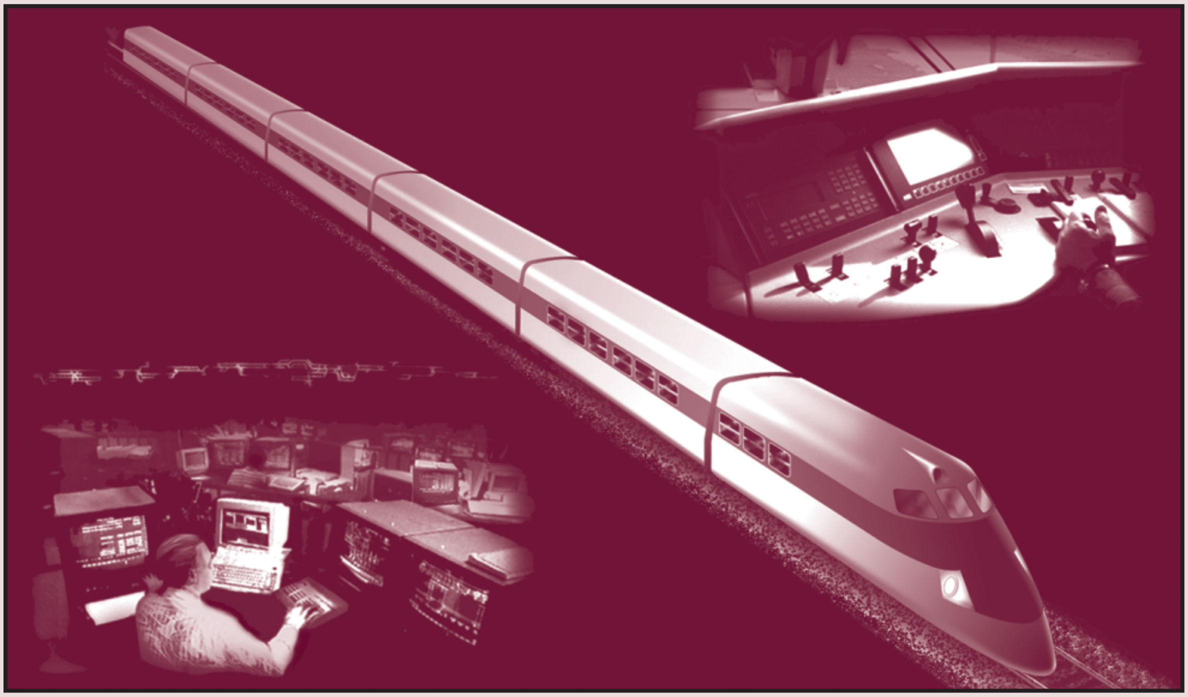
U.S. Department
of Transportation

**Federal Railroad
Administration**

Human Factors Considerations in the Evaluation of Processor-Based Signal and Train Control Systems

Office of Research
and Development
Washington, DC 20590



Human Factors in Railroad Operations

DOT/FRA/ORD-07/07

Final Report
June 2007

This document is available to the
public through the National Technical
Information Service, Springfield, VA 22161.
This document is also available on the
FRA Web site at www.fra.gov.

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Notice

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

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 aspects of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for information Operations and Reports. 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA. 222202-4302, 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 June 2007	3. REPORT TYPE AND DATES COVERED September 2003-September 2004

TITLE AND SUBTITLE Human Factors Considerations in the Evaluation of Processor-Based Signal and Train Control Systems: Human Factors in Railroad Operations	5. FUNDING NUMBERS RR04/CB101
AUTHOR(S) John Wreathall, Emilie Roth, Dennis Bley, and Jordan Multer	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Department of Transportation John A. Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142-1093	8. PERFORMING ORGANIZATION DOT-VNTSC-FRA-07-05
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Transportation Federal Railroad Administration Research and Innovative Technology Administration 1120 Vermont Avenue, NW Mail Stop 20 Washington, DC 20590	10. SPONSORING/MONITORING AGENCY REPORT NUMBER DOT/FRA/ORD-07/07
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public through the National Technical Information Service, Springfield, VA 22161. This document is also available on the FRA Web site at www.fra.dot.gov.	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

In August 2001, the Federal Railroad Administration issued the notice of proposed rulemaking: Standards for Development and Use of Processor-Based Signal and Train Control Systems (49 Code of Federal Regulations Part 236). This proposed rule addresses the design and implementation of processor-based train control systems. Under the proposed rule, a railroad wishing to implement a positive train control (PTC) system in revenue service must develop and submit a product safety plan (PSP) and assess the risk associated with the new system.

