtain an indication of the impact that adoption of the "new"

methodology might have upon safety validation as practiced by these industries. No attempt is made to ascertain or compare the effectiveness, relative to the level of safety assurance achieved, associated with the various methodologies.

All comparisons are based on the material contained in the previously presented methodology overviews. It should be noted that these overviews are high-level in nature. Further, those depicting present practices in both the U.S. and Europe are composites of the practices of three separate organizations. The two industry-wide safety assessment/validation methodologies (U.S./Canadian ATCS specifications and the European Community's CENELEC standards) are not yet employed. It should also be noted that the various "methodologies" are not consistent in their structures or use of the terms assurance, verification, and validation. Therefore, those safety validation processes and activities which are explicit in one, may be imbedded in broader safety assurance processes and activities in another. Nevertheless, the methodology overviews provide a general basis for broad comparisons.

### **6.2.1 Comparison with U.S. Practice**

Both present U.S. practice regarding safety assurance and the recommended safety validation methodology are based on the conduct of a formal safety effort as an integral part of the overall product development process. These efforts are directed by system program plans and executed according to specific sub-plans (e.g., verification and validation plans). Likewise, both recognize the unique and significant impact of software on the safety of the product, and direct specific effort to assuring software quality/safety. However, present practice places less emphasis on software verifications as an integral part of the software development process. Further, those software development processes presently employed are generally less formally structured than that which would be required to properly apply the recommended methodology.

The recommended methodology is, by intent, directed to the topic of safety validation, whereas present U.S. methodologies tend to focus on the broader area of product safety assurance. Therefore, less attention is now specifically directed to carrying out safety validation, and generating a proof-of-safety, as a distinct and separate activity. Nevertheless, the realization of a safe product is the primary goal of current safety assurance efforts. Whereas the recommended methodology emphasizes V&V activities directed to confirming that the design/product meets applicable safety requirements, current practice tends to emphasize the broader issue of hazard identification and control. Safety "validation" may then become primarily a matter of showing that all identified hazards have been suitably controlled, and that analysis/testing of the equipment has not revealed any unsafe conditions.

Where "verification" and "validation" are specifically cited under present methodologies, they are usually related to design phases and the overall system/product, respectively. This is in general agreement with the recommended methodology except that, presently, the V&V process is usually less structured, and safety validation per se is commonly directed to the integrated system only. Further, at present, safety validation is usually addressed integrally with system validation in general.

Both present and recommended methodologies recognize the need for safety validation to extend to specific applications of basic products, and to modifications to either the products or their applications. Likewise, the need for documenting safety-related activities and findings is common to both; this includes the ability to provide evidence that safety has been achieved for use **and/or** assessment by the product end-users or others.

The safety assurance methodology proposed for use in the development of ATCS-related equipment is, as is the recommended methodology, intended to be utilized by system suppliers. Both methodologies are to be applied throughout the product **design/development** process. The ATCS methodology is primarily directed to safety assurance, rather than just safety validation, and is somewhat less definitive than that recommended here. It is, in part, an application guideline containing both a general process and suggestions/recommendations relative to its content and application. Both methodologies are applied under the direction of a "system safety program plan:" that for ATCS usage is contained within a larger System and Safety Assurance Plan. The ATCS methodology does not call for the generation or use of a safety **V&V** plan as such.

The ATCS methodology **addresses** both safety activities that support the design process and those that are used to confirm the safety of the resulting design. The latter is covered under "verification and testing" activities and, like the recommended methodology, is directed to **verifying/validating** compliance with safety requirements. There is considerable reliance upon "testing," however, of both hardware and software. Both methodologies place emphasis on the elimination of software defects via a quality assurance effort directed by a structured software development process. ATCS Specification 130 addresses practices for assuring software quality. The recommended methodology is not specific as to software **development** practices, but does presume the use of a formal structured approach (part of a quality system). It places emphasis on software **V&V** requirements which are directed to specific phases of software development.

The ATCS methodology and that recommended here are directed to different aspects of assuring the safety of newly designed/developed products; the former being more general, and the latter emphasizing **V&V**. Therefore, they cannot be compared on a one-for-one basis: however, to the extent their coverage does overlap, they are in general agreement. However, as noted, the recommended methodology is significantly more comprehensive for safety verifications and validations. Accordingly, the recommended methodology can be considered as "generally" compatible with that proposed for ATCS-related product development.

## **6.2.2 Comparison with Foreign Practice**

**Present** Western European system assurance practices include safety assurance, and associated **V&V** activities, as specific and integral aspects of the overall product development process. This is in agreement with the placement and utilization of **V&V** activities as called for under the recommended methodology. However, the European approach more specifically addresses and calls for the conduct of safety activities directed to hazard identification and control; these are often treated as preliminary safety assurance activities. The recommended approach distinguishes between **V&V** activities and hazard control activities and concentrates on the

former. This difference is, in part, attributable to the generally narrower scope of interest associated with the recommended methodology.

Western European methodology, as does that recommended here, approaches overall safety validation through a V&V process that entails the application of selected analysis/testing techniques to hardware and software, both as separately developed and following their integration. Likewise, both methodologies address the significant role of software in designing a safe product, and direct specific attention to the development, verification and validation of error-free software. The European methodologies commonly include, or reference, standard national or international guidelines for developing quality software.

As does the recommended safety validation methodology, the European methodologies call for the generation of V&V documentation that can serve as a primary basis for demonstrating proof-of-safety of the resulting product. Likewise, both require utilization of a V&V process, and generation of associated proofs, for not only the basic product, but for specific applications thereof. This requirement extends to subsequent modifications to the product as well.

Both methodologies are primarily directed to railroad system/equipment suppliers and address safety V&V issues and activities that are to be covered. However, European methodologies call for greater involvement, in validation, by external parties such as end-users and independent "experts." These methodologies also call for the use of a final review/audit of a product's proof-of-safety by an industry or national authority: the recommended methodology is less definitive in this regard.

The CENELEC methodology generally parallels that recommended here in that, it too, directs safety V&V to be carried out as part of an overall safety assurance effort which includes broad quality control and safety management programs as well. Likewise, the safety management program associated with each requires the application of formal system safety techniques. This includes a definitive safety plan and a safety V&V plan that addresses both verification and validation activities as distinct items. Both apply V&V to software, hardware, and the integrated system. However, CENELEC tends to treat the latter two items in a continuous manner rather than as more-or-less distinct entities to be validated separately.

CENELEC's view of software safety V&V is likewise based upon the use of a software development program directed to achieving safety integrity; its methodology includes a separate document devoted to that topic. In this regard, it is somewhat more explicit than is the recommended methodology; however, both are concerned with assuring the quality of the software. The CENELEC requirements for overall product proof-of-safety (and overall safety assurance), and acceptance thereof, are somewhat broader than that of the recommended methodology. While both require the generation of a comprehensive "safety assurance report" as a major part of the overall proof, CENELEC also requires the conduct of an independent "safety assessment." Such may involve additional V&V activities beyond those performed by the supplier.

All-in-all, the CENELEC methodology and that recommended here are in close agreement as to the placement of the safety V&V activity within an overall product safety assurance effort. Further, there is general agreement on the nature of the V&V activities and the documentation required to support a proof-of-safety.

### **6.3 FEASIBILITY REVIEW**

It is necessary to achieve a high degree of safety for new vital computer-based systems, and to be able to demonstrate conclusively that such has been realized. This will foster the development and utilization of these systems, and such is the intent of the recommended safety validation methodology. However, the imposition of this methodology upon the U.S. railroad industry will, as would any new "requirements," impact the overall industry in various ways. If adopted, the methodology would have the status of a "national standard," the use of which would be strongly recommended, if not mandatory. All members of the industry would be affected to various degrees; especially the suppliers since they would be most directly involved in its application and execution.

Adoption of a common safety validation methodology, on a national basis, would provide a definitive and acknowledged basis for demonstrating that new vital computer-based systems are acceptably safe for their intended operational applications. Suppliers and end-users would have a common basis for requiring and conducting safety validations of vital products, and for generating acceptable proofs-of-safety. Further, all related requirements would be well understood by all parties prior to the time a supplier offered a product for acceptance by the end-users. This should facilitate the introduction of new systems into service.

Even if adoption of the recommended methodology provides all the benefits expected and/or desired, the techno-economic feasibility of its usage must be considered. In short, can it be effectively utilized without undue burden on the railroad industry, or excessive negative impact upon the utilization of "new" technology in safety critical applications. Accordingly, technical and economic feasibility issues associated with employing the recommended methodology were reviewed. This was done in terms of three broad topic areas (technical considerations, economic considerations, and technology advancement considerations); these are discussed below.

As was previously stated, the "findings" resulting from this feasibility review are necessarily both general and preliminary since the recommended methodology itself is still of a preliminary nature. Therefore, the following review commentary does not attempt to resolve issues, but rather to promote awareness of them. It will be noted that many of the cited feasibility considerations are of a generic nature not dependent upon the specifics of the methodology. Therefore, they would apply to other, similar, methodologies as well.

### **6.3.1 Technical Considerations**

The basic issue of concern here is – will compliance with the recommended methodology require excessive expense of technical effort on the part of both the suppliers and end-users? The following considerations are applicable.

1. While it is the suppliers who would be faced with the actual application of the V&V techniques, it will be necessary for end-users, and others, to fully comprehend the purpose and technical nature of the individual activities comprising the overall methodology.
2. The individual V&V activities (e.g., reviews, analyses, simulations, tests) called for by the methodology are largely in keeping with those practices currently utilized in the U.S. for supporting system safety programs. Indeed, the safety assurance processes presently utilized by railroad industry suppliers employ many of the V&V techniques cited here. However, it is probable that present usage is not as extensive nor as diverse as called for in the recommended methodology. Its adoption could, therefore, necessitate additional technical effort and expertise although probably not to an "excessive" extent.
3. One major part of the system safety validation activity is based on testing. However, validation by means of testing is an activity that could become both complex and extensive, especially if exhaustive fault insertion is conducted. Further, it may well require the development of lengthy and detailed test plans. Nevertheless, the safety of the integrated system must be validated, and testing, even if difficult, is important and should prove to be manageable.
4. Although a specific quantitative value for an "adequate level of safety" has not been cited in the recommended methodology, the need to conduct a quantitative analysis has been identified. Quantitative analyses require failure rate data for component failure modes and means to ascertain mean-time-between-unsafe-failure (MTBUF) for vital circuits and/or functions. The availability of appropriate failure rate data, and the ability to determine MTBUF in the context of integrated hardware-software configurations, will depend upon the specific design being validated. In any event, some measure of "difficulty" is likely to be experienced in carrying out quantitative analyses.

### **6.3.2 Economic Considerations**

The basic issue of concern here is – will compliance with the recommended methodology pose undue financial burden on the part of both the suppliers and end-users? The following considerations are applicable.

1. There will be various financial costs associated with utilizing the recommended methodology; these will be **incurred** across the entire transit industry. The primary burden will fall to the suppliers since they will be **directly** employing

the methodology in the context of their product design/development processes. However, the end-users will need to acquire expertise in the application of the methodology so they can fully comprehend the suppliers' V&V activities and resulting proofs-of-safety. Further, there may well be a need for methodology "oversight" by "industry associations" and/or "governmental agencies" (e.g., FRA). Such will require both training to provide familiarity with the nature and use of the methodology, and active participation in those activities associated with performing all necessary oversight. These activities will result in some additional costs as well.

2. The extent to which adoption of the recommended methodology will disrupt safety validation, safety assurance, and/or product development processes now in place will vary with the individual supplier. It appears that all U.S. suppliers will need to make revisions to their existing practices in order to fully accommodate utilization of the methodology; in some cases these may prove to be considerable. Validation processes, and associated V&V activities, presently in place will be most directly affected. However, the impact will probably extend into the overall safety assurance area and, in some cases, into the product development process as well. The latter can arise due to the relationship between V&V activities and the hardware, software, and system integration development phases to which they are keyed. The software development process will likely be impacted the most since it can be highly structured and complex.
3. The suppliers' financial costs associated with utilizing the recommended safety validation methodology will be of two basic types: those associated with converting to the use of this methodology, and those associated with its application. The former is essentially a capital cost related to installing the validation process within an existing product development framework. This will entail the development of plans and procedures to affect all necessary changes and/or additions. Also, the possibility exists that additional technical personnel will be required to carry out the V&V activities and existing personnel will require selected training. It is also possible that some amount of additional equipment (e.g., certain software development tools) may be required. The latter is a recurring cost associated with each specific application of the methodology. This may vary somewhat with the complexity of the product being validated, but will be essentially constant. It is not possible to quantify these costs at this time; however, the capital cost will probably be "substantial." The recurring cost can be "significant," but should be viewed as an incremental amount relative to that presently incurred for conducting safety validation activities.



### 6.3.3 Technolow Advancement Considerations

The basic issue of concern here is – will the requirements imposed by the recommended methodology serve to impede rather than promote the advancement of new technology? The following considerations are applicable.

1. Regardless of the technology utilized as the basis for designing/implementing vital railroad systems and equipment, it will be necessary to conclusively demonstrate the safety of these products prior to their introduction into actual service. If, for whatever reasons, the recommended safety validation methodology proves to be unsuitable for application to a given existing technology, several options are possible. First, it may be necessary to prohibit the use of the technology if the methodology cannot be complied with and safety cannot be properly demonstrated. Second, it may be necessary to review the methodology to see if it could be revised in an appropriate manner to accommodate a given technology that was not considered. Third, a formal "waiver process" could be established whereby a supplier could request relief from specific portions of the methodology--this option, however, is not highly recommended.

It should be noted that many of the safety methodologies reviewed in this program, and especially those developed in Europe, address both development and assessment (e.g., safety V&V) aspects, and place restrictions on the use of certain technologies/design philosophies in highly safety critical applications. This matter could be further addressed in a follow-on program that addresses the "bigger picture" of overall system safety assurance and gets more into the design issues themselves.

2. The recommended methodology is directed to vital computer-based/software-driven systems in general, and its use is not confined to a specific type(s) of hardware, software, or system configuration. Further, its adoption should not deter the railroad industry's development and utilization of computer-based systems. However, it must be recognized that the industry is still in the process of exploiting the potential of computers for signalling and control applications, so something essentially novel could be devised. If, in such case, application of the methodology proved to be unfeasible, the options discussed in Item 1 above would be applicable.
3. It can be expected that certain design techniques and/or implementations (both hardware and software) thereof, will be more amenable to the application of the methodology than others. Nevertheless, there is no firm basis to presuppose that, should such differences occur, they alone would constitute sufficient basis for selecting one design/implementation over another. Neither can it be assumed that suppliers would be reluctant to pursue potentially advantageous new technology, solely because of concerns over their ability to validate the resulting products in accordance with the methodology.

## 6.4 CONCLUSIONS

A methodology for validating the safety of vital computer-based systems and equipment has been developed for possible use by the U.S. railroad industry. If eventually adopted as a "national standard," its use could be viewed as a "recommended practice" or could become mandatory. It is expected that availability of a common, industry-approved, safety validation methodology would yield significant benefits. In particular, it would promote the development and utilization of new vital signaling, control, and communication products. Suppliers could have confidence that application of the methodology would assist in the development of safe products, and end-users could be assured that safety was, in fact, achieved if so demonstrated in the associated proofs-of-safety. This situation would facilitate the acceptance of new vital products into service.

Despite the potential benefits, the overall and final feasibility of imposing this methodology on the U.S. railroad industry remains to be determined. The activity conducted here was specifically directed to the examination of techno-economic feasibility considerations. Since the recommended methodology is still in preliminary form, the feasibility review "findings" were necessarily both general and preliminary in nature.

Comparison of the recommended methodology with current practices of U.S. railroad suppliers, relative to safety verification and/or validation, indicates that there are various differences between the processes now employed and that proposed here. These are primarily related to content and placement of the verification/validation function within the larger safety assurance process. In particular, present practice does not appear to utilize the structured software development process, with integrated verification activities, to the extent called for here. Also, the role of safety validation per se vis-a-vis that of hazard control is less distinct in present practice, which tends to combine them. Further, there is presently a lack of uniformity in the documentation provided by individual suppliers as evidence that a given product is "safe." The recommended methodology calls for definitive proof-of-safety documentation.

Even with the differences cited, U.S. suppliers presently perform, as part of their safety assurance processes, many of the individual V&V activities called for by the methodology. This situation suggests that changes to these processes, necessitated by adoption of the methodology, will be centered on management and planning issues as well as on the accommodation and execution of certain specific V&V activities. Therefore, while employing the methodology may prove to be initially disruptive to ongoing practices, no reason which would preclude its use has yet surfaced.

Comparison of the recommended methodology with that proposed for use with the development of ATCS-related products indicates the two are directed to different aspects of overall safety assurance. The ATCS methodology is directed to assuring product safety via the application of hazard identification and control followed by verification testing (more of an overall safety assurance process), while that recommended here is centered on safety verification and validation. The latter methodology considers hazard control activities to be a necessary but separate aspect of the overall safety assurance process. Therefore, while the

two methodologies are by no means "equivalent," neither are they at "odds;" they represent differing approaches and cannot be compared on a one-for-one basis.

Comparison with safety assurance/safety validation methodologies currently employed in Western Europe indicates that, for the most part, the two methodologies are in agreement. This is especially so relative to the "standards" now nearing completion by the European Community's CENELEC associate. As does the recommended methodology, European practice tends to focus on safety verification/validation as a distinct function. European methodologies also provide for end-user participation in product validation and, especially, in formal product acceptance activities. External oversight by independent parties is also utilized, and to a greater extent than now called for in the recommended methodology (although, at the present time, independent oversight of some nature is suggested).

The techno-economic feasibility review, as directed, focused on three topic areas--technical considerations, economic considerations, and technology advancement considerations. It was concluded that:

- The level of technical expertise necessary to conduct the V&V activities required by the recommended methodology is generally in keeping with the present capabilities of U.S. suppliers. In fact, they already conduct many of the cited activities. However, in some cases, additional staff may be required, or present staff trained, particularly in the area of software related verifications and associated testing. The effort relative to validating the integrated system could be difficult depending on system complexity; some degree of ingenuity may be required to accomplish this efficiently. The availability of data and appropriate techniques for carrying out quantitative analyses is an area of concern. However, it is believed that the majority of U.S. suppliers already have or are looking into quantitative analysis procedures.
- The financial cost of utilizing the recommended methodology will largely and directly fall upon the suppliers. These costs will be of two primary types: those associated with restructuring existing safety assurance and product development processes to accommodate new practices, and those related to applying and conducting the actual V&V activities. While no dollar values were developed here, it is expected that these costs, especially the former, will not be insignificant. Details regarding costs can be better developed after issues addressed earlier in this report are resolved and a final methodology is established. Associated with the costs will be some amount of disruption to normal product development activities.
- It is not expected that imposition of the methodology will impede the development of "new" computer-based products. Indeed, the contrary is anticipated. The methodology was devised for application to computer-based systems in general, and its use is not confined to specific designs or implementations. However, the possibility that some presently unforeseen technology, resistant to application of the methodology, will arise must be

considered. Therefore, provisions to accommodate such should be set forth prior to adoption of the methodology.