This report attempts to fill the gap provided by the lack of knowledge about the kinds of human performance challenges and safety risks that will occur with these proposed systems. To fill this gap, the authors identified human factors issues that arose in other industries where similar kinds of technology and human-machine interfaces were used. This literature review, along with an analysis of PTC-preventable accidents, served as the basis for structuring interviews with employees at several railroads that had experience with train control technology containing elements of PTC. The answers to these questions provide the reader with a roadmap of human performance issues to consider in preparing or evaluating a PSP, along with the implications for risk.

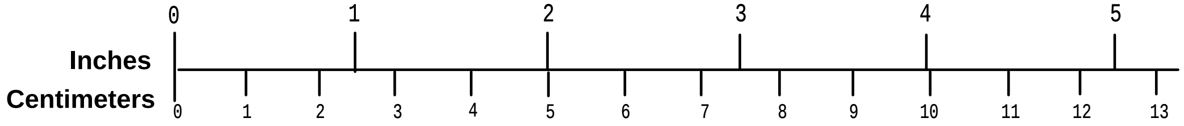
14. SUBJECT TERMS Cognitive task analysis, communications, decisionmaking, human factors, human reliability analysis (HRA), positive train control (PTC), probabilistic risk assessment (PRA), railroad operations	15. NUMBER OF PAGES 160 16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	LIMITATION OF ABSTRACT Unclassified

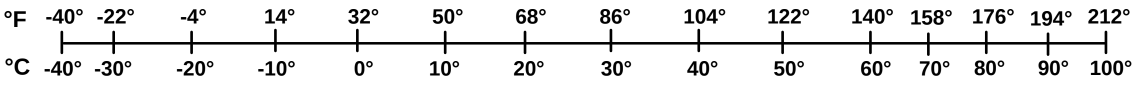
METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC		METRIC TO ENGLISH	
LENGTH (APPROXIMATE)		**LENGTH** (APPROXIMATE)	
1 inch (in)	= 2.5 centimeters (cm)	1 millimeter (mm)	= 0.04 inch (in)
1 foot (ft)	= 30 centimeters (cm)	1 centimeter (cm)	= 0.4 inch (in)
1 yard (yd)	= 0.9 meter (m)	1 meter (m)	= 3.3 feet (ft)
1 mile (mi)	= 1.6 kilometers (km)	1 meter (m)	= 1.1 yards (yd)
		1 kilometer (km)	= 0.6 mile (mi)
AREA (APPROXIMATE)		**AREA** (APPROXIMATE)	
1 square inch (sq in, in^2)	= 6.5 square centimeters (cm^2)	1 square centimeter (cm^2)	= 0.16 square inch (sq in, in^2)
1 square foot (sq ft, ft^2)	= 0.09 square meter (m^2)	1 square meter (m^2)	= 1.2 square yards (sq yd, yd^2)
1 square yard (sq yd, yd^2)	= 0.8 square meter (m^2)	1 square kilometer (km^2)	= 0.4 square mile (sq mi, mi^2)
1 square mile (sq mi, mi^2)	= 2.6 square kilometers (km^2)	10,000 square meters (m^2)	= 1 hectare (ha) = 2.5 acres
1 acre = 0.4 hectare (he)	= 4,000 square meters (m^2)		
MASS - WEIGHT (APPROXIMATE)		**MASS - WEIGHT** (APPROXIMATE)	
1 ounce (oz)	= 28 grams (gm)	1 gram (gm)	= 0.036 ounce (oz)
1 pound (lb)	= 0.45 kilogram (kg)	1 kilogram (kg)	= 2.2 pounds (lb)
1 short ton = 2,000 pounds (lb)	= 0.9 tonne (t)	1 tonne (t)	= 1,000 kilograms (kg)
			= 1.1 short tons
VOLUME (APPROXIMATE)		**VOLUME** (APPROXIMATE)	
1 teaspoon (tsp)	= 5 milliliters (ml)	1 milliliter (ml)	= 0.03 fluid ounce (fl oz)
1 tablespoon (tbsp)	= 15 milliliters (ml)	1 liter (l)	= 2.1 pints (pt)
1 fluid ounce (fl oz)	= 30 milliliters (ml)	1 liter (l)	= 1.06 quarts (qt)
1 cup (c)	= 0.24 liter (l)	1 liter (l)	= 0.26 gallon (gal)
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^3)	= 0.03 cubic meter (m^3)	1 cubic meter (m^3)	= 36 cubic feet (cu ft, ft^3)
1 cubic yard (cu yd, yd^3)	= 0.76 cubic meter (m^3)	1 cubic meter (m^3)	= 1.3 cubic yards (cu yd, yd^3)
TEMPERATURE (EXACT)		**TEMPERATURE** (EXACT)	
[(x-32)(5/9)] °F	= y °C	[(9/5) y + 32] °C	= x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSION



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

Updated 6/17/98

PREFACE

In August 2001, the Federal Railroad Administration (FRA) issued the notice of proposed rulemaking: Standards for Development and Use of Processor-Based Signal and Train Control Systems (49 Code of Federal Regulations Part 236). This proposed rule addresses the design and implementation of processor-based train control systems. Under the proposed rule, a railroad wishing to implement a positive train control (PTC) system in revenue service must develop and submit a product safety plan (PSP) and assess the risk associated with the new system.

Submitting this information will require knowledge of the human-machine interface (HMI) and its impact on human performance. Similarly, FRA will require knowledge of HMI and its impact on human performance to evaluate the safety of the new system. The first system expected to fall under the proposed rule is the North American Joint Positive Train Control (NAJPTC) system. This PTC system differs significantly from train control systems that have come before it. The NAJPTC system is a complex train control system that will significantly alter the current method of operation. This change in operation will significantly alter the way railroad employees interact with the train control system and may create the potential for a variety of new failure modes.

The current report provides guidance to the railroad industry, specifically to those people who must submit human factors analyses of HMI as part of the PSP and to FRA staff, which must evaluate those analyses. The challenge for the railroad is to identify how these new systems or components will affect human performance, identify new failure modes, and address how to prevent or mitigate these failure modes. FRA must decide whether the human factors analysis has identified all the potential human factors-related safety risks and addressed them in a satisfactory way.

This report attempts to fill the gap provided by the lack of knowledge about the kinds of human performance challenges and safety risks that will occur with these proposed systems. To fill this gap, this report identifies human factors issues that arose in other industries, such as aviation and nuclear power, where similar kinds of technology and human-machine interfaces were used. This literature review, along with an analysis of PTC-preventable accidents, served as the basis for structuring interviews with employees at several railroads that had experience with train control technology containing elements of PTC. The answers to these questions provide the reader with a roadmap of human performance issues to consider in preparing or evaluating a PSP, along with the implications for risk.

As knowledge about these technologies grows and experience using the new HMIs increases, it will become easier to identify potential safety risks and evaluate the solutions for addressing them.

ACKNOWLEDGMENTS

The Federal Railroad Administration's Office of Research and Development funded this research effort. We would like to thank FRA's Office of Research and Development for the opportunity to advance the state of knowledge in assessing human reliability and risk in the use of positive train control systems. We would like to thank Dr. Thomas Raslear, Senior Human Factors Program Manager, for his support and guidance.

We would like to acknowledge a number of individuals who generously provided their time and support. We would like to thank Alan Polivka, Communications & Train Control Technologies General Manager North American Joint Positive Train Control (NAJPTC) Project Transportation Technology Center, Inc., and Dan Steinhoff, Union Pacific, for providing us the opportunity to ride a test train during one of the early NAJPTC field tests that was conducted in Bloomington, IL, on October 29, 2002, and sharing their insights. We are particularly grateful to Bill Moore Ede, CANAC; Dennis Sutherland and Keith Sutherland, Westinghouse Air Brake Technologies Corporation (Wabtec); Christopher Goeren and Martin Bogdahn, Lockheed Martin; Mark Ryan, Union Pacific, and Mark Burris, Amtrak, for sharing their knowledge of the NAJPTC system, the technical challenges faced, and lessons learned from early experiences with the system.

We would like to thank Bob Kollmar, Amtrak, for providing us the opportunity to learn about incremental train control system (ITCS) and the lessons learned from the system's development and implementation. We are grateful to Bob for arranging for us to get a head-end ride on an ITCS-equipped train and making available ITCS locomotive engineers, conductors, signalmen, electronic technicians, and maintenance-of-way workers to be interviewed in Chicago, IL, and Niles, MI. We would also like to thank Angela Brazzale of Amtrak for all the time and effort she put in to organize the interview meetings and for sharing her time and knowledge with us. Angela's broad perspective helped us to understand the motivation for the ITCS system, the phased development and implementation process, and lessons learned.

David Fernauld of Norfolk Southern provided particularly helpful information concerning the infrastructure of ITCS for freight operations. We would also like to acknowledge Jim Chiles, Locomotive Engineer, for agreeing to be interviewed by phone and sharing his experiences and perspective on the benefits and challenges of running an ITCS-equipped locomotive, particularly for freight operations.

We would also like to thank John Vogler, New Jersey Transit, who provided us the opportunity to interview Advanced Speed Enforcement System (ASES) locomotive engineers, signalmen, and mechanical department personnel. We also want to thank Jim Gee, Assistant Superintendent of Transportation, Ben Smith, Director of Technical Services, and Robert Milazzo, Director of Signal Maintenance, for generously sharing their time and insights, as well as for all their efforts in identifying and making available their personnel.

We would also like to acknowledge the national and local labor representatives of the Brotherhood of Locomotive Engineers (BLE), the United Transportation Union (UTU), the Brotherhood of Railroad Signalmen (BRS), the Brotherhood of Maintenance of Way Employees (BMWE), and the International Brotherhood of Electrical Workers (IBEW), for facilitating interviews of their members. We especially want to thank Bob Harvey, BLE; James Stem, UTU; Rick Inclima, BMWE; and Tim DePaepe, BRS, for communicating with their respective memberships in support of this project. We particularly want to acknowledge Bob Harvey for participating in the phone interview with Jim Chiles, and Rick Inclima and Tim DePaepe for traveling to Niles, MI, to participate in the ITCS interviews. The visible support of labor for this effort was important for reassuring the individuals that we interviewed that both labor and management was interested in their input and supported this work.

We would particularly like to thank the individual locomotive engineers, conductors, signalmen, maintenance-of-way workers, and mechanical department personnel who participated in the interviews and contributed their knowledge and insights.

We would also like to acknowledge Professor David D. Woods, Ohio State University, and Dr. Alan Bing, ICF Consulting, who, as part of a related FRA project, participated in some of the ITCS and ASES interviews and generously shared their insights with us.

From FRA's Office of Safety, we would like to thank Lonnie Ramos and Christopher Schulte for sharing data with us on train collision, derailments, and roadway worker accidents. Finally, we would like to thank Grady Cothen, Deputy Associate Administrator in FRA's Office of Safety for his support.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Since the early days of railroading, the railroad industry has introduced new technology to improve operating efficiency and safety. For example, the railroad industry was an early adopter of telephone and radio technology. As the railroads introduced multiple safety barriers (e.g., new technology, operating rules, training), safety improved but at the cost of increased system complexity.

While the absolute number of hazardous events in the railroad industry has decreased, the causal factors that contribute to unsafe events have changed. Since 1975, the percentage of reportable incidents and accidents attributable to human factors has increased from 24 percent to 38 percent in 2002. Knowledge about equipment-related failures has contributed to the design of more reliable equipment, reducing accidents attributable to system malfunctions. At the same time, the humans working in railroad operations now find themselves in a more complex system. Train crews, dispatchers, and roadway workers play a critical role by adapting to changing conditions that exist in the railroad environment. As the railroad environment becomes more complex, the opportunities for failure that involve human interactions also increase.

Positive train control (PTC) technology has the potential to address some of the failure modes involving the train crews, dispatchers, and roadway workers. The driving safety motivation for PTC systems has been to eliminate the kinds of fatal accidents that have occurred in recent years. They are intended to eliminate train-to-train collisions, to limit exceedance of speed restrictions, and to protect train crews and roadway workers. The National Transportation Safety Board (NTSB) identified over 100 collisions that may have been prevented if a fully implemented PTC system had been in place. The Federal Railroad Administration (FRA) has encouraged the railroads to develop and deploy such systems, provided that they demonstrate a net positive effect on risk.

PTC technology generally has the potential to improve safety because it provides a layer of additional protection beyond that provided by the train crews and dispatchers. However, PTC technology also adds another layer of complexity that may introduce new risks. PTC technology uses new modes of train control that can potentially impact train crew and dispatcher performance. It also employs new technology that may introduce new challenges for system maintainers. The question for railroads seeking to introduce this safety-critical technology is whether the overall safety risk is equal or better than the technology it replaces.