## **7. TRAINING PROGRAM PLAN**

### **7.1 INTRODUCTION**

The purpose of this Training Program Plan (associated with Item 3 of the Option Task) is to describe the overall training approach and outline the course contents, instructor qualifications, and instructor/trainee training material requirements necessary to train appropriate FRA personnel in the recommended safety verification and validation (V&V) methodology. The primary objective of the course is to educate FRA personnel as to the nature and content of the methodology. A secondary objective is to describe a possible approach to conducting an audit (if desired) in order to ensure compliance with the methodology. The training also provides FRA management with an opportunity to discuss internally their perception of the methodology and how it would be applied.

### **7.2 TRAINING COURSE APPROACH AND CONTENT**

The overall approach to the training course is based on a qualified instructor presenting information (via lectures and appropriate visual materials) relative to the nature, content and expected application of the safety V&V methodology. Supporting the course is the use of an instructor guide, a trainee workbook, and, possibly, examinations. It is understood that different levels of FRA personnel would be trained, which could include inspectors, specialists, and management.

The preliminary training course content is presented as a topic outline in Table 7.1. The content is based primarily on the methodology and compliance assurance process as described in Section 5.0 of this report, and includes additional background material as needed to understand the methodology.

### **7.3 PRESENTATION TECHNIQUES**

A variety of presentation techniques will be used to convey the course contents. These are described on the following pages.

**TABLE 7.1 TRAINING COURSE TOPIC OUTLINE**

Module 1: Introduction

- Purpose of course
- Course schedule and outline
- Course objectives
- Background and purpose of the **FRA** safety verification and validation methodology
- **FRA** role in safety verification and validation
- Basic terminology

Module 2: Overview of System Safety Assurance and Background Concepts

Unit 2.1: Basic Aspects of Overall System Safety Assurance

- Role of quality management
- Role of safety management
- Role of safety verification and validation

Unit 2.2: Quality Management

- Quality process, management, and planning
- System aspects controlled by quality management
- Quality plan
  - Hardware and software quality assurance plans
- Quality audits and other aspects

Unit 2.3: Overall System Development Process

- System development process
- ISO 9001 guidance

Unit 2.4: Hardware and Software Development Processes

- Hardware and software development process
  - ISO 9001 guidance

**TABLE 7.1 TRAINING COURSE TOPIC OUTLINE (cont.)**

**Unit 2.5: Safety Management**

- Overall safety process, management and planning
- System aspects controlled by safety management
- System safety plan
- Safety related specifications
- Role of safety verification and validation
- Safety management organization and reviews

**Unit 2.6: Safety Verification and Validation**

- Definition of safety verification and validation
- Integration of safety verification and validation and system, hardware, and software development processes
- Relationship of safety verification and validation with safety management and quality management

**Unit 2.7: Computer System Safety Concerns**

- Possible computer system **configurations/design** philosophies
- Need for proof of safety during normal operations, failure conditions and **external/internal** influences
- Types of errors and failures (system, hardware and software)
- External and **Internal** influences
- Need to ensure safety after system modifications

**Module 3: FRA Safety Verification and Validation Methodology**

**Unit 3.1: Overall Safety Verification and Validation Approach**

- Definitions of terms related to the methodology
- Safety verification and validation planning
- Software safety verification and validation activities
- Hardware safety verification and validation activities
- System safety verification and validation activities
- System modification safety verification and validation activities
- General documentation/reporting requirements

**TABLE 7.1 TRAINING COURSE TOPIC OUTLINE (cont)**

**Unit 3.2: Safety Verification and Validation Planning Activities**

- System documentation to be used as input
- Planning activities
- Associated planning documentation

**Unit 3.3: Software Safety Verification and Validation Activities**

- Software error types, and related requirements
- General approach to ensuring error-free software
- Software verification and validation process activities and limitations
- Software safety verification process
- Examples of various verification techniques
- Software safety validation process
- Examples of various validation techniques
- Reporting requirements

**Unit 3.4: Hardware Safety Verification and Validation Activities**

- Hardware types
- Types of, and requirements for, hardware failures
- Hardware verification and validation process activities and limitations
- Hardware safety verification process
- Examples of various verification techniques
- Hardware safety validation process
- Examples of various validation techniques
- Reporting requirements

**Unit 3.5: System Safety Verification and Validation Activities**

- Software and hardware integration
- Types of, and requirements for, system failures
- Documents and specifications to be reviewed
- System verification and validation process activities and limitations
- System safety verification process
- Examples of various verification techniques
- System safety validation process
- Examples of various validation techniques
- Reporting requirements



**TABLE 7.1 TRAINING COURSE TOPIC OUTLINE (cont.)**

<p>Unit 3.6: Safety Verification and Validation of Software and Hardware Modifications</p> <ul style="list-style-type: none"><li>• Need to have verification and validation process for modifications</li><li>• Safety verification and validation <b>process/activities</b> for modifications</li><li>• Need to determine impact of modifications on system <b>hardware/software</b></li><li>• Methods to identify aspects of the system to be verified and validated due to the modification</li><li>• Conduct of safety verification and validation</li><li>• Reporting requirements</li></ul> <p>Module 4: Supplier Implementation of Safety Verification and Validation Requirements</p> <ul style="list-style-type: none"><li>• <b>FRA</b> policies and requirements for suppliers implementation of the methodology</li><li>• Supplier implementation expectations</li><li>• Documentation expected from supplier as evidence of the application of the methodology and associated results</li></ul> <p>Module 5: FRA Compliance Ensurance Process</p> <ul style="list-style-type: none"><li>• FRA views of supplier compliance with the methodology</li><li>• Overall audit process</li><li>• Audit notification</li><li>• Evidence and source of the evidence sought</li><li>• Audit procedures</li><li>• Audit reporting requirements</li><li>• Follow-up activities</li></ul>
--

### **7.3.1 Lectures**

The primary mode of presentation will be through lectures. The training content is factual and knowledge based in nature and thus lends itself to lecture rather than any other presentation mode. However, extended lectures can detract from the learning process. Consequently, lectures will need to be short and concise. Further, there will need to be other activities to maintain trainee interest and attention, including class discussions, video tapes, and other visual materials, as appropriate.

### 7.3.2 Discussion Sessions

Instructor and FRA management led discussion sessions will be used to get the trainees active in the learning process. These sessions will be implemented throughout the **training** program to provide variety to the course. Discussion topics could be identified by the instructor, trainees, or other FRA personnel.

### 7.3.3 Video Tapes

There may be video tapes available of interest to the trainees. Although there are no known tapes which directly relate to the safety verification and validation methodology itself, there may be some which deal with specific analytical testing techniques as well as various aspects of conducting an audit. For example, there are tapes on interviewing techniques, dealing with difficult people, etc., which may improve skills used in the auditing process.

### 7.3.4 Demonstration of the Methodology

In complying with the methodology, a supplier would perform various activities including the conduct of various analyses, tests, calculations, etc. to demonstrate safety of the **system/equipment**. So that the trainees can better understand supplier activities with respect to the methodology, the instructor will provide and demonstrate examples of the activities **and/or** techniques that may be encountered.

### 7.3.5 Practice of the Audit Process

During an audit the auditor would need to perform certain activities to obtain and review information. Some of these **activities** would entail reviews of **evidence/documentation** which indicate how the supplier applied the methodology and the results that were obtained. It is recommended as part of the learning process that the trainees review and discuss examples of typical documentation that may be submitted in order to gain experience in evaluating evidence related to application of the methodology.

## 7.4 INSTRUCTOR QUALIFICATIONS

The **instructor(s)** for this training will require a thorough knowledge of the subject matter (e.g., safety V&V, system/software/hardware development). The course content to be taught is somewhat complex, and the methodology itself originates from, and relates to, verification and validation methodologies developed **and/or** utilized by others. In order to convey this material, the **instructor(s)** needs to be knowledgeable of, primarily, the methodology and its application, but also the audit process. Further, the **instructor(s)** needs to be familiar with other relevant methodologies to be able to discuss the basis of the FRA methodology and how it relates to other methodologies.

To ensure a smooth delivery, the instructor will need to rehearse the presentation. This will be done, in part, during a pilot test of the training course.

It is recommended that, as part of the training program, FRA management discuss the methodology from an FRA viewpoint. The FRA presenter will need to receive some training in the basic methodology, its content and recommended audit process. This training can be accomplished through discussions and appropriate documentation. This presenter will need to represent FRA and present FRA's policies related to the methodology, its use and the audit process expectations.

## **7.5 TRAINING MATERIALS**

A variety of training materials need to be developed to organize and present the information.

### **7.5.1 Instructor Guide**

An instructor guide will be prepared in cooperation with the instructor and will be used to help lead the presentation. It will include a plan of instruction consisting of: course objectives, a course outline and schedule, where in the course sequence visual aids are used, and questions for the trainees. The course outline will be based on the training course contents and sequence as presented in Table 7.1. The outline will contain markers which cue the instructor as to which visual aid is to be used at which point. Questions will be included that the instructor can pose to the trainees to assess the learning progress and provide variety to the course.

### **7.5.2 Overheads/Slides**

Overheads and slides will be used to present the training material. They will correlate with the sequence of material in the instructor guide, and will be prepared according to the instructor's wishes and teaching style. Their content will be simple, succinct, and meaningful statements in a style and size to be easily read by everyone in the audience.

### **7.5.3 Student Workbook**

A student workbook will be prepared, and will be used by each trainee to follow along in the course as the instructor presents it. The workbook will belong to the trainee and will contain information that can be referred to at a later date. The workbook will contain:

- Course objectives
- Training course outline and schedule
- Copies of the overheads/slides

- Written explanation of the methodology
- Course evaluation form
- Other pertinent handouts (examples of supplier reports and data, audit forms, sections of relevant documentation)
- Copy of the **audit/inspection** aid (described below).

#### **7.5.4 Training Course Topic Outline and Time Schedule**

A Training Course Topic Outline and Time Schedule will be prepared which contains the basic topics of the course, times presented, and sequence of course contents in order of presentation. The Training Course Topic Outline will be an expansion of the preliminary outline presented in Table 7.1. This outline will provide the student with the complete course contents as well as an advanced look at where the course is headed. Also, a time schedule will be included to temporally structure the course and keep it on schedule. It will further identify beginning and end times, as well as break times.

#### **7.5.5 Audit/Inspection Aid**

To assist appropriate FRA personnel in auditing the application of the methodology by the suppliers, it is recommended that an **audit/inspection** aid be prepared. The aid would essentially be a checklist to help the auditor perform a complete and accurate audit in a systematic manner. The aid would be explained and demonstrated during the training course.

#### **7.5.6 Course Evaluation Form**

It is anticipated that the course would be given more than once to accommodate the need to train other appropriate personnel in the future. Thus, it is desirable for the trainees to evaluate the first course so that improvements can be made. An evaluation form will be developed and distributed at the conclusion of the course. The form will include questions on the quality of the instructor's performance, the course contents, the visual aids used, the workbook and its contents, the training materials used, any testing performed, and provide the opportunity to give suggestions on how to improve the course.

#### **7.5.7 Audit Exercise Materials**

A set of exercises and associated materials will be developed for the trainees to practice parts of the audit process. These materials are expected to be examples of the types of documentation which would indicate applications of the methodology.

## **7.6 EXAMINATIONS**

Examinations are given in technical training courses of this nature for several reasons:

- To motivate the trainees to pay attention
- To measure trainee learning, i.e., how well did the trainee achieve the course objectives
- To indicate where additional training is required
- To measure course success and instructor performance.

It is recognized that the FRA may not desire examinations for their staff, but exams can be given for various reasons, such as those described above. It is, therefore, recommended that testing be included to motivate the trainees and to measure course success and instructor performance. Several possible aspects of testing are described below.

### **7.6.1 Quizzes**

Short quizzes of about 10 questions each could be given frequently throughout the course. Each quiz would cover a meaningful block of material, and would be composed of questions based on the course objectives. They would be scored by the trainees and the answers discussed later.

### **7.6.2 Final Exam**

A final exam would be given at the conclusion of the course. It would cover all the important aspects of the course contents, and would be composed of questions based on the course objectives. These also would be scored by the trainees and the results discussed later. This exam would also be used as an overall indication of course success and instructor performance.

### **7.6.3 Certificate of Achievement**

The training course attendees could each be given a certificate to indicate attendance and successful completion.

## **7.7 COURSE EVALUATION**

The Course Evaluation Form will be completed by the trainees. The comments and suggestions will be used to improve succeeding courses.

## 7.8 LONG-TERM TRAINING NEEDS AND REQUIREMENTS

There are long-term training needs and requirements for training new staff and refresher training of existing staff. To accommodate these needs, a full version of the course may need to be repeated on a periodic or "as needed" basis.

In addition, various changes could occur in the industry as well as in the needs and desires within the FRA. For example, there could be a desire to **revise/expand** the methodology in some nature--perhaps add more detailed requirements pertaining to **verification/validation** or address other aspects (*i.e.*, quality requirements). There could also be revisions desired to the audit process. Thus, it may be necessary to revise the course contents and provide further training as appropriate.

## **8. HUMAN FACTORS ASPECTS**

This section (associated with Item 5 of the Option Task) is concerned with the analysis of human factors aspects of computer-controlled subsystems used in high-speed ground transportation (HSGT) systems. This analysis considers safety-related effects of automation and operator physiologically-related responses in the context of current and near future options (e.g., TGV, ICE, MAGLEV). It should be noted that the current human factors study did not directly impact the development of the safety validation methodology described earlier. Rather, it was conducted as a separate task to address some of the general human factors issues in high-speed applications. Further, this study represented only a small portion of the overall program and was not intended to be a comprehensive study of issues. The current study was more directed toward augmenting and extending considerations of the human and automation related elements addressed in previous efforts (e.g., Sheridan et al., 1993).

This section is divided into the following primary subsections: Introduction, Method, Results, Implications for HSGT Development, Summary of Findings and Conclusions and Reference Sources. Reference sources have been listed separately in this section (from those in Appendix A) because of their extensive and integrative use in the present effort.

### **8.1 INTRODUCTION**

The following two sections respectively provide introductory background and delineate the overall purpose of this human factors study.

#### **8.1.1 Background**

There is now enough experience with high-speed rail service in Europe and Japan to enable one to derive a general picture of the characteristics of such transportation systems (e.g., DOT FRA, 1991a-c; GAO, 1993). In the next few years, no major quantitative jump is to be expected in the characteristics of such systems. Rather, it is likely that there will be a steady evolution towards higher speeds. The only qualitatively different systems would be magnetic levitation (Maglev) transportation systems. These would result in two new characteristics: 1) an increment in speed from about 200-320 km/h to about 450-500 km/h, and 2) certain changes in the engineering characteristics of its guideway (vs. rails) and propulsion systems (Dorer & Hathaway, 1993; GAO, 1993). This study does not explicitly address Maglev systems in detail because many major human factors concerns are already present in current and future rail-based high-speed trains.

This study focuses on high-speed trains similar to the French TGV and the German ICE. More documented than other high-speed systems, these seem to be most relevant to the plans to introduce high-speed rail into the United States. The special characteristics of the Swedish X-2000 and the Italian Pendolino mainly consist in the canting of rolling stock to

accommodate fast travel on curves of small radius (DOD FRA, 1991c). These "tilt-trains" offer no special considerations which cannot be covered by considering the TGV and ICE, aside from additional motion related considerations discussed later in Section 8.3.1.

### **8.1.2 Purpose**

The effort reflected in this study had two goals. The first was to identify physiologically and associated psychologically related elements that can effect HSGT personnel (primarily on-board operator) performance and system safety. The second was to determine automation related elements that can also effect HSGT personnel performance and safety.

## **8.2 METHOD**

The general strategy employed in this study was to address operator physiologically related and automation related elements in a two-phased effort (addressing associated psychologically related elements in both phases). Both phases of the effort, however, were built around a common strategy designed to identify how human limits interact with automation in the context of HSGTs (i.e., a combination of Moray, 1993, and Bittner, 1993). This common approach involved combinations of literature reviews, personal communications with researchers and other "experts" cognizant with relevant issues, and analysis. The specific methods used during the two phases are delineated in the following subsections.

### **8.2.1 Operator Physiologically Related Elements Method**

This review was conducted using a two-step approach involving identification of salient physiological and associated elements expected to interact with automation in the context of HSGTs. First, pertinent literature were identified that contained related reviews or incident analyses concerned with physiological and related elements. Identified in this process were several recent internal reports addressing issues related to automation levels and performance (e.g., Kantowitz & Bittner, 1992; Bitmer, Kantowitz & Bramwell, 1993). Based on an initial review of Sheridan et al. (1993) and our previous involvements with high-speed train issues (e.g., Bittner & Kinghom, 1992), these reports suggested that fatigue and related factors could substantially interact with automation to impact performance and safety. During the second step, "informal" discussions were held with researchers and other experts cognizant with physiologically-related issues in a high-speed train context (e.g., J.C. Guignard, 1994, personal communication). This latter approach, it is noteworthy, informally revealed recent "high-speed train incidents," and also suggested fatigue and related issues. Together the two converged on the following elements being identified for further consideration:

Working Hours and Scheduling – This includes shiftwork and extended (>8hr.) work period effects; and

Perceptual Conflict Effects – This includes the "sopite syndrome" and related effects associated with motion and display conflict inducing situations.



Recent literature reviews addressing aspects of both of these physiologically and psychologically related issues were assembled from university and internal sources (e.g., Lewis, 1985; Kiser et al., 1986; Bittner, Schuller et al., 1994; Bittner, Wiker et al., 1993; Bittner & Kinghorn, 1992). These reviews, findings from personal contacts, and relevant HSGT research provided the basis for the results (in Section 8.3.1) concerning physiological and associated elements related to operator performance.

## **8.2.2 Automation Related Elements Method**

This review was divided into two phases that separately addressed the human factors aspects of HSGT speed and increasing automation. This division was made because of the substantial differences in 1) nature and extent of existing literature for the two areas, 2) mixes of methods selected as most appropriate for addressing their aspects, and 3) difficulties of jointly considering the aspects (given the first two differences). Methods applied to HSGT speed and increasing automation are separately considered below.

**8.2.2.1 Speed Implications Method** • This phase was conducted using a two-step approach involving a quantitative analysis of the performance and safety implications of high speed and an integration of analytic results with previous efforts. First, assuming a cruising speed for an HSGT of 360 km/h, an analytic exploration was progressively made of five elements. These were: permissible deceleration force effects, the implication for operator's vision, the potential emergency responses available to the operator, the demands of normal stopping, and monitoring the state of the track. During this analytic exploration, attempts were made to minimize bias from previous work (e.g., Sheridan et al., 1993). This first step was conducted in the manner of a front-end-analysis, one of the methods used to develop and evaluate system requirements (Bittner, 1993). The second step of the analysis involved the selective integration of the analytic results with previous literature. Augmenting this integration were results of personal communications with specialists cognizant of HSGT issues. The results of this review of the safety implications of HSGT speed (Section 8.3.2) largely retain the character of a front-end-analysis.