In August 2001, FRA issued the notice of proposed rulemaking: Standards for Development and Use of Processor-Based Signal and Train Control Systems (49 Code of Federal Regulations Part 236). This proposed rule addresses the design and implementation of processor-based train control systems. Under the proposed rule, a railroad wishing to implement a PTC system in revenue service must develop and submit a product safety plan (PSP) and assess changes in the risks associated with the new system compared with the previous methods of train control.

Submitting this information will require knowledge of the human-machine interface (HMI) and its impact on human and system performance. Similarly, FRA will require knowledge of HMI and its impact on human performance to evaluate the safety of the new system.

In assessing the changes in risk from use of the PTC system, the risk assessment tools chosen must demonstrate sensitivity to the effects of the changes in system and human performance associated with the new system. In particular, PTC systems currently in design or anticipated will affect primarily human-system interactions. Specifically, significant changes in safety and risk will arise from the ways that PTC systems address the major contributors to the kinds of accidents that the systems are intended to prevent. Thus, the probabilistic risk assessment (PRA) must focus on the specific factors seen in the reviews of accidents of concern.

The first system expected to fall under the proposed rule is the North American Joint Positive Train Control (NAJPTC) system. This PTC system differs significantly from previous train control systems. The NAJPTC system is a complex train control system that will significantly change the current method of operation and the way railroad employees interact with the train control system and may create the potential for a variety of new failure modes.

This report provides guidance to the railroad industry, specifically to those people who must submit human factors analyses and PRAs of HMI as part of the PSP, and to FRA staff which must evaluate those analyses. The challenge for the railroad is to identify how these new systems or components will affect human performance, identify new failure modes, and address how to prevent or mitigate these failure modes and the resulting changes in risk. FRA must decide whether the human factors analysis and the PRA have identified all the potential human factors-related risks and addressed them in a satisfactory way.

The study underlying this guidance has examined the interactions between train crews, dispatchers, roadway workers, and the new PTC systems to determine if the designs can create situations that can set the operators up to place the trains, workers, or public at risk (i.e., could the systems actually decrease safety?). The study also examined if human factors and operational aspects of existing PTC systems may reduce the effectiveness of PTC systems in accomplishing these functions or create additional safety concerns.

This study used a three-step process. First, the staff reviewed the literature to identify human factors issues that arise in the development and use of signal process related technologies (i.e., computer and communications technology) in related industries. Based on this review, the staff identified a list of human factors issues to pursue further. Using this list as a starting point, the staff analyzed a series of accidents that could potentially be prevented by PTC systems to assess the failure modes (risk factors) associated with these accidents. The information from both of these activities contributed to a list of questions needed for the third step, where the staff visited many sites of several of the railroads that are using PTC systems on a test basis, including the advanced civil speed enforcement system, advanced speed enforcement system, computer-based train system, and incremental train control system, as well some of the trials of the NAJPTC system.

Based on this process, the following are potential areas for evaluation:

- The braking curve used by PTC systems to ensure the train will stop before its limit of authority or meet speed limit requirements is often conservative—that is, trains must be slowed sooner than an experienced engineer would. This will require train crews to adopt new operating strategies to avoid unnecessary penalty brakes. Unnecessary penalty brakes can contribute to safety problems because they become nuisances to the crews, increasing the likelihood of the system being bypassed. In addition, penalty brakes can lead to trains being stopped in inappropriate locations (on grade crossings or interlockings, or heavy freight trains on uphill grades) that result in systemwide problems, again increasing a tendency to bypass use of the system.

- Manual interactions with the PTC system or use of its in-cab displays can distract train crews from maintaining awareness outside the cab. One example is the use of the countdown-to-penalty-brake displays that engineers closely follow (particularly inexperienced ones). A second interaction is the manual entry of data into the PTC system to describe the train consist (which determines its braking characteristics). Manual entry errors have the potential for braking to be too severe with the risk of derailment during the penalty brake.
- With increasing general use, the systems can become over relied upon, leading to inattention by the crews and problems when it is no longer available. While primarily intended as an overlay system, where safety relies initially on the engineer's own skills, it is known that, operationally, people will behave as if it were a line of defense against accidents. An accident at Southall (UK, September 1997) occurred when a PTC-like system was non-operational on a train, and the driver missed a sequence of signals because he was preoccupied with preparing for the end of his trip.
- The use of the one-size-fits-all aspect of the braking algorithms in PTC systems will act to decouple the experience of the engineer from the handling of the train, which is currently a very skilled task and tracks many complex factors. For example, the PTC system in one railroad was found to add about 7 percent to the duration of commuter service journeys, compared with service before use of the PTC system. This may be expected to reduce the efficiency of the rail service and could become a pressure to bypass the system.
- The potential exists for problems as personnel and equipment transition in and out of PTC service. Equipment may physically transition in and out of covered areas; staff may work on PTC-equipped locomotives one day and not the next, and so on. Issues that are associated with these transitions include crews maintaining awareness of whether the PTC system is operational or not, as well as ensuring that crews maintain an adequate level of experience and training when they use the system only occasionally.
- The location of the PTC system displays can have the potential to be a problem for locomotive crews to see the displays. With two-man cab operations, both crewmembers must back each other up. However, some displays are unreadable by the second person in the cab (usually the conductor) because of the location and size of the display.
- Certain PTC systems combine displays from different locomotive systems, and these may be in conflict. For example, displays may indicate different speed limits concurrently. It now becomes a burden on the train crew to resolve such inconsistencies.
- PTC systems enforce rules of the railroads over which the trains travel; journeys made by operators such as Amtrak may involve operating in territories with different rulebooks. In such cases, it is possible that rules associated with PTC systems may be

different in the different territories. New or inexperienced engineers may find that trying to apply the appropriate rules for each territory to be significant source of workload and distraction.

- Equipment used in PTC systems may involve new technologies for maintenance staffs. The rules will require sufficient training and support (e.g., specialized diagnostic and test equipment, availability of appropriate maintenance manuals, and general vendor support) to ensure the new systems achieve a satisfactory level of availability, both to prevent faults leading to a lack of respect for the equipment in the eyes of the users, and to ensure an adequate availability such that it is not routinely bypassed because of failure.
- With more failures of complex systems, it can often happen that fault diagnosis involves multiple crafts and departments, often across shifts. This can involve more complex coordination and communications than are often seen in typical railroad maintenance departments. In addition, often with new systems, a period occurs where it seems that these systems require a disproportionate amount of maintenance (somewhat of a burn-in process). This can result in resources not being available for maintenance activities of normal systems.
- Use of software-based systems, like PTC, require version control procedures to ensure that only the approved versions of software are in use. While many railroads may use software control for central (static) functions like dispatching, maintaining software control on objects like locomotives may be more problematic.
- The need for testing and maintenance of PTC devices, particularly those located out in track areas (e.g., track-located transponders), can potentially result in increased exposure to signal repair personnel, particularly if such equipment has initial reliability concerns.
- Finally, well-established practices exist for testing and deploying new technologies into work settings to reduce the likelihood of confusion, sources of errors, or sources of distraction. These include person-in-the-loop testing, gradual implementation of designs, and the use of extensive feedback from users. The extent to which such techniques have been used for specific PTC designs will provide an effective measure of the degree that the above concerns are mitigated or eliminated.

1. Introduction

1.1 Background

Since the early days of railroading, the railroad industry has introduced new technology to improve operating efficiency and safety. For example, the railroad industry was an early adopter of telephony and radio technology. As the railroads introduced multiple safety barriers (e.g., new technology, operating rules, training), safety improved but at the cost of increased system complexity.

While the absolute number of hazardous events in the railroad industry has decreased, the causal factors that contribute to unsafe events have changed. Since 1975, the percentage of reportable incidents and accidents attributable to human factors has increased from 24 percent to 38 percent in 2002. Knowledge about equipment-related failures has contributed to the design of more reliable equipment, reducing accidents attributable to system malfunctions. At the same time, people working in railroad operations now find themselves in a more complex system. Train crews, dispatchers, and roadway workers play a critical role by adapting to changing conditions that exist in the railroad environment. As the railroad environment becomes more complex, the opportunities for failure that involve human interactions also increase.

PTC technology has the potential to address some of the failure modes involving the train crews, dispatchers, and roadway workers. The driving safety motivation for PTC systems has been to eliminate many of the kinds of fatal accidents that have occurred in recent years. These systems are intended to eliminate train-to-train collisions and to protect train crews and roadway workers. NTSB recommended that FRA encourage the use of PTC systems as one of its Top 10 Most Wanted Transportation Safety Improvements (NTSB, 2001). NTSB identified over 100 collisions that may have been prevented if a fully implemented PTC system had been in place. FRA has encouraged the railroads to develop and deploy such systems, provided that they demonstrate a net positive effect on risk.