**8.2.2.2 Increasing Automation Implications Method** • This phase was conducted using an approach that paralleled that used earlier to identify operator physiologically related elements (in Section 8.2.1). First, pertinent literature was identified that contained reviews or incident analyses concerning the effects of increasing levels of automation on operators. Identified in this process were several recent reports addressing issues related to automation levels and safety (e.g., Kantowitz & Bittner, 1992; Lee & Moray, 1992). Augmenting this identification process were "informal" discussions with experts cognizant of the effects on operators of increasing automation related issues. Together, the two steps converged on eight aspects related to increasing automation. These were: changes in skill requirements, error potential, skill degradation, workload effects, situational awareness, understanding of the automation, mistrust, and psychosocial aspects. Results of the considerations of these increasing automation issues are reported in Section 8.3.3.

## 8.3 RESULTS

The results of addressing operator physiologically related, speed related and increasing automation related aspects are presented in this section. Leading-off is the presentation of the results for the physiological and associated aspects related to operator performance. This is followed by respective presentations of considerations related to implications of speed and increased automation.

### 8.3.1 Physiological and Associated Aspects Related to Operator Performance

This section considers selected physiological and associated psychological elements that can effect operator performance in the context of high-speed automation options. As described earlier, this consideration builds upon reviews of existing literature. Delineated in this section are the results of the review process and associated implications for HSGT safety.

**8.3.1.1 Physiological and Associated Aspects Review Results** - Addressed separately in this subsection are the effects of 1) working hours and scheduling, and 2) perceptual conflicts.

**8.3.1.1.1 Working Hours and Scheduling** - HSGT personnel can be expected to perform under night shiftwork conditions that create several challenges to their internal sleep-wakefulness systems. This is because such internal systems are generally geared to wakefulness during the day and sleep during the night (Bittner, Schuller et al., 1994; Kiser et al., 1986, pp. 275-303; Bittner, Wiker et al., 1993, Chap. 3&6). Sources of stress encountered by crew members under these conditions include:

Disruption of circadian rhythms – These include desynchronizations in the daily fluctuations in physiological functions such as body temperature, heart rate, blood pressure, and hormone excretion (Bittner, Wiker et al, 1993; Bittner, Schuller et al., 1994). Among other effects, desynchronizations result in 1) sleep being disrupted, 2) reduced wakefulness during duty hours, 3) substantial increases in the time it takes to perform routine tasks, as well as 4) increases in general malaise and fatigue. Endo et al. (1980) recognized that such circadian disruptions could reduce HSGT operator performance and system safety (but apparently did not address such disruptions in his study of Shinkansen operator vigilance decrements).

Disruption of sleep – Such disruption can be attributed to both endogenous and exogenous variables. Endogenous variables are often related to circadian rhythms mentioned above. Exogenous variables that affect the ability of late-shift operators to sleep can include daylight entering their sleeping areas, as well as street and other sounds. HSGT personnel, working late-shifts, may also be expected to voluntarily interrupt and substantially limit sleep to socially interact with others (Mahan, Carvalhais, & Queen, 1990; Rosa, Bonnet, & Bootzin, 1990). Disrupted sleep is associated with personnel experiencing

"micro-sleeps," naps, and other vigilance lapses seen in conventional train and other shift workers (Bitmer, Schuller et al., 1994).

Both of these interacting shiftwork effects contribute to fatigue and associated conditions that reduce vigilance and other aspects of operator performance and safety. Extended (>8hr.) duty periods, currently the rule in the U.S. (Lewis, 1985), can only exacerbate fatigue effects from disrupted sleep and circadian desynchronization. The degree to which they do depends upon the shift schedule and the individual (Bittner, Schuller et al., 1994).

**8.3.1.1.2 Perceptual Conflict Effects** - Perceptual conflict effects can be expected to challenge the performance capabilities of HSGT personnel, particularly vehicle operators. Of the many sources of perceptual conflict recently reviewed (Bitmer, Wiker et al., (1993), two appear to offer the potentially greatest challenges:

Vehicle Motion – Several forms of "motion sickness" can result with well-known effects (e.g., sleepiness, fatigue, nausea, and vomiting) when there is exposure to very low frequency (<1 Hz) passive oscillation or perceptually incongruous acceleration (Reason & Brand, 1975; Bitmer, Wiker et al., 1993). Flat or tilted sustained turns can provide provocative accelerative incongruities, particularly when operators rotate and turn their head downward (Bittner & Guignard, 1985; 1988). Nausea and vomiting usually decline with continuing exposure, but chronic fatigue, lassitude, impaired motivation, and difficulty in concentrating may continue indefinitely (Graybiel & Knepton. 1976; Lackner & Graybiel, 1984; Bittner & Guignard, 1985; Bittner et al., 1993). Informal reports indicate that both this "sopite syndrome" and other perceptual conflict effects have been observed in current HSGT operations.

- Visual Display – A variety of evidence indicates that visual display terminals (VDTs) and other sources of visual distortion (e.g., curved windscreen) can lead to effects akin to motion sickness (Bitmer & Guignard, 1985; Morrissey & Bittner, 1990; Bittner, Wiker et al., 1993 ). VDTs, it is pertinent to note, are the basis of primary displays both on-board current HSGTs (e.g., TGV and ICE) and at their dispatch centers. Vibration-induced visual blurring can also lead to motion sickness-like symptoms that could be expected to combine with other sources to increase sickness. Although higher speeds give the opportunity for greater display vibration, neither the levels of such vibration nor their effects on operators have apparently been evaluated aboard HSGTs. VDT and related visual distortion effects are believed to summate with motion effects (e.g., Bittner & Guignard, 1985). The summation of effects is consistent with perceptual conflict theories of motion sickness (Bitmer, Wiker et al., 1993).

Both motion and display perceptual conflict sources clearly can interactively contribute to fatigue and associated conditions to negatively impact vigilance and other safety-related performance aspects. Exacerbating these perceptual conflict effects, however, are the earlier described fatigue and other effects due to working hours and scheduling (Bittner, Wiker et al.,

1993). The HSGT safety implications of the combination of these physiologically-related effects are considered in the following section.

**8.3.1.2 Physiological and Associated Aspects Safety Implications** - The above results indicate that HSGT operators face larger physiologically-related challenges to their vigilance capabilities than standard train operators. Opportunities for perceptual conflict, for example, are increased with both 1) the increased accelerative forces accompanying higher HSGT speeds, and 2) the increased use of VDT-based displays as primary system interfaces. In turn, increased perceptual conflict related fatigue, together with that associated with working hours and scheduling, would lead to less operator vigilance than on standard trains. Compounding this is a further potential automation related vigilance decrement associated with reductions in operator role and system involvement (as delineated later in Sections 8.3.3.4 and 8.3.3.5).

These potentially compounded physiological and automation related vigilance decrements are particularly disturbing. This is because, arguably, even standard train operators currently experience a loss of vigilance. They, for example, have self reported 11% nightly on-the-job napping and their EEG data suggest more like a 20% rate (Akerstedt, 1988; Bittner, Schuller et al., 1994). The present results consequently point to the need to evaluate physiologically related elements of HSGT operations with regard to their vigilance and safety effects. Unfortunately, this evaluation cannot be addressed in a non-experimental study as only general guidelines currently exist (e.g., Bittner & Guignard, 1985; Bittner, Wiker et al., 1993). HSGT designs consequently need to be experimentally evaluated with regard to the physiological and associated elements described herein.

### **8.3.2 Implications of HSGT Speed**

The most salient characteristic of HSGTs is their speed from which a broad range of other considerations analytically follow. Related to speed are the following: permissible deceleration force effects, the implication for operator's vision, the potential emergency responses available to the operator, the demands of normal stopping, and monitoring the state of the track. Each of these becomes more pronounced as the speed of the train increases. At lower speeds, characteristic of standard trains, many of these concerns are negligible. but at high speeds they increasingly pose significant human factors and safety challenges. For this discussion, we assume a cruising speed for an HSGT of 360 km/h. This assumption has two benefits. First, 360 km/h equates to 100 m/sec and so is convenient for calculations. Second, current HSGTs (e.g., TGV and ICE) cruise at speeds from 200-320 km/h and so 360 km/h represents a reasonable projection of near future HSGT speeds (GAO, 1993). Sheridan et al. (1993, pp. 4-10 to 4-15) presents a separately derived list of HSGT speed implications that partially parallels and is augmented by the following considerations.

**8.3.2.1 Deceleration Forces** - The stopping distance from 360 km/h in an emergency appears, from the literature, to be about 3.5 km (e.g., Sheridan et al., 1993). Normal (non-emergency) braking can be expected to increase this by a factor of about 3. These distances and their associated times are associated with deceleration forces of between 0.25 g and

0.05 g, where g is gravitational acceleration. These forces (0.05 g to 0.25 g) should be acceptable to passengers on the basis of automobile studies, where unacceptable deceleration occurs at about 0.5 g (Bittner & Kinghorn, 1992). At 0.25 g, the only question is whether the drivers should be "strapped in" using a safety harness to prevent them from being flung against the console with the danger of inadvertent activation of controls. Such activations may not be a problem in emergency stops during which many controls may be temporally deactivated, but the potential cannot be generally ruled out from existing documentation (e.g., DOD FRA, 1991a-c; Sheridan et al., 1993). Safety harnesses would be recommended based upon the potential for inadvertent activations during both non-emergency and emergency stops.

Higher decelerations might be physically possible for Maglev vehicles, but it is not likely that they would readily, if at all, be tolerated by passengers. The sudden application of, say, 0.5 g, would lead to considerable injury to passengers, and their baggage and belongings could become projectiles. The deceleration on rail-based HSGTs is limited by the characteristics of regenerative electric braking, the frictional heat which must be dissipated, and the limits at which steel wheel to steel rail adhesion allows skidding. Even with anti-skid brakes, the current values of deceleration seem to be close to the limit of what is practical.

**8.3.2.2 Implication for Operator's Vision** - There are several implications for visual perception of on-board operators that can be drawn from literature *and/or* analytic considerations.

- Little or no information can be picked up visually from wayside signals at 360 km/h, if DOT FRA (1991b) is correct. It follows from this that all status information about the state of the HSGT system will have to be displayed at the on-board operator's console. This is the case on higher speed HSGTs (Sheridan et al., 1993).

HSGT operators cannot rely on vision to make decisions to stop the train because of obstacles on the track. If it takes 3.5 km to bring the train to halt from cruising speed, then even a 6 meter high by 6 meter wide object would subtend only about 4' by 4' of arc of visual angle. It is absolutely impossible for drivers to perceive the nature of an object of that size, or to decide whether it is on the track or merely close to the track (See Endo et al., 1980, for a supporting incident report). It is equally impossible for them to decide perceptually whether the object is a train, and if so, whether it is on the same track or an immediately adjacent track. Even if the object displays a brilliant light, its lateral position with respect to the HSGT operator's track cannot be judged. It is consequently impossible for HSGT operators to make decisions to activate the emergency braking system in time to prevent a collision based on unaided vision.

- It will be absolutely impossible for an HSGT operator's unaided vision to detect any objects which have been placed on the track in acts of vandalism or sabotage in time to avoid them (based on above arguments).

**8.3.2.3 Emergency Response** - It follows directly from the previous section that automation must augment drivers' perception in the control of HSGTs. The nature of control will be supervisory control (Sheridan, 1987). and not manual control, at least with respect to emergency stopping. Some of the work on automobile driver behavior is relevant here. Back in the 1950's, Crawford, at the British Road Research Laboratory. investigated overtaking behavior in a series of studies. He showed that car drivers increasingly delayed **making** a decision as it became harder for them to decide whether the distance to an oncoming car was sufficient for an "overtaking maneuver." This can be seen as a case of speed-accuracy **tradeoff** (although in this case it was necessary to make a rapid decision if they were to overtake at all). Alternately, it can be seen as related to the information-theory notion that, the lower the signal-to-noise ratio, the greater the time required to make a decision. Either way, one can expect that the extreme difficulties of judgments at long visual ranges will lead to delayed decisions, and hence, to a lowered ability to stop in time (should the need arise).

The concern, then, should not be with designing a HSGT operator's station to **support** "reaction time<sup>n</sup>-like responses to perceived danger. Rather, the concern should be toward designing an operator's station which supports rapid decision **making** and providing state diagnosis when alarms are activated or when displayed information identifies abnormal status (which has not yet triggered any automatic system responses).

**8.3.2.4 Normal Stopping** - The documents on Maglev systems (e.g., Dorer, & Hathaway, 1991) indicate that it is important for an elevated guideway train to stop only at designated locations, and not to undershoot or overshoot stations. This is not quite as important for a rail-based HSGT at ground level, where in the event of a disabled train, passengers may more easily descend to the track side. However, it is certainly undesirable for a train to overshoot a platform at high speed, since this implies an **unexpected** passage of the train past passengers who are expecting it to stop. Additionally, passengers may be hurt either by contact with the train or by being buffeted by the wind pressure. Hence, it is important that deceleration be started at an appropriate time and distance, and that operators be able to monitor whether deceleration is proceeding at a rate which will bring the train into the platform at the specified speed. Here again, it will not be possible for drivers to estimate distance by direct perception, unless special signals are provided. The argument for displaying the information on board is very strong in view of the lack of visual perception of trackside information (DOT FRA, 1991b).

**8.3.2.5 Monitoring Track State** - It is obvious that it will not be possible for drivers to visually detect such conditions as icing, incorrect setting of switches, etc. Current practice then assumes that information about the relation of the train to other objects in the system is provided to the train from some form of external communication channel (e.g., radio or induction loops). One must assume that there will inevitably be times when **abnormal** situations arise which cannot be detected by the external and central sensing systems and transmitted to the cab. It seems likely that this will be particularly true in the U.S., where there tends to be much more vandalism and individualistic behavior than in Europe. Hence, it is expected that there will be a far greater likelihood of attempts to gain right-of-way entry for purposes of crossing the line at illegal places, or for purposes of vandalism, than in Europe. There is also the possibility, however unlikely, that a maintenance vehicle or other

train will somehow be on the track and go undetected. Because of the severe consequences of a high speed crash (e.g., Sheridan et al., 1993), we may ask whether there are onboard-sensor technologies available to assist operators in detecting objects approximately 3.5 km ahead. Three possibilities suggest themselves as technological extensions to supplement information received from off-board communications systems.

Radar – This type of ranging is more than able to pick up hard objects at ranges of several kilometers. However, there would be very great ground clutter and backscatter from the ties, catenary poles, bridges, telephone poles, etc. There may also be interference from high frequency electrical equipment and from the power in the catenary. It is an engineering question whether these disadvantages could be overcome. A suggestion in this regard is made below.

Laser ranging devices – It is possible that laser ranging might be an alternative. Again there would be many echoes (from bridges, poles, etc.) that would clutter the display, and care would have to be taken to ensure that laser energy could not injure someone in its path (e.g., their eyes). The most likely case for the latter problem would be when a train was traversing a curve, and a fixed laser would be pointing tangentially outward beyond the right-of-way. This suggests that the laser ranging device should track the curve and point on a chord inside the curve, so that it can pick up objects where the train will be when it has rounded the curve. In that case, the danger would be to people on the inside of the curve but beyond the right-of-way. This may not be a severe problem, however, given the very shallow long-radius curves ultimately proposed for HSGTs (GAO, 1993).

Possible technological developments – It may well be that sufficiently accurate radar and laser devices exist in the military and could be converted to use on HSGTs. Any such device should track on the inside of curves, looking along a chord, and not a tangent. It may be possible to declutter signal return information by using a Global Positioning System (GPS). Because GPS would allow the system to locate the train to within a few meters, a data bank could store echoes expected when looking in the programmed direction from each location. That data could be subtracted electronically from the returning echoes, and hence, any remaining data displayed could constitute a possible obstacle. The use of such a system would have the added advantage that it would provide a meaningful supplementary task for the drivers, so that the danger of a loss of vigilance would be reduced.

### **8.3.3 Implications of Increased Automation**

A number of safety-related issues will be increasingly important with increases in the levels of automation. These issues include: changes in skill requirements, error potential, skill degradation, workload effects, situational awareness, understanding of the automation,

mistrust, and psychosocial aspects. These are separately considered in the following discussions.

**8.3.3.1 Changes in Skill Requirements** - Automation and other increases in technology shift the content of jobs so that they require different skills. Often these additional skills require increased cognitive involvement (and capabilities). Through a series of field studies, Zuboff (1988) discovered numerous situations where advanced automation and display technology change job requirements. Specifically, he found that such technology changes required: 1) more abstract thinking, and 2) the **need/ability** to supervise and monitor automation, rather than interacting with the process directly. Automation consequently tends to shift involvement from physical activity and direct contact with the system to increased intellectual activity through a computer interface. This tendency toward increased intellectual activity through an interface has been repeatedly indicated by HSGT researchers (Endo et al., 1980; Sheridan et al., 1993).

Interacting with a system through a computer intermediary often requires operators to learn new skills and procedures, without which system operation may be difficult or even dangerous. For example, flight management systems (FMS) automate much of what aircraft pilots previously executed manually, such as course changes, holding patterns, climbs and descents. This new technology forces pilots to develop skills for interacting with this complex automation that were previously unrelated to flying the aircraft. Curry (1985) and Sarter (1991) used surveys to show that pilots have not been entirely successful in acquiring these skills. The surveys showed more than 50% of the high time pilots (more than 1,200 hours of FMS experience) report that they did not completely understand the automation and that the automation sometimes "surprised them." Supporting this finding, Bittner, Kantowitz and Bramwell (1993) have found several types of increased hazards directly related to lack of understanding of increased automation. These results illustrate that increasingly complex automation may introduce new skill and knowledge requirements that operators may not currently possess, and may entail significant training to acquire. With regard to HSGTs, Sheridan et al. (1993) have pointed out that current ICE and TGV practices both differ in operator selection. Though both draw from the most experienced operators, ICE requirements emphasize in-depth technical knowledge of the locomotive and all levels of its operation. TGV selection, in contrast, is based on measurements of psychomotor or cognitive aptitudes and personality variables. Based upon experience in other domains (Bittner, Kantowitz & Bramwell, 1993), the TGV selection emphasis appears most likely to result in selection of operators with the capabilities to meet the increased requirements of HSGTs.

Sheridan et al. (1993) have also pointed out that ICE and TGV philosophies differ on the operator training conducted after selection. ICE apparently uses two types of training facilities: 1) a "cutaway" of real equipment that is used for training on the dynamic response of some system aspects (e.g., electrical response to control input), and 2) desk-top simulations on personal computers to train operators as to required responses to, e.g., in-cab and external signals. TGV, in contrast, apparently uses a "sophisticated moving-base simulator with high-fidelity computer-generated out-the-window views." Before commenting on their differences, it is useful to consider the additional skills that automation requires. These additional skills stem from three sources:



Complexity of the task and the multitude of the functions available – These may impose a significant burden on operators.