Railroads in the United States and Canada are developing a variety of PTC systems that are intended to improve the safety and productivity of railroad operations. The PTC systems under current consideration accomplish safety goals by providing backup warnings to train crews and by stopping trains that are about to do the following:

- Violate positive train separation
- Exceed speed restrictions (including civil engineering restrictions and temporary slow orders)
- Enter track segments protected for roadway workers and their equipment operating under specific authorities

PTC technology has the potential to improve safety by providing a layer of additional protection. However, it also adds another layer of complexity that may introduce new risks. PTC technology uses new modes of train control that can potentially impact train crew and dispatcher performance. It employs new generations of digital technology that may introduce new challenges for system maintainers. The question for railroads seeking to introduce this safety-critical technology is whether the overall safety risk is equal or better than the technology and operating practice it replaces.

Railroads seeking to receive approval from FRA to implement PTC systems must submit a PSP to FRA. A PSP includes a risk assessment that compares the railroad operations with and without use of the processor-based control system to show that no reduction in safety would occur from implementing the system. The PSP must describe all the elements and practices to assure these products are developed consistent with generally accepted safety principles and include acceptable procedures for implementation, testing, and maintenance. These elements and practices explicitly call for a human factors analysis of the HMIs.

FRA has developed draft guidance (Department of Transportation, 2001) on information to be submitted as part of the PSP for approval of PTC systems. That guidance emphasizes the use of PRAs to demonstrate the safety performance of the PTC system being proposed. The objective is to provide evidence that the new PTC system does not degrade safety below the level of the existing system (Department of Transportation, 2001). The evidence can take the form of a PRA that compares the total risk associated with the new system to the total risks associated with system it will replace. This PRA includes performing a human reliability analysis (HRA) that estimates risk associated with human actions or failure to take actions. FRA is charged with evaluating the PSP to determine whether the evidence provided supports claim that the overall safety with the PTC system in place will be equal or better than the technology it replaces.

1.2 Study Objectives and Approach

In anticipation of PSP submissions, FRA initiated a study to identify emerging human performance issues and potential new sources of risk that can arise with the introduction of PTC systems. This report documents the results of that study.

The objective of the study is to provide FRA with guidance on specific human performance issues that must be considered in evaluating PSP submission for new PTC systems, as well as general guidance for identifying important human performance issues that can impact safety. The report also provides the railroad industry with guidance on the kinds of human performance issues that are important to address as part of quantitative risk analyses and related qualitative analyses that are performed to support PSP submissions.

The study examined the interactions between train crews, dispatchers, roadway workers, and the new PTC systems to determine if the designs can create situations that can set up the operators to place the trains, workers, or public at risk (i.e., could the systems actually decrease safety?). The study also examined if human factors and operational aspects of PTC systems exist that may reduce the effectiveness of PTC systems in accomplishing these functions or create additional safety concerns. It was provided as one source of guidelines to FRA as it reviews submissions by railroads for approval to use PTC systems.

Risk analysis is a tool that must always be used with understanding and judgment. The strengths of PRA stem from its ability to integrate important aspects of safety equipment and human response so the decisionmaker can make comparisons between alternative scenarios. However, the modeling of human performance remains more of an art than a science because the roles of humans in systems can change in subtle, and sometimes unexpected, ways with the introduction of new technologies into established work settings. The decisionmaker must take care to incorporate what is known from the behavioral sciences about the system, environmental, and internal factors affecting human performance. The decisionmaker must also organize the analysis in ways that provide clarity in the analysis and results, as well as showing the subtleties and complexities that can restrict the range and applicability of results.

This report discusses potential safety concerns associated with PTC operations that involve human interactions. This report also presents specific safety concerns that have been identified from a range of human factors and system safety perspectives. The analysis and identification of important human performance issues and safety concerns was accomplished partly as an extension to an earlier review of the Communications Based Train Management (CBTM) system (Wreathall, Roth, Bley, and Multer, 2003), from visits to other PTC systems in trial operation, and from the review and analysis of accidents that are considered to be potentially preventable by use of PTC.

Section 2 introduces a framework for conducting a PRA/HRA in support of a PSP to focus attention on the areas of primary concern from a risk perspective. The section summarizes historical data on railroad accidents that helped to define human performance issues that can contribute to risk and are thus important to address in evaluating new PTC systems. Sections 3-6 present additional human performance issues important to risk that are drawn from interviews that were conducted to elicit the perspectives of operational, maintenance, and management staff with experience with four PTC systems in trial operation. Section 7 of this report provides specific guidance to FRA on how to approach the review of these issues in the PSPs and associated PRAs.