- Design of the automation interface – This may require specific knowledge to operate and inhibit operators' understanding of the system. For example, Saner and Woods (1991a) report that pilot expertise with the FMS was inhibited by the opaque interface through which operators were forced to operate. Specifically, the system provided poor feedback concerning the current mode and activity of the system (Kantowitz & Bittner, 1992 identifies errors due to such opaqueness).

Supervisory controller requirements – This is the result of the shift of operators from active participants in the process toward supervisory controllers (Sheridan, 1987; Sheridan & Hennessy, 1984).

With regard to the "complexity of task and functions," successive 'part-task' use of ICE-type equipment cutaways and desk-top simulations appear most appropriate for introducing operators to HSGT control. In turn, to accommodate the "design of the automation interface," ICE-type desk-top simulations would appear most appropriate. Of note, together with training on the "philosophy" used in FMS design, this desk-top simulator approach was recently recommended as a means of addressing the opaqueness of the FMS (Bittner, Kantowitz & Bramwell, 1993). Finally, with regard to "supervisory controller requirements," ICE-type desk-top simulations might be initially used (if they provided the comprehensiveness seen in some PC-based flight simulators). However, the TGV-type sophisticated simulator would be most appropriate for final stages of such training because of its fidelity. Thus, the means for training to meet changes in skill requirements appears to be represented in a combination of current ICE and TGV approaches. This combined approach to HSGT operator training remains to be fully developed and evaluated with regard to its performance and safety enhancement effectiveness.

In summary, the supervisory **controller** role demands use of new skills by the HSGT operator to ensure adequate performance and safety. These are related to monitoring information flows, intervening to compensate for the limits of the automation, and setting the parameters that govern automation. Approaches for selecting and training operators in these new skill requirements have been identified from existing literature. Evaluations of the precise extent of changes in the skill requirements for HSGTs operators and means for addressing these changes through selection and training remain to be conducted.

**8.3.3.2 Error Potential** - Technology has often been introduced to eliminate human error. However, humans still interact with the system and in many cases automation results in new, and potentially more disastrous errors. Eliminating such automation errors, it is pertinent to note, may inherently not be achievable in automated transportation and other systems (Littlewood & Strigini, 1992). Inevitably, because automation often increases the operator's sphere of influence by integrating the control of many components that were once independent, it can act to amplify errors, making their consequences more severe than in a manual system. In the realm of process control, relevantly akin to HSGT, Bainbridge (1987)

identified what is called "ironies of automation." One irony lies in the realization that as systems become more automated, the contribution of the human becomes more crucial because humans are left to control situations that the automation cannot. Likewise, human errors often become more critical as a consequence of systems becoming more automated.

Not only are the effects of human errors often magnified by highly automated systems, but automation introduces new types of errors that did not exist in less automated systems. Sarter and Woods (1992) identify numerous instances of mode errors with flight management systems. In these highly complex systems, the large number of operating modes makes it possible for the same action to be correct in some instances and incorrect in others. For example, a pilot may engage the CLIMB MODE to direct the plane to a cruising altitude. When the plane reaches the specified altitude, the automation reverts to the ALTITUDE HOLD MODE. Transitions between these modes change the meanings of operator actions. In one mode a set of actions may be perfectly acceptable, but in another mode those same actions may produce disastrous results. Thus, the transition between modes provides new opportunities for human error and has led to inadvertent deviations from desired altitudes and airspeeds, as well as accidents.

This potential for error suggests that a careful evolutionary approach be used in the automation of HSGTs. One evolutionary approach, it is noteworthy, has been proposed by Sheridan et al. (1993, p. 6-2). Specifically, they have suggested an approach that "begins with full control by a human driver who observes 'optimal control' advice, later progresses to driver discretionary use of automatic control, and perhaps eventually evolves to full automatic control with driver monitoring and override." There may be some flaws, however, in this approach. For example, there are a number of high-speed situations where automated control is required for safe HSGT operation (see Section 8.3.2.2). These situations consequently need to be automated to the extent required to provide safe operation. Given this, the most appropriate evolutionary approach might start with giving full control to an operator of all functions not requiring automation for safety. This "balanced" evolutionary approach to automation of HSGTs would seem appropriate given the question of automation reliability (Littlewood & Strigini, 1992).

**8.3.3.3 Skill Degradation** - In some instances automation eliminates low-level control tasks, and in others it radically changes control strategies and information sources. In such situations, manual skills deteriorate and leave personnel ill-prepared to 1) intervene when the automation fails (a primary operator purpose), or 2) perform their functions if they are required to operate a less sophisticated system (as could happen if operators were required to move from HSGTs back to standard trains). For example, Curry (1985) documents situations where pilots of highly automated aircraft lost flight skills when they relied upon automation. For example, skill losses in co-pilots of highly automated wide-body jets were made apparent when they became captains of less sophisticated narrow-body jets. To avoid this skill loss, pilots learned to disengage the autopilot and control the wide-body aircraft manually prior to transition training to the narrow-body aircraft. Wiener and Curry (1980) suggest that well-learned manual skills will be particularly affected by increased automation. The impacts of skill degradations has apparently not been explored in the context of current HSGTs. Based upon aircraft experience, however, it is suspected that skill degradations could significantly

impact HSGT operator ability to safely intervene during automation failures. Selective disengagement of HSGT features could provide one means for off-setting such skill degradations if implemented in the design and operation of HSGTs.

**8.3.3.4 Workload Effects** - Increased automation can have several negative effects on workload (Bittner, Kantowitz & Bramwell, 1992). At one extreme, advanced technology may eliminate many tasks, leaving the operator with nothing to do but to monitor the automation. This "underload" situation may leave operators disconnected from the system, and their low level of involvement may lead them to ignore dangerous situations. Underload can consequently compound the physiologically-related fatigue and vigilance decrements such as discussed earlier (in Section 8.3.1.2). At the other extreme, poorly designed automation may actually increase workload, which is especially critical during periods of abnormally high workload. Endo et al. (1980) evaluated Shinkansen operator workload using psycho-physiological measures (e.g., heart rate). Though aware of shiftwork effects, their study did not directly address the compounding effects of physiologically-related fatigue and vigilance decrements. The combined effects of physiologically related fatigue and automation related workload effects could have large impacts on HSGT safety as noted earlier. Considered in the following are aspects of automation related workload and its control.

Woods, Potter, Johannesen, and Holloway (1991) have identified several ways in which "clumsy" automation has increased workload during high workload periods and lowered it during workload troughs. For example, Cook et al. (1991), investigating a new monitoring and information management system to support cardiac surgery, found it often made tasks more difficult than the older system it was meant to replace. This was especially true of high workload periods where good performance is crucial. Cook et al. (1991) used two prime indicators of clumsy automation (i.e., system tailoring and task tailoring) and a process (i.e., process tracing) that could be applied to HSGTs.

System and task tailoring involve changes that operators make to maintain safe performance. System tailoring, in particular, consists of modifications or reconfigurations that users perform so that the system will be able to support their needs. Task tailoring describes how users change activities to circumvent equipment design errors to maintain critical functions with a minimum workload. Ideally, system design should not force either system or task tailoring. Poorly designed or clumsy automation promotes system and task tailoring which lead to increased workload during critical periods. Observation of task and system tailoring must occur as it develops (at the introduction of automation), otherwise skillful adaptation to poorly designed systems will mask designer errors. In addition to "tailoring," process tracing (detailed observation and analysis of users' behavior) can identify critical information processing and cognitive strategies that well-designed automation should support. Process tracing should be applied as part of the HSGT design and evaluation process to ensure well-designed interfaces and balanced workload.

In summary, HSGT automation-related workload effects can have serious impacts on operator performance and safety. Physiologically related fatigue and associated vigilance decrements can compound automation related workload effects. Process tracing 1) offers one means of

ensuring well-designed HSGT interfaces with balance workload, and 2) should be applied as part of the HSGT design and evaluation process.

**8.3.3.5 Situation Awareness** - Operators often are distanced from their systems as automation supplants their observation and control, leading to failures to recognize critical circumstances and act accordingly. Psychologists have coined the term "situational awareness," which has received considerable attention recently (e.g., Endsley, 1988). In advanced flight decks, a negative effect of automation is a reduction of situation awareness and a consequent degrading of aircraft safety (e.g., Bittner, Kantowitz & Bramwell, 1993). As a new psychological construct, a thorough understanding of the phenomena has not been developed. In fact, Sarter and Woods (1991b, pg. 45) question whether "... situation awareness really denotes a distinct psychological concept or only illustrates the tendency of applied cognitive science to coin new terminology in the face of ill-understood issues." In response to this confusion, Sarter and Woods developed their own definition of situation awareness. This definition states that situation awareness consists of the accessible knowledge (based upon the results of recurrent situation assessments) that can be integrated into a coherent picture, that when required, can be used to assess and cope with the situation. This definition is consistent with that used by Sheridan et al. (1993, p. 3-3). Sheridan et al.'s assumption that the operator's situation awareness is always available when required is basic to their function analysis for driving a high-speed train (p.3-3ff.). Understanding how the design parameters of automation influence situation awareness is consequently a critical factor in enhancing the safety of HSGTs. However, a thorough understanding of such influence remains to be developed.

**8.3.3.6 Understanding of Automation** - Failing to understand the capabilities of automation can lead to inefficient interactions and increased potential for misuse. These effects can, in turn, threaten system performance and safety. Roth, Bennett, and Woods (1987) describe how a design philosophy that treats automation as an alternative to human frailties (a prosthesis) inhibits user interaction with the system, leaving the human with a poor understanding of the capabilities and limits of the system. Such poor understandings, it should be noted, can generally not be completely addressed through operator selection and training. In field studies with power plant maintenance workers, Roth et al. (1987) used verbal protocol analysis (VPA) to show how an automated troubleshooting aid, designed using the prosthesis philosophy, failed to adequately support workers. For example, if the aid was off-track in its diagnosis of the system, the operator had to infer the machine's intentions and redirect its investigation to a more productive path. This burden fell on the human with no support from the machine (Roth et al., 1987). Bittner, Kantowitz, and Bramwell (1993) have reported similar instances where increased aircraft automation was accompanied with less understanding and a consequent increase in unsafe incidents. An alternate design philosophy treats technology as a tool, extending rather than replacing human capabilities. Roth et al. (1987) and Woods (1986) suggest that by using a tool-approach to the design of automation can alleviate the need to infer the intentions of the automation and lead to a much more fluent and effective interaction between humans and automation. Use of the tool approach for the design of HSGT interfaces offers one means for avoiding the automation understanding problems seen in aviation and process control systems.

The difference between tool and prosthesis design philosophies is only one dimension that leads to poor understanding of automation. Through surveys, Wiener (1989) and Sarter and Woods (1991a) showed that even after substantial experience with the advanced FMS, its behavior still surprised pilots. In addition to implications for training (as discussed earlier), these findings have implications for both the design of automation and the training that should accompany its introduction. Specifically, Sarter and Woods (1991a) argue that system opaqueness (also touched on in 8.3.3.1) results from inadequate feedback from the automation of the past, present, and future system states and behavior. In addition, they found designers included functions that had little relationship to the controllers' operational needs. This unneeded functionality increased system complexity, making comprehensive understanding of the automation more difficult. Overall, poor understanding of automation may lead users to rely on automation when it is not warranted, or it may inhibit their ability to use the automation when they need it. HSGT interfaces designed to avoid opaqueness and unnecessary functionality can directly enhance automation understanding (reducing the need for partially compensating selection and training approaches delineated in Section 8.3.3.1).

In summary, failure of HSGT operators to understand the capabilities of automation can threaten system performance and safety. Use of the "tool approach" for the design of HSGT interfaces and methods to avoid opaqueness and unnecessary functionality can directly enhance automation understanding. HSGT operator interfaces designed for automation understanding will reduce the requirements for operator selection and training.

**8.3.3.7 Mistrust** - Related to poor understanding of automation, mistrust can lead people to both use automation when it is inappropriate, and use manual control when automatic control would be more effective. Muir (1988) defines mistrust as a mismatch between the true capabilities of the system and those perceived by the person. This mismatch can result in distrust when the perceived capabilities are lower than the actual capabilities. Likewise, mistrust includes the situation where the person endows the technology with capabilities it doesn't have, leading to an over-trust in the equipment. In many situations, automation has been introduced and its potential has never been realized because of poor user acceptance (Zuboff, 1988). Likewise, situations have occurred where automation has been relied upon in inappropriate situations. Several authors have identified trust in automation as a critical variable in this situation (Zuboff, 1988; Muir, 1988; 1989, Halpin, Johnson & Thornberry, 1973; Lee & Moray, 1992). Trust represents the users' global perception of whether the automation will accomplish current objectives. As such, it represents more than an understanding of automation because it also depends on the user's intuitive feelings for what the automation is likely to do. All other things being equal, distrusting automation will lead to predominantly manual control, whereas highly trusted automation will be used more frequently (Muir, 1989, Lee & Moray, 1992). The design of automation and the training that accompanies its introduction should ensure that users' trust matches the capabilities of the system. This calibration of trust is essential to ensure appropriate use of sophisticated technology. It can be questioned whether this is entirely the case for existing HSGT, or will be in future cases.

**8.3.3.8 Psychosocial Aspects** - Introducing automation into the workplace has potential for severe disruptions in the psychosocial aspects of work. While not related to immediate job performance, issues related to job satisfaction, motivation, and interaction with others play a critical role in system performance (Zuboff, 1988; Bittner, Wiker et al., 1993). Failing to recognize the effects of automation on the social structure and psychological rewards of the job may severely compromise system performance. A study by Ekkers et al. (1979) showed correlations between control system characteristics and operators' subjective feelings of health and achievement. Specifically, they showed that highly complex systems, with high coherence of process information and high process controllability, led to low levels of stress and good health. When the opposite was true, workers reported higher stress and poorer health. There appears to be a shortage of formal assessments of either the coherence of process information or the other psychosocial aspects of existing HSGTs.

## **8.4 IMPLICATIONS FOR HSGT DEVELOPMENT**

This section respectively addresses broad implications for future HSGT development in the U.S. and HSGT display and control guidelines.

### **8.4.1 HSGT Development in the U.S.**

HSGTs (e.g., TGV and ICE) currently utilize high levels of automation (e.g., DOT FRA, 1991a-c; Sheridan, 1993). Sheridan et al. (p. 6-1), in this regard, reports that all major HSGT systems have generally adopted the following:

- Automated means to preclude collisions – This includes automatic braking systems and other means of overcoming the inadequacies of the HSGT operator's inability to visually avoid collisions.

In-cab signaling – This is mandated by the inability of operators to visually perceive wayside signals at HSGT operational speeds (it also provides the basis for automated braking when restrictions are ignored).

Technology for monitoring operator alertness – This reflects an electronic extension of the concept of mechanical dead-man controls in standard trains (with more failure options).

Use of automation is likely to increase as speed increases, as is apparent from earlier discussions centered around several human factors related concerns. Indeed, as noted earlier, the need for automation is apparent in the requirements for such functions as monitoring the state of the track. Each of these concerns, as described earlier, becomes more pronounced as the speed of the train increases (though at low conventional speeds many are negligible). Increased levels of automation or other accommodations, even for existing systems (e.g., TGV), may be required to address special problems unique in the U.S.:

Extended length of runs – The distances between stops in at least certain parts of the U.S. will likely be longer than any in Europe or Japan (GAO, 1993). increasing the risk of greater vigilance decrements. In this regard, Endo et al. (1980) noted that very soon after becoming an HSGT operator, any stress associated with the task disappears, and a loss of alertness may ensue. Extended runs would have the potential of compounding the existing vigilance problems observed in standard train engineers (e.g., high rates of nightly on-the-job napping as per Akerstedt, 1988). Also in this regard, the TGV runs for more than an hour between stops on certain routes, and no vigilance decrement related critical incidents have been officially delineated (but there have been some "informal" suggestions of such effects). However, it is noteworthy that a group at the Universite Rene Descartes (in France) is currently doing psychophysiological studies of vigilance (perhaps also addressing extended run effects) on trains and planes (group is lead by Monsieur Mollard at the Faculte de Medicine de Paris). HSGT automation could be designed to minimize vigilance decrements by better involving the operator (as suggested in Section 8.3.3).

Track Features – Shared tracks (i.e., mixtures of train types and speeds on the same track) with grade-level crossings tend to be the rule in the U.S. in the near term (GAO, 1993). It appears that shared track is the case for the TGV at Tours. However, the trend outside the U.S. is for HSGTs to have dedicated dual tracks at all times when running at design speeds (significantly above the speed of other trains on the line). Likewise, the trend is to preclude grade-level crossings for animals, humans, or vehicles; bridges or tunnels are used where crossings are permitted. Track feature differences suggest that there may be more false alarm emergency stops in the U.S. than HSGTs in other parts of the world have experienced. Increased automation would offer one means to offset the challenges presented by shared tracks and grade-level crossings.

With regard to single track lines, it is noteworthy that 1) the history of railways indicates that trains running in both directions are a recipe for disaster (see, e.g., Rolt, 1978, for case studies), and 2) there is a greater potential for disasters at HSGT operational speeds. The special problems described above and expected future increases in speed both argue for increased automation in future U.S. HSGTs.

#### **8.4.2 HSGT Display and Control Guidelines**

Delineated in this section are general HSGT display and control guidelines, some of which were addressed during earlier considerations (particularly in Section 8.3.2). These are not comprehensive due to literature information limitations and the substantial numbers of unknowns also identified in earlier sections (particularly in Sections 8.3.1 and 8.3.3). Rather, they are offered for potential use as a general checklist in the development and evaluation of HSGT systems. Presented, in turn, are recommendations regarding basic status information and predictor display information.

- Basic status information required for operator decisions in the cab -- this would include:
  - Maximum allowable speed
  - Actual speed
  - Overspeed indication
  - Station location/distance (particularly for maglev)
  - Location of obstacles on the line (possibly supplemented by an on-board object detection system using Radar or other appropriate technique)
  - Train control system status
  - Braking and propulsion system status
  - Communications (data and voice) system status
  - Door closing mechanism status
  - Environmental control system status (in passenger areas and cab), and
  - Passenger information system status.
  
- Predictor display information to assist an on-board operator in emergency stopping situations and in the manual control of station arrivals -- this could include:
  - Route map displaying positions of train and others ahead
  - Headway both in terms of distance and time at current running speed
  - Predicted position of the train if under full emergency braking, and
  - Predicted position of the train under normal (manual) braking, taking into account the dynamics of controlled deceleration.

## **8.5 SUMMARY OF FINDINGS AND CONCLUSIONS**

This section is divided into two subsections that respectively summarize the significant findings of this study and offer general conclusions based on those findings.

### **8.5.1 Summary of Human Factors Aspects Study Findings**

The current study has been concerned with the analysis of human factors aspects of computer-controlled subsystems use in high-speed ground transportation (HSGT) systems. Its first aim was to selectively address physiologically related aspects that can effect HSGT operator performance and system safety. Its second aim was to determine automation related elements that can also effect HSGT personnel performance and safety. The overall purpose of this effort was to augment and selectively extend earlier considerations of human and automation related elements of HSGTs. To achieve these goals and overall purpose, a three part analysis was conducted that addressed: Physiological and Associated Aspects Related to Operator Performance, Implications of Speed, and Implications of Increased Automation. Summaries of the findings associated with these three analyses are presented below. They include some specific recommendations.



**8.5.1.1 Physiological and Associated Aspects Review Summary** - This effort addressed the individual and joint effects of 1) working hours and scheduling, and 2) perceptual conflict effects. Findings included the following:

- Disruptions of circadian rhythms and sleep due to shiftwork can both contribute to fatigue and other associated conditions that reduce HSGT operator vigilance.
- "Perceptual conflict" effects associated with both HSGT motion and visual display terminal (VDT) system interfaces can interactively contribute to fatigue and negatively impact vigilance.

Perceptual conflict and shiftwork together are expected to result in greater HSGT operator vigilance decrements than previously seen on standard trains.

It was also noted, in anticipation of later findings, that these physiologically related vigilance decrements could be compounded by automation related vigilance decrements (associated with reductions in HSGT operator roles and system involvement). This was particularly disturbing because standard train operators currently experience a loss of vigilance (11%-20% experience on-the-job napping). This concern points to the need to experimentally evaluate HSGTs with regard to the identified physiological and associated elements (see Section 8.3.1).

**8.5.1.2 Implications of Speed Review Summary** - This effort addressed the following aspects of speed: 1) permissible deceleration force effects, 2) implication for operator's vision, 3) potential emergency responses available to the operator, 4) demands of normal stopping, and 5) monitoring the state of the track. Concerns associated with each of these aspects becomes more pronounced as the speed of the train increases. Findings included the following:

- Deceleration forces of about 0.25 g represent a practical HSGT limit, and emergency stopping distances for HSGTs would be on the order of 3.5 km (based on a reasonable speed projection for the near future).
- Operator safety harnesses will be needed based upon the potential for inadvertent control activations during both non-emergency and emergency stops.
- HSGT operators will be incapable of perceiving wayside signals at operating speed and given the 3.5 km stopping distance, will not be able to rely on direct vision to make decisions to 1) stop the train because of obstacles on the track, or 2) determine whether or not an object is a train; hence, all applicable safety related status information about the state of the HSGT system must be displayed at the on-board operator's console.
- Automated emergency responses will be required to compensate for the operator's visual and response limitations, particularly with respect to emergency stopping.

- It is important for HSGTs to stop properly at stations; it will not be possible for drivers to achieve this, unless appropriate on-board information is provided.

Direct visual monitoring of the track state from inside the cab will not be possible for a number of conditions (e.g., icing and objects on track), and such information must be provided to the HSGT system from external sensing sources; proper responses must be ensured automatically by appropriate control equipment.

- Onboard-sensor technologies are available that might enable operators to detect objects approximately 3.5 km ahead (radar, laser and other). GPS or other positional information could be used to assist in interpreting the return signals.

These findings provided the basis for a subsequent consideration of future HSGT development in the U.S. This consideration pointed out that the distances between some stops was likely to be longer than those currently utilized in Europe or Japan, increasing the risk of vigilance decrements. Additionally, it was pointed out that shared tracks and grade-level crossings would tend to be the rule in the U.S. in the near term. These aspects of U.S. HSGT operations argue for increased automation in future U.S. HSGTs relative to counterparts in Europe and Japan.

**8.5.1.3 Implications of Increased Automation Review Summary** - This effort addressed the following aspects of increased automation: 1) changes in skill requirements, 2) error potential, 3) skill degradation, 4) workload effects, 5) situational awareness, 6) understanding of automation, 7) mistrust, and 8) psychosocial aspects. Findings included the following:

Changes in operator skill requirements tend to occur with increasing HSGT automation: 1) more abstract thinking, and 2) an increased demand to supervise and monitor automation, rather than interacting with the process directly.

Increased automation requires new skills and procedures, without which, system operation may be difficult or even dangerous; a variety of methods for selection and training of HSGT operators are currently in use to ensure that operators acquire requisite skills and procedures.

- The TGV selection approach is based on measurements of psychomotor or cognitive aptitudes and personality variables; it appears most likely to result in selection of operators with the capabilities to meet the increased requirements of HSGTs.

A combination of current ICE and TGV training approaches appears to be more ideal than either by itself. A combined approach to HSGT operator training remains to be fully developed and evaluated with regard to its performance and safety enhancement effectiveness.

- Automation can increase potential for errors, can amplify them. and make their consequences more severe than in manual systems: this suggests a careful evolutionary approach be used in the automation of HSGTs which recognizes that some functions must be automated for safety purposes.
- Skill degradations occur when automation eliminates low-level control tasks or radically changes control strategies and information sources; this leaves operators ill-prepared to intervene when the automation fails. Selective disengagement of HSGT features would provide one means for off-setting skills degradation if implemented in the design and operation of HSGTs.
- Workload can be inappropriately increased during high stress times and reduced during low stress times by "clumsy" automation. Both of these overload and underload effects can have disastrous effects unless addressed with appropriate methods. "Process tracing" offers one means of ensuring well-designed HSGT interfaces with balanced workload, and should be applied as part of the HSGT design and evaluation process.
- Automation can reduce operator "situation awareness" when it supplants their observation and control, leading to failures to recognize and respond to critical circumstances. Understanding how the design parameters of automation influence situation awareness is consequently a critical factor in enhancing the safety of HSGTs.
- Failing to understand the capabilities of automation can threaten system performance and safety. Use of the "tool approach" for the design of HSGT interfaces and methods to avoid "opaqueness" and "unnecessary functionality" can directly enhance automation understanding and system safety (also minimizing the need for operator selection and training).
- "Mistrust" can lead operators to prefer manual control when automatic control would be more effective (or safer), and has led to the rejection of otherwise well-designed automated systems. Design of HSGT automation and training to ensure that users' trust matches the capabilities of the system is critical to its ultimate success.
- Introducing automation into the workplace has potential for severe disruptions in the "psychosocial aspects of work" and significant compromising of system performance and safety. There appears to be a shortage of formal assessments of either the "coherence of process information" or the other psychosocial aspects of existing HSGTs.

These findings indicate that a number of aspects of automation can have severe safety effects when not "individually addressed." Unfortunately, most of these do not appear to have been well-addressed in existing HSGTs. More of a concern, however, would be their combined and interacting effects. The potentially severe impacts of the combination of these

automation related aspects point to the need for their comprehensive evaluation relative to existing and future HSGT systems.

## **8.5.2 Conclusions**

Three broad safety-related conclusions can be drawn from the individual findings presented above. These are:

HSGT speed, emergency stop, and other control dynamics imply safety-related system requirements to compensate for operator visual, vigilance, and response limitations – these include 1) automated emergency response systems (e.g., emergency braking), 2) on-board console presentation of HSGT status (e.g., speed, equipment failures) and track state (e.g., obstacles on the track), 3) predictor-display/control information to augment basic status information, and 4) operator safety harnesses.

HSGT operator vigilance can be expected to be unacceptably degraded due to the compounding effects of a number of physiological, psychological, automation, and system aspects -- these aspects include 1) disruptions of circadian rhythms and sleep due to shiftwork. 2) "perceptual conflict" effects associated with HSGT motion and VDT interfaces, 3) "underload" and other automation effects degrading operator attention, and 4) extended length of runs expected in certain parts of the U.S.

HSGT automation to compensate for operator limitations and to augment strengths can be successively designed and implemented using appropriate approaches, procedures, and methods -- these include 1) a careful evolutionary approach that recognizes that some functions must be automated for safety, 2) a "tool approach" for the design of interfaces and methods to enhance automation and situational understandings, 3) "Process Tracing" and other means of ensuring a balance between workload and understandings, 4) assessments to ensure users' trust matches system capabilities, 5) operator selection based upon requirement-driven performance and personality testing (e.g., TGV approach), and 6) procedural to full-simulation training (e.g., combination of ICE and TGV approaches).

# **APPENDIX A**

## REFERENCE SOURCES

The following reference sources pertain to the Human Factors Aspects task found in Chapter 8.

1. Akerstedt, M., "Sleepiness As a Consequence of Shift Work," *Sleep*, 11, 17-34, 1988.
2. Bainbridge, L., "Ironies of Automation," In J. Rasmussen, K. Duncan, & J. Leplat (Eds.), *New Technology and Human Error* (pp. 271-283), New York: John Wiley & Sons, 1987.
3. Bittner, A. C., Jr., "Requirements Testing and Evaluation: Human-in-the-Loop Systems," *Ergonomics in Design*, October, 29-32, 1993.
4. Bittner, A. C., Jr. & Guignard, J. C., "Human Factors Engineering Principles for Minimization of Adverse Ship Motion Effects: Theory and Practice," *Naval Engineers Journal*, 97(4), 205-213, 1985.
5. Bittner, A. C., Jr. & Guignard, J. C., "Shipboard Evaluation of Motion Sickness Incidence," In F. Aghazadeh (Ed.), *Trends in Ergonomics/Human Factors V* (pp. 529-541). New York: North-Holland, 1988.
6. Bittner, A. C., Jr., Kantowitz, B. H., & Bramwell, A. T., "Workload Assessment of Automated Flight Decks: Analysis of ASRS Incident Reports," (Final Report), Seattle WA: Battelle Human Affairs Research Centers, 1993.
7. Bittner, A. C., Jr. & Kinghorn, R. A., "Maglev Design Requirement Inputs: Passenger Movement, Food Service, Handicapped Access, Seating Arrangements, and Human Factors," Seattle, WA: Battelle Human Affairs Research Centers, 1992(a).
8. Bittner, A. C., Jr. & Kinghorn, R. A., "Seating Biomechanics and Fatigue: Critical Review of the Literature," Seattle, WA: Battelle Seattle Research Center, 1992(b).
9. Bittner, A. C., Jr., Schuller, C. R., Toutonghi, G. M., Ronhovde, N., & Worl, J. C., "Recommended Protective Force Working Hour and Scheduling Guidelines," Seattle, WA: Battelle Seattle Research Center (Rev. January), 1994.
10. Bittner, A. C., Jr., Wiker, S. F., Kinghorn, R. A., & Bramwell, A. T., "82' Capability Replacement Human Factors Engineering Recommendations: Integrated Literature Review and Baseline Design Evaluation," Seattle, WA: Battelle Seattle Research Centers, 1993.
11. Cook, R. I., Woods, D. D., & Howie, M. B., "The Natural History of Introducing New Information Technology Into a High-Risk Environment," *Proceedings of 35th Annual Meeting of the Human Factors and Ergonomics Society* (pp. 429-433). Santa Monica, CA: Human Factors Society, 1990.

- Curry R. E., "The Introduction of New Cockpit Technology: A Human Factors Study," (NASA Technical Memorandum 86659). Moffen Field, CA: Ames Research Center, 1985.
13. Dorer, R. M. & Hathaway, W. T., "Safety of High Speed Magnetic Levitation Transportation Systems," Washington, DC: U.S. Department of Transportation/ Federal Railroad Administration, 1991.
  14. Ekkers, C. L., Pasmooij, C. K., Brouwers, A. A. F., & Janusch, A. J., "Human Control Tasks: A Comparative Study in Different Man-Machine Systems," In Rijnsdorp (Ed.), Proceedings of IFAC Workshop, Case Studies in Automation Related to Humanization of Work: Enschede, Netherlands (pp. 23-29), New York: Pergamon Press, 1977.
  15. Endo, T., Inomata, O., Ikeda, M., Fukano, S., Sugiyama, I., Tanizawa, H., Hosoya, M., & Matsuda, Y., "Physiological Load of High-Speed Train Operation," Tokyo: Japanese National Railways, Railway Labour Scientific Research Laboratories, 1980.
  16. Endsley, M. R., "Design and Evaluation for Situation Awareness Enhancement," Proceedings of the Human Factors and Ergonomics Society 33rd Annual Meeting (pp. 102-106), Santa Monica, CA: Human Factors Society, 1988.
  17. Government Accounting Office, "High Speed Ground Transportation: Issues Affecting Development in the United States," Washington, DC: U.S. Government Printing Office, 1993.
  18. Graybiel, A. & Knepton, J., "Sopite Syndrome: A Sometimes Sole Manifestation of Motion Sickness," Aviation, Space, and Environmental Medicine, 47, 873-882, 1976.
  19. Halpin, S., Johnson, E., & Thornberry, J., "Cognitive Reliability in Manned Systems," IEEE Transactions on Reliability, R-22, 3, 165-169, 1973.
  20. Kantowitz, B. H. & Bittner, A. C., Jr., "Using Aviation Safety Reporting Systems Database As a Human Factors Research Tool," Proceedings of the 15th Annual Aerospace and Defense Conference (pp. 31-39), New York, NY: Institute of Industrial Engineers, 1992.
  21. Kiser, D. M., Murphy, T. J., & Rogers, S. H., "Hours of Work," In Ergonomic Design for People at Work, (Vol. 2, pp. 275-336), New York: Van Nostrand Reinhold, 1986.
  22. Lackner, J. R. & Graybiel, A., "Elicitation of Motion Sickness by Head Movements," Aviation, Space and Environmental Medicine, 55, 513-520, 1984.
  23. Lee, J. & Moray, N., "Trust, Control Strategies and Allocation of Function in Human-Machine Systems," In Ergonomics (pp. 1243-1270). London: Taylor & Francis, 1992.
  24. Lewis, P. M., "Shift Scheduling and Overtime: A Critical Review of the Literature," (PNL-5391), Richland, WA: Pacific Northwest Laboratory, 1985.

25. Littlewood, B. & Strigini, L., "The Risks of Software," *Scientific American*, November, 62-75, 1992.
26. Mahan, R. P., Carvalhais, A. B., & Queen, S. E., "Sleep Reduction in Nightshift Workers: Is It Sleep Deprivation or a Sleep Disturbance Disorder?" *Perceptual and Motor Skills*, 70, 723-730.
27. Moray, N., "Technosophy and Humane Factors: A Personal View," *Ergonomics in Design*, October, 33-37, 39, 1993.
28. Morrissey, S. J. & Bittner, A. C., Jr., "Development of Motion Sickness Symptoms with Prolonged VDU Use: Artifact or Real-Effect?" In B. Das (Ed.), *Advances in Industrial Ergonomics and Safety II* (pp. 365-371), Bristol, PA: Taylor & Francis Inc., 1990.
29. Muir, B. M., "Operators' Trust in and Use of Automatic Controllers in a Supervisory Process Control Task," Unpublished Doctoral thesis, University of Toronto. Toronto Canada, 1989.
30. Muir, B. M., "Trust Between Humans and Machines. and the Design of Decision Aides," In E. Hollnagel, G. Mancini, & D.D. Woods (Eds.), *Cognitive Engineering in Complex Dynamic Worlds* (pp. 71-84), London: Academic Press, 1988.
31. RAC. "Advanced Train Control Systems," Ottawa, Canada: Railway Association of Canada. 1984.
32. Reason, J. T. & Brand, J. J., "Motion Sickness," New York: Academic Press. 1975.
33. Rochlin, E., LaPorte, T., & Roberts, K., "The Self-Designing High Reliability Organization: Aircraft Flight Operation at Sea," *Naval War College Review*, Autumn, (pp. 76-91), 1987.
34. Rolt, R. T, "Red For Danger," London: Pan Books, 1978.
35. Rosa, R. R., Bonnet, M. H., & Bootzin, R. R., "Intervention Factors Promoting Adjustment to Nightwork and Shiftwork," In A. J. Scott (Ed.), *Shiftwork, Occupational Medicine State-of-the-Art Reviews*, Philadelphia: Hanley & Belfus, 1990.
36. Roth, E. M., Bennett, K. B., & Woods, D. D., "Human Interaction With an 'Intelligent' Machine," *International Journal of Man-Machine Studies*, 27. 479-525, 1987.
37. Sarter, N., "The Flight Management System: Pilots' Interaction With Cockpit Automation," *Proceedings of the International Conference on Systems, Man, and Cybernetics* (pp. 1307-1310). New York, NY: Institute of Electrical and Electronic Engineers, 1991.



- Sarter, N. B. & Woods, D. D., "Pilot Interaction With Cockpit Automation I: Operational Experiences With the Flight Management System (FMS)," Columbus Ohio: The Ohio State University Cognitive Systems Engineering Laboratory, Department of Industrial and Systems Engineering, 1991(a).
39. Sarter, N. B., & Woods, D. D., "Situation Awareness: A Critical But Ill-Defined Phenomenon," *The International Journal of Aviation Psychology*, 1(1), 45-57, 1991(a).
  40. Sarter, N. B. & Woods, D. D., "Mode Error in Supervisory Control of Automated Systems," *Proceedings of the Human Factors Society 36th Annual Meeting*, (pp. 26-29), Santa Monica, CA: Human Factors Society, 1992.
  41. Sheridan, T. B., "Supervisory Control," In G. Salvendy, (Ed.), *Handbook of Human Factors*, New York: Wiley, 1987.
  42. Sheridan, T. B. & Hennessy, R. T., "Research and Modeling of Supervisory Control Behavior," Washington, D.C.: National Academy Press, 1984.
  43. Sheridan, T. B. & Johannsen, G., "Monitoring Behavior and Supervisory Control," New York: Plenum, 1976.
  44. Sheridan, T. B., Lanzilotta, E., & Yin, S., "Human Factors and Safety of High Speed Rail Systems," Massachusetts: M.I.T., Human-Machine Laboratory, 1993.
  45. U.S. Department of Transportation/Federal Railroad Administration, "Safety Relevant Observations on the ICE High Speed Train," Washington. DC: U.S. Government Printing Office. 1991(a).
  46. U.S. Department of Transportation/Federal Railroad Administration, "Safety Relevant Observations on the TGV High Speed Train," Washington, DC: U.S. Government Printing Office, 1991(b).
- U.S. Department of Transportation/Federal Railroad Administration, "Safety Relevant Observations on the X-2000 Train," Washington, DC: U.S. Government Printing Office, 1991(c).
48. Wiener, E. L., "Human Factors of Advanced Technology ("Glass Cockpit") Transport Aircraft," (NASA Contractor Report No. 177 528), Moffea Field, CA: NASA-Ames Research Center, 1989.
  49. Wiener, E. L. & Curry, R. E., "Flight-Deck Automation: Promises and Problems," *Ergonomics*, 23(10), 995-1011, 1980.
  50. Woods, D. D., "Paradigms for Intelligent Decision Support," In E. Hollnagel, G. Mancini, and D. D. Woods (Eds.), *Intelligent Decision Support in Process Environments*, New York: Springer-Verlag, 1986.

51. Woods, D. D., Potter, S. S., Johannesen, L. & Holloway, M., "Human Interaction With Intelligent Systems: Trends, Problems, New Directions," Columbus, Ohio: Ohio State University, 1991.
52. Zuboff, S., "In the Age of the Smart Machine: The Future of Work and Power," New York: Basic Books, 1988.

# **APPENDIX B**

## **INFORMATION SOURCES**

Below is a list of information sources used in this Option Task. As noted earlier, references sources used in the Human Factors Aspects task are listed separately in Appendix A.

- 1) MIL-STD-882C, "System Safety Program Requirements," U.S. Department of Defense, January 19, 1993.
- 2) MIL-STD-882B, Notice 1, "System Safety Program Requirements," U.S. Department of Defense, July 1, 1987.
- 3) DOD-STD-2167A, Revision A, "Defense System Software Development," U.S. Department of Defense, February 29, 1988.
- 4) MIL-STD-SDD, "Software Development and Documentation," Draft, (Revision to DOD-STD-2167A), U.S. Department of Defense, December 22, 1992.
- 5) DOD-STD-2168, "Defense System Software Quality Program," U.S. Department of Defense, April 29, 1988.
- 6) MIL-STD-1574, "System Safety Standard for Space and Missile Systems," U.S. Department of Defense, August 15, 1979.
- 7) MIL-STD-1629A, "Procedures for Performing A Failure Mode, Effects and Criticality Analysis," U.S. Department of Defense, November 24, 1980.
- 8) AF Regulation 122-9, "The Nuclear Surety Design Certification Program for Nuclear Weapon System Software and Firmware," Department of the Air Force, August 24, 1987.
- 9) AF Regulation 122-10, "Nuclear Surety Safety Design Criteria for Nuclear Weapon Systems," Department of the Air Force, January 5, 1982.
- 10) DOD 5200.28.STD, "Trusted Computer Security Evaluation Criteria (TCSEC)" or "Orange book," U.S. Department of Defense, December 1985.
- 11) CMU/SEI-91-TR-24, "Capability Maturity Model for Software," Research Access/U.S. Department of Defense, 1991.
- 12) CMU/SEI-87-TR-23, "A Method for Assessing the Software Engineering Capability of Contractors," Preliminary Version, Software Engineering Institute, September 1987.
- 13) "TRILLIUM Model, Telecom Software Product Development Capability Assessment," Bell Canada, 1992.

- 14) "Software Process Improvement and Capability Determination Model (SPICE)," Project Overview, International Electrotechnical Commission (IEC) and International Standards Organization (ISO), 1993.
- 15) MIL-HDBK-287 "A Tailoring guide for DOD-STD-2167A, Defense System Software Development," U.S. Department of Defense, August 11, 1989.
- 16) AFSC/AFLC Pamphlet 800-5, "Software Independent Verification and Validation," Department of the Air Force, May 20, 1988.
- 17) 14 CFR Part 21 and 25, "Certification Procedure for Products and Parts" and "Airworthiness Standards for Transport Category Airplanes," Federal Aviation Administration (FAA).
- 18) Advisory Circular 25.1309-1A, "System Design and Analysis," FAA, June 21, 1988.
- 19) RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," RTCA, December 1, 1992.
- 20) ARP 4754, Draft 23C, "Systems Integration Requirements," Society of Automotive Engineers (SAE), January 19, 1993.
- 21) ARP 4761, Draft 4, "Safety Assessment Guidelines for Civil Airborne Systems and Equipment," SAE, February 26, 1993.
- 22) Regulatory Guide 1.152, "Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," Nuclear Regulatory Commission (NRC), November 1985.
- 23) ANSIIIEEE-ANS-7.4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," ANSIIIEEE, July 6, 1982.
- 24) IEEE Standard 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE, 1991.
- 25) P-7.4.3.2, Draft 7, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE, 1993.
- 26) ASME NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities," ASME, 1989.
- 27) ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications," ASME, 1990.

- 28) ANSUANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry," American Nuclear Society, May 13, 1987.
- 29) Wallace, D.R., Kuhn, D.R., Ippolito, L.M., and Beltracchi, L., "An Analysis of Standards for the Assurance of High Integrity Software," National Institute of Standards and Technology, U.S. Nuclear Regulatory Commission.
- 30) IEEE STD 467-1980, "Standard Quality Assurance Program Requirements for the Design and Manufacture of Class 1E Instrumentation and Electric Equipment for Nuclear Power Generating Stations," IEEE.
- 31) IEC Standard Publication 880, First Edition, "Software for Computers in the Safety Systems of Nuclear Power Stations," IEC, 1986.
- 32) 982C-H69002-0001, Revision 00, "Standard for Software Engineering of Safety Critical Software," Ontario Hydro/AECL-Candu, December 21, 1990.
- 33) "State of the Art Report on Software Important to Safety in Nuclear Power Plants," Version 2, International Atomic Energy Agency, May 13, 1993.
- 34) ANSUIEEE Std 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," ANSUIEEE.
- 35) IEC/CEI 987, "Programmed Digital Computers Important to Safety for Nuclear Power Stations," IEC/CEI, November 1989.
- 36) ANSUIEEE 730-1989, "Software Quality Assurance Plans. ANSUIEEE.
- 37) ANSUIEEE 828-1990, "Standard for Software Configuration Management Plans, ANSUIEEE.
- 38) ANSUIEEE 829-1983, "Standard for Software Test Documentation," ANSVIEEE.
- 39) ANSUIEEE 830-1984, "Guide for Software Requirements Specification," ANSUIEEE.
- 40) ANSVIEEE 1012-1986, "Standard for Software Verification and Validation Plans," ANSVIEEE, February 10, 1987.
- 41) ANSVIEEE 1016-1987, "Recommended Practice for Software Design Descriptions," ANSVIEEE.
- 42) ANSVIEEE 1028-1988, "Standard for Software Reviews and Audits," ANSVIEEE.
- 43) "IEEE Software Engineering Standards Collection," Spring 1991 Edition, IEEE, April 5, 1991.

- 44) P1228, "Standard for Software Safety Plans," Draft J, February 11, 1993.
- 45) Bowen, J., Stavridou, V., "Safety Critical Systems, Formal Methods and Standards," Oxford University Computing Laboratory.
- 46) FPS PUB 101. "Guideline for Lifecycle Validation, Verification and Testing of Computer Software," National Bureau of Standards (NBS), June 6, 1983.
- 47) FPS PUB 132, "Guideline for Software Verification and Validation," NBS, 1987.
- 48) "A Comparison of U.S and Foreign Safety Regulations for Potential Application to Maglev Systems," Draft Final Report, Arthur D. Little, October 1992.
- 49) Wallace, D.R. and Fuji, R.U., "Software Verification and Validation: An Overview," IEEE Software, 1989.
- 50) Leveson, N.G., "Software Safety in Embedded Computer Systems," Communications of the ACM, Vol. 34, No. 2, February 1991.
- 51) NIST Special Publication 500-165, "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards." NBS, 1989.
- 52) NHB 1700.1 (V1-B), "NASA Safety Policy and Requirements Document," National Aeronautics and Space Administration (NASA), Advance Copy, June 1993.
- 53) NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the National Space Transportation System," NASA.
- 54) "The Computer Control of Hazardous Payloads," Final Report, NASA, July 24, 1991.
- 55) "Draft Computer Development and Performance Requirements" for Space Shuttle Payloads, 1993.
- 56) "Software Safety Standard," Draft, NASA, May 26, 1993.
- 57) SSP 30309 (Rev. B), "Safety Analysis and Risk Assessment Requirements Document," NASA, October 1991.
- 58) TSS 30666, "Program Master Verification Plan: Avionics and Flight Software Integration and Verification Plan," Volume 4, Part 1, Change Request, NASA, 1993.
- 59) JPL D-576, "Independent Verification and Validation of Computer Software: Methodology," Jet Propulsion Lab (JPL), February 9, 1983.
- 60) JPL D-10058, "Software Systems Safety Handbook," JPL, May 10, 1993.

- 61) "A Brief Overview of NASA Langley's Research Program in Formal Methods," NASA Langley Research Center, September 18, 1992.
- 62) ATCS Specification 130, "Recommended Practices for Software Quality Assurance," Revision 3.0, Railway Association of Canada (RAC)/Association of American Railroads (AAR), March 1993.
- 63) ATCS Specification 140, "Recommended Practices for Safety and Systems Assurance," Revision 3.0, RAC/AAR, March 1993.
- 64) "ATCS Industry Standard Software Development Request for Information," AAR, 1993.
- 65) TP 10770E, "ATCS System Safety Validation Programs," Transport Canada, November 1990.
- 66) "FDA Policy for the Regulation of Computer Products," Food and Drug Administration (FDA), Draft, 1989.
- 67) "Reviewer Guidance for Computer Controlled Medical Devices Undergoing 510 (k) Review," FDA, August 29, 1991.
- 68) "Application of the Medical Device GMPS To Computerized Devices and Manufacturing Processes-Medical Device GMP Guidance for FDA Investigators," Draft, FDA, November 1990.
- 69) IEC 62 (Secretariat) 69, "Electrical Equipment in Medical Practice," Draft, IEC, March 1993.
- 70) IEC 65A (Secretariat) 122, "Software for Computers in the Application of Industrial Safety Related Systems," Draft, International Electrotechnical Commission (IEC), November 1991.
- 71) IEC 65A (Secretariat) 123, "Generic Aspects: Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems," Version 7, Draft, IEC, 1992.
- 72) DIN V VDE 0801, "Principles for Computers in Safety Related Systems," DIN/VDE, January 1990.
- 73) DIN V 19250, "Fundamental Safety Analyses for MSR (Measurement-Control-Regulation) Protective Devices. DIN/VDE, January 1989.
- 74) DIN VDE 0831, "Electrical Equipment for Railway Signalling," DIN. June 1983.
- 75) Mü 8004, "Principles of Technical Approval for Signalling and Communications Technology," (with supplements and revisions), German Federal Railway (DB).



- 76) "Minimum Requirements for Safety Related Computers in Railroad and Nuclear Engineering," Research Report, TÜV Rheinland and TÜV Deutschland. 1988.
- 77) Holscher, H. and Rader, J., "Microcomputers in Safety Technique-An Aid to Orientation for Developer and Manufacturer," TÜV Rheinland and TÜV Bayern, 1986.
- 78) "Safety Related Computers, TC7: Systems Reliability, Safety and Security," TÜV Rheinland, European Workshop on Industrial Computer Systems, 1985.
- 79) SBT 90.01/00/E, "Guidelines for the Assessment of Safety Relevant Computer Systems in Railroad Technology." TÜV Rheinland.
- 80) Krebs, H., "Verification of Safety Related Programs for a Maglev System," WP 520, TÜV Rheinland, European Workshop on Industrial Computer Systems, July 21, 1986.
- 81) Blomerius, J., "Status of the Safety Certification Process of the Transrapid System," TÜV Rheinland. 1993.
- 82) Haspel, U., "Procedure for the Coordinating Safety Certification of the New Automatic Passenger Transfer System (PTS) at the Frankfurt Rhein Main Airport." TÜV Rheinland, 1993.
- 83) Jopke, K., Knigge, R., and Schnieder, E., "Functional Specification of Vital Computer Software for High-Speed Maglev Systems," SAFECOMP 1992.
- 84) Krebs, H., "Recommendations for the Determination of the Test Interval for Redundant Safety Related Systems," European Workshop on Industrial Computer Systems TC7 Safety and Security, March 1981.
- 85) CLC/TC9X/SC9XA/WGA1, "Railway Applications: Software for Railway Control and Protection Systems," Draft, CENELEC, 1993.
- 86) CLC/TC9X/SC9XA/WGA2, "Railway Applications: Safety Related Electronic Control and Protection Systems," Draft, CENELEC, April 1993.
- 87) TC9X-WG5B, "Dependability for Guided Transport Systems, Pan 4: Specification and Demonstration of Safety," CENELEC.
- 88) Freudenreich, P. and Gilles, L., "Validation and Certification of the Track-To-Engine Signal Transmission System TVM 430 for the TGV-North High-Speed Train," SNCF/CSEE Transport.
- 89) Guilleux, B., "The Signalling of the New Lines Is Evolving Toward TVM 430," SNCF.
- 90) "Automatic Train Control Systems," 4.92 VT 191, Siemens AG, 1993.

- 91) "Chapter 3: Assessment Methods for Safety Critical Software by Siemens," Siemens AG, 1993.
- 92) A25000-P0001-01-0035, "Software Development Guidelines: Software for Computers in the Industrial Application of Safety Critical Systems-Methods and Tools," Siemens AG, August 12, 1992.
- 93) Goddard, E.O., and Zufferey, C.H., "Report of the Technical Committee, Cross-Acceptance of Vital Signalling Systems," Institution of Railway Signal Engineers (IRSE), March 12, 1992.
- 94) Report No. 1, "Safety System Validation With Regard to Cross-Acceptance of Signalling Systems by the Railways," IRSE, January 14, 1992.
- 95) FS 3019, "Safety Review Process," ABB Signal AB, January 27, 1993.
- 96) Sundvall, K-E., FS 2059, "Design of Fail-Safe Equipment: Organization of Safety Measures in Different Product Phases," ABB Signal AB, April 23, 1992.
- 97) Technical Specification No. 23:1991, "Safety Related Software for Railway Signalling." Consultive Document, Railway Industry Association (RIA), 1991.
- 98) Cribbens, A.H., "Solid-State Interlocking (SSI): An Integrated Electronic Signalling System for Mainline Railways," IEE Proceedings, Vol. 134, Pt. B, No. 3, May 1987.
- 99) Cribbens, A.H., "Microprocessors in Railway Signalling: The Solid State Interlocking," Microprocessors and Microsystems, Vol. 11, No. 5, June 1987.
- 100) Cribbens, A.H. and Mitchell, I.H., "The Application of Advanced Computing Techniques to the Generation and Checking of SSI Data," British Rail Research, July 23, 1991.
- 101) Ingleby, M. and Mitchell, I., "Proving Safety of a Railway Signalling System Incorporating Geographic Data," British Rail Research.
- 102) BS 5887, "Code of Practice for Testing of Computer-Based Systems, British Standards Institute (BSI), 1980.
- 103) BS89/33006DC, "Software for Computers in the Application of Industrial Safety Related Systems," BSI.
- 104) BS89/33005DC, "Functional Safety of Programmable Electronic Systems: Generic Aspects," BSI.
- 105) 89197714. "Guide to the Assessment of Reliability of Systems Containing Software," BSI, September 12, 1989.

- 106) ELS-DOC-4817 Issue A, "Code of Practice for Validation of Modifications to Previously Validated Code," British Rail Research, September 6, 1990.
- 107) ELS-DOC-4888 Issue A, "Code of Practice for the Validation of Safety Critical Software," British Rail Research, October 26, 1990.
- 108) SSU-D-SVA-RR-1, "Software Verification and Validation Policy Review," British Rail Research, November 27, 1992.
- 109) "Programmable Electronic Systems in Safety Related Applications, Part 1: An Introductory Guide," Health and Safety Executive, 1987.
- 110) "Programmable Electronic Systems in Safety Related Applications, Part 2: General Technical Guidelines, Health and Safety Executive, 1987.
- 111) "SafeIT, The Safety of Programmable Electronic Systems: A Government Consultation Document on Activities to Promote Safety of Computer-Controlled Systems, Part 1-Overall Approach and Part 2-Standards Framework," Interdepartmental Committee on Software Engineering (ICSE), June 1990.
- 112) UIC 738 R, "Processing and Transmission of Safety Information," International Union of Railways (UIC), 2nd Edition, January 1, 1990.
- 113) Report RP 8, "On Proving the Safety of Transmission Systems," UIC/Office of Research and Experiments (ORE), April 1986.
- 114) Report RP 11, 'Proof of Safety of Computer-based Safety Systems," UIC/ORE, September 1987.
- 115) Akita, K., Watanabe, T., Hanakmura, H., and Okumura, I., "Computerized Interlocking System for Railway Signalling Control: SMILE," IEEE Transactions on Industry Applications, Vol. 1A-21, No. 4, May/June 1985.
- 116) Akita, K. and Nakamura, H., "Safety and Fault-Tolerance in Computer Controlled Railway Signalling Systems," International Working Conference on Dependable Computing for Critical Applications, August 23-25, 1989.
- 117) Guiho, G. and Hennebert, C., "SACEM Software Validation," IEEE, 1990.
- 118) Martin, M.J., "Vital Processing by Single Coded Unit," Matra Transport.
- 119) Forin, P., "Vital Coded Microprocessor Principles and Publication for Various Transit Systems," Matra Transport.
- 120) Abrial, J.R., "A Formal Approach to Large Software Construction," Matra Transport, March 1989.

- 121) NF F 71-011, "Railway Fixed Equipment and Rolling Stock, Data Processing, Software Dependability, Generalities." AFNOR, 1990.
- 122) NF F 71-012, "Railway Fixed Equipment and Rolling Stock, Data Processing, Software Dependability, Stresses on Software," AFNOR, 1990.
- 123) NF F 71-013, "Railway Fixed Equipment and Rolling Stock, Data Processing, Software Dependability, Adapted Methods for Software Safety Analyses," AFNOR, 1990.
- 124) ESA PSS-05-0 Issue 2, "ESA Software Engineering Standards," European Space Agency (ESA), February 1991.
- 125) ESA PSS-01-40 Issue 2, "System Safety Requirements for ESA Space Systems and Associated Equipment," European Space Agency.
- 126) STANAG 4404, "Safety Design Requirements and Guidelines for Munition Related Safety Critical Computing Systems," Draft, NATO, March 7, 1990.
- 127) NSWC TR 89-33, "Software Systems Safety Design Guidelines and Recommendations." Naval Surface Warfare Center, March 1989.
- 128) Interim Defence Standard 00-55 (Part 1)/Issue 1, "The Procurement of Safety Critical Software in Defence Equipment, Part 1: Requirements," Ministry of Defence. April 5, 1991.
- 129) Interim Defence Standard 00-55 (Part 2)/Issue 1, "The Procurement of Safety Critical Software in Defence Equipment, Part 2: Guidance," Ministry of Defence, April 5, 1991.
- 130) Interim Defence Standard 00-56 Issue 1, "Hazard Analysis and Safety Classification of the Computer and Programmable Electronic System Elements of Defence Equipment," Ministry of Defence, April 5, 1991.
- 131) SEB6-A, "System Safety Engineering in Software Development," EIA Bulletin, April 1990.
- 132) SRAS-02-S-000-3. "The SQMS Approach Applied in the Development of the S. R. ASCV Project," SASIB (no date).
- 133) SRAS-03-S-000-4, "Software Verification and Validation Plan for the S. R. ASCV System." SASIB (no date).
- 134) "V&V Methodologies for Computer-based Equipment." SASIB (no date).
- 135) STANAG 4452, "Safety Assessment of Munition Related Computing Systems," first draft, NATO, no date.

- 136) UL 1998, "Proposed First Edition of the Standard for Safety Related Software," draft, Underwriters Laboratory. July 30. 1993.
- 137) IS 402, "Technical Specifications for the Supply of Electronic Equipment for Safety and Signalling Systems," January 1988 Edition, Italian State Railways.

# APPENDIX C

## INDIVIDUAL CONTACTS

- 1) Mr. Chinnarao Mokkalpati, Manager - Design Assurance Engineering, US&S
- 2) Mr. Neal Illenberg, Manager - Engineering Support, GRS
- 3) Mr. Hany Rizkalla, Director of Quality Assurance, ALCATEL-Canada
- 4) Mr. Jeff Utterbach, Manager - Product Assurance, Harmon Electronics
- 5) Mr. William McClaren, Chief - Current Technology Division, Transportation Development Center/Transport Canada
- 6) Mr. Ian Naish, Railway Safety Directorate/Transport Canada
- 7) Mr. Howard Moody, Manager-Advanced Train Technology, AAR
- 8) Mr. Robert Ayers, Manager-C(4) Systems, ARINC Research
- 9) Ms. Delores Wallace, National Institute of Standards and Technology/National Computer Systems Laboratory
- 10) Mr. Lea Beltracchi, U.S. Nuclear Regulatory Commission
- 11) Mr. Joseph Joyce, U.S. Nuclear Regulatory Commission
- 12) Mr. James Stewart, U.S. Nuclear Regulatory Commission
- 13) Mr. John Harauz, Senior Design Specialist-Control Computers, Ontario Hydro
- 14) Mr. Peter Saraceni, Jr., Program Manager-Flight Safety Research Branch, FAA
- 15) Mr. John Dimtroff, Acting Manager-Flight Test and Systems Branch, FAA
- 16) Mr. Philip White, Director of Office of Standards and Regulations, Food and Drug Administration
- 17) Mr. Bernard Liebler, Director-Standards and Electromedical Programs, Health Industry Manufacturers Association
- 18) Mr. Walter Frazier, Head of Systems Electronics Branch, NASA Headquarters
- 19) Ms. Kathrine Kemp, Office of Safety and Mission Assurance, NASA
- 20) Mr. John Kelley, Software Product Assurance Group, Jet Propulsion Laboratory

- 21) Ms. Karen L'Heureux, Systems Safety Office, Jet Propulsion Laboratory
- 22) Mr. David Tadlock, Senior Engineer, Flight Data Systems Division, NASA Houston
- 23) Mr. William Bates, Space Station Safety and Mission Assurance Division, Control Systems-Branch Chief, Johnson Space Center, NASA
- 24) Mr. George Sabolish, Software Product Assurance Manager, NASA Headquarters
- 25) Robert Hinson, Chief of Shuttle Data Systems Branch, Johnson Space Center/NASA
- 26) Mr. Jim Lloyd, Acting Safety Director, NASA Headquarters
- 27) Mr. Donald Sova, NASA Headquarters
- 28) Mr. Robert Hoi, Aerospace Engineer, Flight Systems Safety, Johnson Space Center/NASA
- 29) Mr. George Finelli, NASA Langley Research Center
- 30) Mr. Gerhard Aue, Senior Engineer, Transportation Systems Group, Siemens AG
- 31) Mr. Hans Knape, Engineer, Distribution Department, Transportation Systems Group, Siemens AG
- 32) Dr. Reder, Software Development, Transportation Systems Group, Siemens AG
- 33) Mr. Horst Strelow, Hardware Development, Transportation Systems Group, Siemens AG
- 34) Mr. Gunter Martitz, Siemens Transportation Systems (U.S.)
- 35) Dr. Heinrich Krebs, Institute for Software, Electronics and Railroad Technology, TÜV Rheinland
- 36) Mr. Joachim Blomerius, Institute for Software, Electronics and Railroad Technology, TÜV Rheinland
- 37) Mr. Ken Burrage, Director of Technical Standards, British Rail
- 38) Mr. Keith Hacker, Safety Validation Manager, British Rail
- 39) Mr. C.J.A. Edwards, Technical Standards Engineer, British Rail
- 40) Dr. Maurice Pollard, Director-Engineering Research and Development, British Rail Research



- 41) Mr. Michael Powell, Commercial Director , British Rail Research
- 42) Dr. Allen Cribbens, Head of Safety Critical Systems Unit. British Rail Research
- 43) Mr. R. Bell, Health and Safety Executive (U.K.)
- 44) Mr. Roger Short. Principle Inspecting Officer of Railways, Railway Inspectorate (U.K.)
- 45) Mr. Karl Lennartz, Section Head of Safety Related Systems and Safety Related Requirements, Bundesbahn Zentralamt (BZA), German Federal Railway
- 46) Mr. Karl-Erik Sundvall, Manager-Fail-safe Department, ABB Signal AB
- 47) Mr. W.R. Smith, Deputy Director-Technical and Production, ERRI
- 48) Mr. Bengt Sterner, Chairman of Signalling Subcommittee for UIC; also, Swedish State Railways
- 49) Mr. Jacques Balause, Director of International Affairs, SNCF
- 50) Mr. Jean-Paul Guilloux, Chief of Signalling Department, SNCF
- 51) Mr. Pierre Freudenreich, Engineer-Signalling Department, SNCF
- 52) Ms. Nancy Gurd, Attorney, SYSTRA/SOFRERAIL
- 53) Mr. Jean Martin, ATC Business Development and Marketing, Matra Transport
- 54) Mr. Walter Schon, RAMSS Division Assistant Manager, Matra Transport
- 55) Mr. Jean-Louis de Montlivault, Space Activities Director, Bureau Veritas
- 56) Mr. Robert Record, Project Manager (Space), Bureau Veritas
- 57) Mr. Giuseppe Bonfigli, General Manager-Signalling Division, Sasib
- 58) Mr. Katsuji Akita, Chief-Signalling Laboratory, Railway Technical Research Institute
- 59) Mr. Yasuo Sato, General Manager, Planning Division of RTRI
- 60) Mr. Horoshi Tachikawa, Manager-Signal Engineering Department, Nippon signal
- 61) Mr. Akiyoshi Yamamoto, Deputy Director, New York Office of Japan Railways Group
- 62) Mr. Kazamaru Shinoya, Safety Research Laboratory, East Japan Railways

- 63) Hiromitsu Yoshida, Safety Research Laboratory, East Japan Railways
- 64) Mr. Shinichiro Asano. International Division, East Japan Railways
- 65) Mr. Korefumi Tashiro, Industrial System Control Section, Hitachi Research Laboratory
- 66) Mr. Tony Zawilski. Chairman of IEEE Software Safety Working Group
- 67) Mr. William Brykeynski, Institute for Defense Analyses
- 68) Mr. Roger Fuji, Operations Manager, Systems Technology Operation, Logicon
- 69) Mr. Jean-Mormand Drouin, Quality Assurance, Bell Canada
- 70) Dr. A. Sethy, Arsenal-Federal Institute for Testing and Research (Vienna, Austria)
- 71) Attilio Ciancabilla, SASIB (Bologna, Italy)
- 72) Mathew Vlasaty, Engineering Team Leader, Underwriters Laboratory

Note: Special thanks to Mr. Jeff Gordon (VNTSC) and Mr. Arne Bang (FRA) for assisting in the identification, procurement and/or translation of relevant documentation.

# **APPENDIX D**

## RESPONSES FROM INDUSTRY SURVEY

In November of 1992, the High-Speed Ground Transportation Special Projects Office of the Federal Railroad Administration (FRA) with support from the Volpe National Transportation System Center, initiated a study of the methodologies used for verification and validation of safety-critical software by several organizations worldwide. These included domestic and foreign railroads, signal and train control equipment suppliers/developers, as well as military and medical organizations.

The study was separated into two distinct parts: the first was an overview of the state-of-the-art of software validation, and the second involved development of a "composite" methodology, which would include the best elements of those reviewed, and could serve as a prototype for consideration by FRA for possible application to safety-critical software in railroad control systems.

At present, there are no FRA standards that specifically apply to software-driven safety-relevant railway signaling and train control devices to demonstrate safe operation. To fill this void, the FRA has been considering requiring that a process be followed throughout the life cycle of safety-relevant software-driven products. This process could become a uniform standard to be followed by the railroad industry in the United States and be required by the FRA of manufacturers and users of microprocessor-based safety-critical railroad signalling and train control equipment. Adherence to the process should demonstrate that the software driven system will operate with adequate levels of safety. This process or methodology should also allow freedom to the supplier in system design as well as freedom in how to demonstrate its safety. It should not stifle development and application of other more efficient technologies. Compliance with the process could be established by audit conducted by qualified personnel from FRA or, possibly, from a recognized certification organization. The enclosed report on Development of a Safety Validation Methodology represents a preliminary attempt at developing a uniform validation process for the railroad signal industry.

Since industry comments and critiques on this proposed methodology are important to us, draft copies of the two reports generated during the safety validation project are enclosed for your review. The first volume contains the review of the methodologies of approximately twenty-five organizations. The second volume describes the proposed methodology as developed from an assessment of those described in the first volume.

We would appreciate **your** review of these reports as well as any comments regarding the content of the proposed methodology. If telephone contact is needed for further clarifications, you may reach Manuel Galdo, FRA Office of Research and Development at **202-366-1344**. However, should you desire to respond to this request, we prefer that all comments and remarks be addressed in writing to:

Jeff Gordon  
US DOT/RSPA  
Volpe National Transportation Systems Center, DTS-76  
55 Broadway  
Cambridge, MA **02142**

Sincerely,

Claire L. Orth  
Director, Office of Research and Development

cc: Philip Oleksyzk  
William Goodman  
**Lang** Nguyen  
William Paxton  
Manuel **Galdo**  
Robert Dorer  
Jeffrey Gordon

encl: Distribution list  
Base Task Report  
Option Task Report

Lt. Col. Dave **Alberico**  
HQ Air Force Safety Agency/SES  
9700 Avenue G, Suite **250B**, SE  
**Kirtland** AFB, New Mexico 87117-5670

Mr. Robert **Ayers**  
Manager - **C(4)** Systems  
**ARINC** Research Corporation  
MS 5-371.2551 **Riva Road**  
Annapolis, MD 21401

Mr. **Gideon Ben-Yaacov**  
Automated Monitoring & Control International, Inc.  
11819 Miami **Street**  
Omaha, NE **68164**

Mr. William J. **Berger**, Director  
Communication and Signals Engineering  
Chicago and Northwestern Transportation Company  
165 North **Canal**  
Chicago, IL 60606

Mr. Dennis G. Boll  
Superintendent Signals  
**Burlington Northern** Railroad Co.  
176 East 5th S t  
Saint Paul, MN 55101

Mr. Bill **Breeden**, Director  
Signal **Engineering**  
Union Pacific Railroad  
1416 Dodge S t  
Omaha, NE **68179**

Mr. Jim **Bullough-Latsch**  
**Rockwell International** Corporation  
21115 **Devonshire** Sheet, #287  
Chatsworth, CA 91311

**Brymer** Chin  
**AT&T** Bell Labs  
Room **15C-245**  
67 **Whippany** Road  
**Whippany**, NJ 07981

Mr. Frank Cooper, Jr.  
General Superintendent, Communications Systems  
**Southern** Pacific Transportation Co.  
**Southern** Pacific Building, One Market Plaza  
San Francisco, CA 94105

Mr. John C. Fink III  
Vice President, **Marketing** Signaling Equipment  
AEG **Westinghouse** Transportation Systems, Inc.  
**1501** Lebanon Church Road  
**Pittsburgh, PA** 15236-1491

Mr. Chuck Gibson  
**Marketing** Representative  
AEG Transportation Systems  
1501 Lebanon Church Road  
Pittsburgh, PA **15236-1491**

Mr. Ted **Giras**  
Director Advanced Technology Group  
Union Switch & Signal **Inc.**  
**5800** Corporate Dr.  
Pittsburgh, PA 15237

**Ken Gullins**  
Transport Canada  
**ASRB**  
344 **Slater Street**, 15th Floor  
Ottawa, Ontario  
**K1A 0N5**  
CANADA

Mr. Robert E. **Heggstad**  
Vice President - Technology  
Harmon Electronics, Inc.  
1300 Jefferson Court  
Blue Springs, Missouri 64015

Seti **Helmi**  
10711 Rochester Avenue  
**Los Angeles**, CA 90024

Mr. Hugh **Henry**, Executive Director  
Communications and Signal Division  
Association of American Railroads  
50 F **Street, N.W**  
Washington, DC 20001

Mr. Bob **Jahn**  
Signaling Systems  
Siemens Transportation Systems, Inc.  
**767, 5th** Ave.  
New **York**, NY 101053

Donald Johnson  
Sensors and Communications Systems Division  
Hughes **Aircraft Company**  
Bldg. 676, **MS DD345**  
P.O. Box 3310  
Fullerton, CA 92634

Mr. John **LaForce**, P.E  
Assistant **Chief** Engineer  
**Power** Signals Communications, Commuter Rail  
**Southeastern Pennsylvania** Transportation Authority  
200 W. Wyoming Avenue  
Philadelphia, PA 19140-1597

Mr. Lawrence E. Light  
**Senior** Director, Communications and Signals  
National Railroad Passenger Corporation  
2000 **Market** St.  
**Philadelphia**, PA 19103

**Mr. John Marino**  
**MATRA Transit, Inc.**  
25 East Spring Valley Avenue  
Maywood, NJ 07607

Kevin Marky  
10450 Wilshire Boulevard  
**Apt. 8H**  
Los Angeles, CA 90024

Mr. William **McClaren**  
Chief, **Current** Technology Division  
Transportation Development **Center/Transport**  
Canada  
**Canada** Building  
344 **Slater** Street. 15th **Floor**  
Ottawa, ON **K1A** ON5  
Canada

**Brian Moriarty**  
**TRW**  
P.O. Box 10400 (**W1-2426**)  
**Fairfax**, VA 22031

Mr. Roland E. **Moseley**  
Director, **Strategic** Planning  
**Harris Corporation**  
P.O. Box 37. **MS** 211730  
Melbourne, **EL** 32902

Mr. Joseph F. **Noffsinger**  
Chief, **Engineer** Communications and Signals  
Consolidated Rail **Corporation**  
2001 **Market** S t  
Philadelphia. PA 19101-1417

Mr. Ronald B. Page  
General Director Telecommunications and Signals  
Communications and Signal Department  
**The Atcheson, Topeka & Santa Fe Railway Co.**  
1700 **East Golf** Rd  
**Schaumburg**, **IL** 60173

Mr. William Petit  
**Product** Design Manager  
General Railway Signal  
P. O. Box 20600  
Rochester, NY 14602-0600

Mr. W. D. **Pickett**  
President  
Brotherhood of Railroad Signalmen  
601 West Golf Road, Box U  
Mount Prospect, **IL** 60056-9048

Mr. **Hany Rizkalla**  
D i t o r of Quality Assurance  
**Alcatel Canada, Inc.**  
1235 **Ormont** Dr.  
**Weston**, ON M9L 2W6  
Canada

Mr. David B. Rutherford, Jr.  
Manager, Digital Applications  
Rail Transportation Systems. **Inc.**  
2041 Clinton Avenue South  
Rochester, NY 14618

George **Sebolish**  
NASA Software TV & V Facility  
100 **University** Drive  
**Fairmont**, West **Virginia** 26554

Mr. Harold R. Shaffer  
Senior **Director**, Advanced Signal Systems  
**CSX Transportation, Inc.**  
500 Water SL  
Jacksonville, **EL** 32202

Mr. John T. **Sharkey**  
**Engineer/Signals**  
**Illinois** Central R. R. Co.  
455 North **Cityfront** Plaza Dr.  
Chicago. **IL** 60611-5504

Mr. Thomas D. **Simpson**  
**Vice President**  
Rail **Progress** Institute  
700 N. **Fairfax** St Suite 601  
**Alexandria, VA 22314**

Mr. G. **J. Sniffen, Jr.**  
Assistant Vice President  
Communications and Signals  
Norfolk Southern  
**185 Spring St., S.W**  
Atlanta, GA 30303

Mr. David **Tadlock**  
NASA • **JSC**  
Mail Code **EK12**  
**2101 Nasa Road**  
Houston, **TX 77058**

Mr. Stanley R. Taylor  
Signal Engineer  
The **Kansas** City Southern Railway Co.  
**4601 Blanchard Rd.**  
**Shreveport, LA 71107**

Mr. Glenn **Voss**, Assistant Chief Engineer  
Signal, Communication and Power  
Long Island Rail Road Co.  
Jamaica **Station**  
Jamaica, NY **11435**

Salem **Wahby**  
**ABB** Traction  
East 18th **Street**  
**Elmira, NY 14903**

Mr. Glen **Wilson**  
**Vice President** and Chief Technology Officer  
**Safetran** Systems Corporation  
**10655, Seventh Street**  
Rancho **Cucamonga, CA 91730**

Mr. Richard Van **Woerkom**  
National Transportation Safety Board  
**490 L'Enfant Plaza East, S.W**  
Washington, **DC 20594-2000**

Mr. Jaime **Zamlung**  
Executive Vice Resident  
CMW Systems, Inc.  
**15260 Ventura Blvd., Suite 800**  
Sherman Oaks, CA **91403**



OCT 12 1994

To: Jeffrey E. Gordon

From: Lang Nguyen

Subject: State-of-the Art and Assessment of Safety  
Verification/Validation Methodologies (for the Base Task)

The following corrections should be made in **Appendix A: Acronyms**, p. A1. This information can be verified through this reference source: "Acronyms, Initialisms & Abbreviations Dictionary, Nineteenth Edition by Jennifer Mossman, Editor, published by Gale<sup>a</sup>.

ASC - Automatic Speed Control  
 BR - British Railways  
 CAD - Computer Aided Design  
 DB - Deutsche Bundesbahn (German Federal Railway)  
 DIN - Deutsches Institut fuer Normung (German Standard Institute)  
 DoD - Department of Defense  
 DTP - Department of Transport (England)  
 EN - European Norm (Issued by European Committee for Standardization)  
 ETSI - European Telecommunications Standard Institute  
 EUROCAE - European Organization for Civil Aviation Electronics  
 FAR - Federal Air Regulations  
 IEE - Institute of Electrical Engineers  
 SNCF - Société Nationale des Chemins de Fer  
 SRM - safety, Reliability, and Maintainability.

cc: Philip Olekzyk  
 William Goodman  
 William Paxton  
 Manuel Galdo  
 Robert Dorer

OPTIONAL FORM 99 (7-80)

## FAX TRANSMITTAL

To	JEFF GORDON	From	LANG NGUYEN
Dept/Agency	VOEPE	Phone #	202-366-0498
Fax #	617-494-3616	Fax #	202-366-7136
NSN 7540-01-317-7388		5010-101	
GENERAL SERVICES ADMINISTRATION			

SEP 20 1994

To: Jeffrey E. Gordon,

From: Lang Nguyen *Lang Nguyen*

Subject: Development of a Safety Validation Methodology (for the Option Task)

This Task was not well prepared due to the following reasons.

The two terms Verification and Validation are not defined by Battele even though they are framework for their project. Battele copied these terms by using IEEE definition in "Standard Glossary of Software Engineering Terminology" document (page 15). It is not a current document it has been published almost four year (1990).

The expression "It is believed that, in this program, the desired (safety validation) methodology is.." gave us an impression that Battele is still in doubt about the definition of safety validation methodology (page 16).

For the above reasons, the terms VERIFICATION, VALIDATION, THE SAFETY VALIDATION METHODOLOGY must be defined by Battele clearly, concisely since they are guidelines for this project.

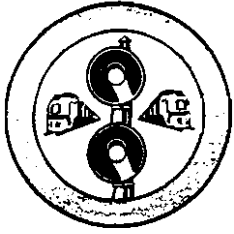
cc: Philip Olekzyk  
William Goodman  
William Paxton  
Manuel Galdo  
Robert Dorer

OPTIONAL FORM NO. (7-90)

FAX TRANSMITTAL

# of pages ▶ 3

To	JEFFREY GORDON	From	LANG NGUYEN
Dept./Agency		Phone #	202-366-0498
Fax #	617-494-3686	Fax #	366-7136
NSN 7540 01 317-7368		5099 101 GENERAL SERVICES ADMINISTRATION	



# Brotherhood of Railroad Signalmen

601 W. GOLF ROAD  
BOX U  
MOUNT PROSPECT, ILLINOIS 60056  
PHONE: 708-439-3732  
FAX: 708-439-3743

W.D. "DAN" PICKETT  
PRESIDENT

R.R. FOLEY  
SECRETARY-TREASURER

September 26, 1994

Mr. Jeffrey E. Gordon  
Research and Special Programs Administrator  
U.S. Department of Transportation  
Volpe National Transportation Systems Center, DTS-76  
55 Broadway  
Kendall Square  
Cambridge, MA 02142

Dear Mr. Gordon:

We have reviewed both FRA reports concerning Base Task and Opinion Task for "Analytical Methodology for Safety Validation of Computer Controlled Subsystems Used in Guided Ground Transportation Systems." The Brotherhood of Railroad Signalmen is encouraged that the FRA has initiated an active investigation of this critical safety aspect of the nation's transportation system. Software-driven railway signaling and train control equipment is being developed and integrated into existing systems at a rapid pace. The assurance of the safety of such critical computer-based railroad control equipment through a uniform process is long overdue.

The FRA is to be commended for the research efforts. Based on a preliminary review, the research into present forms of "Safety Verification/Validation Methodologies" appears to be comprehensive in nature and well organized. Additionally, the inclusion of a Training Program Plan section in the report addresses an aspect that has long been overlooked. The report also points out that requirements developed in the United States under ATCS Spec 140, while fairly comprehensive in nature, fail to assure sufficient levels of safety in the areas of latent failures and hardware or software modifications as well as other areas.

The report appears to confirm concerns being expressed by BRS members working in this field. Among those concerns is the lack of sufficient, uniform methods of testing software-based safety sensitive signal equipment, whether it be grade crossing warning

Mr. Jeffrey E. Gordon  
September 26, 1994  
Page 2

devices or train control equipment, for safe operation when installed, modified or repaired.

Signalmen are charged with the difficult task of installing, maintaining and assuring the safety of these highly diversified computer based train control and signalling systems. Obviously, safety assurance and efficient operation of such systems are not only of immense importance to this organization, but ultimately have an impact on the general public as well.

Thus, we encourage the FRA to proceed forward with a project to establish standard safety procedures for the verification/validation of critical computer-based railroad control systems. We would highly recommend that any such procedures apply to the initial design, installation, modifications and repair of such equipment, and that periodic testing be required throughout the equipment's operational life to ensure proper operation. We also recommend that such procedures address integration testing and system testing of all such software-based systems and associated subsystems.

The Brotherhood of Railroad Signalmen further recommends the formation of an advisory committee to study and recommend a uniform validation process for safety-critical software used in railroad control systems. A committee consisting of knowledgeable representatives from concerned parties such as the FRA, the High-Speed Rail Association, the American Association of Railroads, railroad train control equipment manufacturers and the BRS could provide valuable input into any attempt to develop a uniform validation process for U.S. railroads.

In conclusion, this organization would welcome the opportunity to participate in the development of any formal standards for such safety sensitive equipment.

Sincerely,



W.D. Pickett  
President

cc: Jolene Molitoris, FRA Administrator  
Bruce M. Fine, FRA Associate Administrator  
Claire L. Orth, FRA Office of Research and Development

September 26, 1994

Mr. Jeffrey E. Gordon  
U. S. Department of Transportation  
Research and Special Programs Administration  
Volpe National Transportation System Center, DTS-76  
55 Broadway  
Kendall Square  
Cambridge MA 02142


Subject: Review of the Software Safety Validation Methodology

Dear Mr. Gordon,

Enclosed is a review of the software safety validation methodology reports. These reports included an extensive review of the evolving art of the validation techniques for safety critical computer controlled systems in many industries. As noted in the documents, the safety validation for critical software is still evolving across multiple industries, at different rates, and with conflicting terminology. Enclosed are:

1. A few specific comments on the "State of Art and Assessment of Safety Verification / Validation Methodologies!"
2. Comments and recommendations on "Development of a Safety Validation Methodology:"
3. General recommendations, comments, and suggestions on future efforts.
4. Copy of a Hazard Prevention article "Software Safety - Less Successful Techniques and How to Mitigate Them" on some of problems encounter in performing software safety on a space program.

An additional suggestion is that this effort be considered by the Intelligent Transportation Systems (Formerly IVHS) as an integrated approach towards software for safety critical applications for ground transportation systems.



Jim Bullough-Latsch  
Computer Diet and Maintenance Systems

CC: Intelligent Transportation Society (Formerly IVHS - America)  
Software Safety Team

Comments on "State-of-the-Art and Assessment Of Safety Verification/Validation Methodology"

Table 3-1

**ANSI/IEEE**

IEEE 1228-1994 was released this year.

US Air Force

AFSIC SSH-1 Software System Safety, 5 September 1985. should be used as a source for two reasons: it is the oldest handbook available and it forms the foundation for several of the other standards referenced.

NASA

1740.13 Software Safety Standard was released as an interim NASA Standard

SSP 30309 "E" is in draft form

SSP 50038 The approach of International Space Station Alpha's "Computer-Based Control System Safety Requirements" should be a candidate for consideration in the follow on assessment.

Section 4.2.2.3 Attributes and Limitation

The assessment appears to assume that these standards and verification methods are fully followed by software developers and safety engineers. For many safety critical software systems, that is not the case, there are usually significant real life problems that make a significant portion of these standards "goals". It is suggested that a follow on investigation of the "problems, restriction and experience" be perform, and a section 4.2.2.4 be added including these results.

Comments on "Development of A Safety Validation Methodology"

## 5.0 Recommended Safety Verification Methodology

### 5.2 General Safety Requirements

Recommend adding "Software Failure" as a cause.

#### 5.3.2.1.1 Software Safety Requirements Specification Verification

Suggest this is more of a review than a verification.

If this is done as part of the development life cycle, the requirements are usually incomplete. How should this limitation be accommodated?

#### 5.3.2.1.2 Software Design Verification

How will the use of commercial-off-the-shelf (COTS) software be addressed?

One of the most fruitful design techniques (from the safety verification approach) is to isolate the safety critical software to a few modules and routines or in more complex systems to a subset of the processors in the system.

#### 5.3.2.1.3 Software Code Verification

How should incremental code releases be handled?

Automated tools to support safety analysis of software have not meet the level of confidence implied here.

Another reason for reviewing code to assess the unintended side effects.

#### 5.3.2.1.5 Software Integration Testing

One of the more effective areas to investigate for possible adverse safety effects are developmental engineering anomalies. Particularly transient failures or can not duplicate problems should be investigated.

## 7.0 Training Program Plan

### 7.2 Training Course Approach and Content

Section 7.2 should include some assumptions on the background (prerequisite) of the trainee. In other disciplines, when attempting to train to address software safety, there have been experienced safety engineers trying to adjust to software safety; software engineers trying to learn safety; junior engineers and inspector trying to learn both; software product assurance (quality) engineers try to expand the their background, and

mangers just sampling. A detailed understanding of the issues and concerns was beyond the background of the audiences. One of the biggest problems with most of the current approaches to software safety is that it takes a strong understanding of software techniques, safety techniques, and a full understanding of the end application (*i.e.* the superman syndrome).

Table 7.1 Include a module on real-time computer systems operations, and definition.

### 7.5.3 Student Workbook

Having the workbook include copies of some the recent standards and recommended checklist helps the student and instructor to focus the efforts. Also is **makes the** manual more usable after the course. DO-178B is still my favorite for general software safety, and EIA-6B as a checklist for simple software.

### 7.6.3 Certificate of Achievement

For effective safety program, a certification should require more than just a short course. Suggest it should include a hands-on team safety assessment of a system to a reasonable level.

## 8.0 Human Factor Aspects

### 8.3.3.6 Understanding Automation

This is a major concern and potential problem.

One of the possible differences between some of rail applications and the other recent applications of computer to safety critical systems is the level of operator training. In many other applications (Space, Aerospace, Nuclear, and Medicine, and Military) there is a very heavy emphasis on the training and certification of the operators. For untended systems such as rail signals, this imposes an **unusually** (newj application of software for critical systems. For train crews, I am unable to judge if this should be an issue or not.



## General Comments, Questions and Recommendations

1. Are there significant differences between computer system for the rail industry from other industries? If so what are they?
2. Low cost alternative: Given then initially voluntary approach toward "software safety validation", could the goals for the next five years (until 1999) be achieved by the application of ISO 9000 for software development (Quality), the IEEE 1228-1994 (recent released) for software safety planning, and the use of some FRA provided check lists.
3. What are the difference between the Rail Industry and the Highway Industry for the next ten years?
4. Or more generally, should there be an Department of Transportation System Safety Handbook?
5. Comment: Successful use of standards versus intent. Suggest that an interesting and productive follow on research tasks would be collect some of the problems associated with applying these software safety standards to real systems. Many safety critical computer controlled applications do not meet all of the goals in the standards.
6. Another major problem is reliable data on hazardous computer failures. Several case studies have been published, but few statistics are available.
7. Future updates of this effort should consider including some of the sample checklists. Two types are recommend: 1. Examples that will provide in sight into rail safety concerns for computer professionals; 2. Examples that will demonstrate the intended scope of computer and software effort to the rail industry.
8. "Evaluating Software Engineering Standards," IEEE Computer, September 1994, describes some significant difficulties with software standards that should be considered with this effort.
9. National Institute of Standards (NIST) performed a similar review for the nuclear industry documented in NIST SP500-204, NUREG/CR-5930 (December 1992). This should be reviewed as a cross check.
10. It appears that common terminology for software safety should be addressed via some forum. Will the DOT recommend this to the IEEE?

THE AEROSPACE CORPORATION



Post Office Box 92957, Los Angeles, California 90009, Telephone: 213-336-3044

November 3, 1994

Federal Railroad Administration  
Office of Research and Development, RDV-31  
400 7th St. SW  
Washington D.C. 20590

Attention: Mr. Manuel Galdo

It was a pleasure meeting with you and others in the **Office** of Research **and** Development last week. At your request, I've written down my comments on the **report** titled, "**Development** of a Safety Validation Methodology," authored by Batkille, **presented** to the **Volpe National** Transportation Systems Center, and dated April 13, 1994. **As** I **indicated** during my **discussion** with you, my **overall** impression of this document is very favorable. I believe the **recommendations** presented by **Battelle** are based on a good technical foundation, and the methodology **is** a **reasonable** approach.

My **comments** reflect a review that **was** targeted at **assessing** the high-level **objectives** of **this method-ology**. Please feel free to contact me regarding any **questions** or further elaboration on these comments.

Also, I've also **enclosed** a subset of a list of questions (Software Development Capability Evaluation) that we use to evaluate the software safety capability of software development suppliers. You had **expressed** some interest in this list.

Best regards,

Charles H. Lavine

Enclosures: Development of a Safety Validation Methodology review  
Software Development Capability Evaluations questions for **software** Safety

cc: J. Sifer (Aerospace)

Comments on the report titled, 'Development of a Safety Validation Methodology,' developed by **Battelle** for the Volpe **National** Transportation System Center, **and** dated **April** 13, 1994.

Page **18**, Section **4.1.3 FRA's** Role and Intent of Methodology:

This methodology is intended **to** be a "recommended practice" for suppliers, yet, this section states that **an after-the-fact** audit may be **performed** after an accident to determine compliance with the methodology. I don't think that compliance can be determined without **metrics** or common practice experience that is used throughout the industry. One supplier may implement the methodology much differently than another supplier. Also, my experience has been that suppliers will interpret the methodology to accommodate their already established practices. I understand the desire not to enforce to the methodology, but some guidance will be required to establish common industry practice.

Page **18**, Section **4.1.4** Nature of the Methodology:

In my opinion, the industry input cycle is **necessary**.

Page **19**, Section **4.1.5** Applicability of **the** Methodology:

I **agree** with the decision not to **impose** design **philosophies**. **Designs** should be evaluated on their **own** merits for the intended operating **environment**. However, criteria or an approach that **defines** what **is a** reasonable design should be developed.

Page **20**, Section **4.1.5** Applicability of **the** Methodology:

I believe this **section** implicitly suggests that this methodology be limited to computer software and hardware and a few other system safety aspects, but not the entire system. When **assessing hazards**, I believe this approach may be problematic. In fact, it was a **similar** approach used in **MIL-STD-882B** (isolating the software hazard analysis from the rest of the system) that prompted a rewriting and update to **MIL-STD-882C**. A hazard analysis should be done in a system context. Since nearly all hazards are a combination of several actions throughout the system occurring in a particular sequence or simultaneously, the system must be evaluated as a whole.

Page **21** (second paragraph), Section **4.1.6.1** Level of Safety:

Not only are there no widely accepted metrics for quantifying software errors, it has been shown that software reliability is not tightly coupled with software safety. In fact, it is **difficult** to determine to what extent one affects the other. This was reported by Herbert Hecht at the **NIST** sponsored **1993** Compass (Computer **Assurance**) conference.

Page **22**, Section **4.1.7** Safety **V&V** Vs. Hazard **Analysis/Risk** Assessment:

When I hear the term formal methods, I infer that mathematical proofs are used. Although MOD 00-55 does recommend the use of **formal** methods, it is only for highly critical system software.

Page **23**, Section **4.1.8** Safety Inherently **Levels**:

The Aerospace Corporation is **currently** developing a set of **integrity** levels applied to **space systems' software**. I will be glad to **share this** information when it is approved by the Air **Force** for **wider** release.

One **difficulty** we're currently addressing is the aggregation of **multiple system components (separate products)** at varying integrity **levels**. We've recognized that some mrt of **composition "rules"** must **exist** to achieve an overall integrity level. This topic should be discussed in **this** section of **this** report.

*Page 26, Section 4.2.1.2 Software Developmnt Process:*

Choosing ISO-9001-3 is a good choice.

*Page 27, Section 4.2.2 Safely Management:*

This section is a bit confusing. Up to this point in the document, software safety has been the main **focus**. In this section, the focus seems to shift from discussing the *software safeiy process* to the *system safeiy* process. Consequently, the discussion progresses from the safety process, to the integration of the system safety **process**, to the development of the system. While I **agree** with the information that is provided in this section, I believe the concerns of the **software** safety **process** and integrating **software** aafety into the software development **process** need to be **addressed**.

*Page 27,28,29, Section 4.2.2 Safely Managemeni:*

In addition to the process and key steps to this process, I think the **FRA** should **propose** certain products that result from these steps. The **FRA does not** have to specify how to perform **each step**, but you can **specify** the **information** that should be derived **from** the step. Additionally, if you plan to perform an audit at any time during or after development of the **system**, evidence that the step was performed and **satisfactory** results were obtained should be provided by the supplier.

*Page 34, Figure 5-1. Safeiy V&V Methodology Activities:*

This figure illustrates a dual approach methodology, with one side of the house developing hardware; and the other side of the house developing software. Along with these separate development activities, separate hardware and software verification and validation activities are proposed. While **some** verification activities must be targeted to either software or hardware, many verification activities should be performed on the hardware and software together. As **I** discussed in my comment for page 20 above, I believe there are some inherent difficulties with this approach.

*Page 35, Section 5.3.2 Software Safely V&V Activities:*

The second paragraph in this section recommends that a development phase be ended and a **success-ful** verification activity be completed before entering into the next development phase. I don't think this **is** a realistic expectation. In many development environments, there is not a **clear** separation between development phases (**regardless** of management declarations that a different phase **has been** entered). Many of the issues from one phase may not be closed before another phase begins. In fact many issues may span the the entire development cycle. **What** should be emphasized is an **effective** problem tracking mechanism to make sure that safety-relevant issues are properly addressed before

being closed.

*Page 36, Section 5.3.2.1 Software Safety Verification:*

It is important to state that a safety verification should be performed at various development phases. However, just stating this, will do little to advance software safety verification. The interpretation of this statement will vary widely throughout the railroad industry. Improved software safety technology will be achieved through the communication of successful efforts between suppliers. The FRA can be instrumental in providing these communication channels. The FRA should seek out and document effective verification efforts to provide guidance to suppliers, and then encourage suppliers to use proven techniques.

*Page 37, Section 5.3.2.1 Software Safety Verification:*

The second paragraph discusses software redundancy as an example of where software verification may not be necessary because the design philosophy ensures safety. I disagree with the idea that a verification can be waived for this reason. The example provided in the report demonstrates this. Even though software redundancy is used, software safety may not be improved. First, it is not clear that software redundancy improves safety. Second, the supplier may have little experience in developing such systems, and may in fact increase risk to the system by a) introducing complexity, and by b) improperly implementing software redundancy. I don't think that waiving verifications because of design philosophy should be advocated.

*Page 37, Section 5.3.2.1.1 Software Safety Requirements Specification Verification:*

This section suggests that requirements be verified using manual techniques. Automated/semi-automated techniques for requirements specification verification exist and are very useful. In some cases, not using automated techniques may be negligent.

*Page 40, Section 5.3.3 Hardware Safety V&V Activities:*

I do not see a reason for discussing hardware in this document. Although the title of the document says that this is a safety validation methodology, in reality it is focused on software safety and in general is not applicable to computer hardware or other system hardware. We do not need to consider hardware either for safe design criteria or for verification techniques to ensure that safety was properly addressed. For hazard analysis, hardware and software must be considered together as a system, but a document providing a software safety methodology needs to address only the software interface to the hardware. Another document discussing computer hardware should be considered separately.