1.3 Method

A three-step process took place to collect the information that serves as guidance in evaluating the safety of PTC systems and components. First, the authors reviewed the literature to identify human factors issues that arose in the development and use of signal process related technologies (i.e., computer and communications technology) in related industries. Based upon this review, the staff identified a list of human factors issues to pursue further. Second, using this list as a starting point, the staff analyzed a series of accidents that could potentially be prevented by PTC systems to assess the failure modes (risk factors) associated with these accidents. The information from both of these activities contributed to a list of questions needed for the third step. In this step, the authors visited several sites where railroads were testing or beginning to use new train control technology with elements of positive train control. These systems included the four shown in Table 1. Appendices A-D show the questions that guided the structured interviews. The authors interviewed employees to identify new sources of risk and human performance issues associated with the use of these new systems. The authors conducted interviews to elicit the perspectives of operational, maintenance, and management staff with experience in four railroads experimenting with train control systems using elements of PTC.

Table 1. Systems for which Site Visits Were Made

System Name	Railroad Interview Date	Groups Interviewed
Advanced Speed Enforcement System	New Jersey Transit March 2004	Locomotive engineers, conductors, signalmen, cab mechanical maintenance personnel, management
Communications Based Train Management	CSX October 2001	Locomotive engineers, conductors, dispatchers, roadway workers, management
Incremental Train Control System	Amtrak October 2003	Locomotive engineers, signalmen, trackmen, cab mechanical maintenance, management
North American Joint Positive Train Control System	Amtrak Union Pacific October 2002	Train crews, training instructors, system engineers

2. Framing the PRA/HRA to Support PSPs

A railroad preparing to implement positive train control technology must submit a risk assessment to FRA as part of its PSP demonstrating that the new system is as safe or safer than the existing system. However, risk assessment comes in many forms and deciding how the risk assessment should be structured is important because it affects the clarity of the analysis, as well as its cost. An analysis focused on the key issues can often be more helpful than a complete model, if complexity makes it difficult to understand and verify.[1] A crafted-scope model can provide significant depth in the areas most relevant to the primary concerns and accept simplifications in areas not decisive to the issues to be resolved.

Turning to the historical record, to the real world, shows what the important issues for PTC safety should be, which include what safety-related factors are driving the move toward PTC systems and what have been the historical contributors to risk. The risk analysis should show that the deployment of the new PTC system reduces historical contributions to risk. In addition, the risk assessment must search for new failure modes arising from unanticipated detrimental effects of the new system. As mentioned in the introduction, new systems will add complexity to the hardware, software, and the human-machine interaction. This report searches for potential cognitive challenges that could lead crews to defeat the benefits of the PTC system, ways that the system can change operator performance or that can lead to new sources of error.

2.1 Structuring a PRA/HRA Around Key Issues

The PRA of the PTC can be structured to focus attention on the salient issues if following the schema of Figure 1. The PTC should reduce the risk of current accidents, so the report first looks at the history of the railroad accidents to learn what factors are responsible for those accidents. Second, under the terms of the proposed FRA rule, the new systems should not increase the risk. To confirm whether this is indeed the case, the search for ways that this could happen by interviewing the personnel most familiar with similar existing systems, to identify potential operational vulnerabilities, occurs.

Section 2.2 examines the operating history where four sources of detailed accident information all point to the same issue of human performance under difficult situations. So the PRA must be organized to ensure that human performance under particular contexts is examined; HRA is a primary tool in that effort. Section 2.3 describes the state-of-the-art PRA/HRA modeling approaches. They point to the need for a formal search process for ways that the new systems can interact with train crews and maintenance personnel to induce new possibilities for accidents. Knowledge of human performance and ways that new technologies can impact performance both positively and negatively inform this search process (see Section 2.4). To begin the search process the authors conducted interviews with operational, maintenance, and management staff experienced with four PTC systems that were undergoing early field trials. Sections 3-6 present human performance issues important to risk that were identified based on those interviews.

---

[1] All models are simplifications of the real world. The art in modeling is to discriminate between issues essential to the question that the study wants to answer and those that are of secondary importance.

2.2 History of Accidents without PTC

2.2.1 Train Accidents

The authors examined the following four sources of information about historical accidents and their impact:

- NTSB report on accident reviews and recommendations
- Discussions with members of the Railroad Safety Advisory Committee (RSAC) Accident Review Team (ART)
- Switching Operations Fatality Analysis (SOFA) report
- Detailed FRA investigation files for specific accidents

All four sources confirm the importance of human error in the more severe accidents.

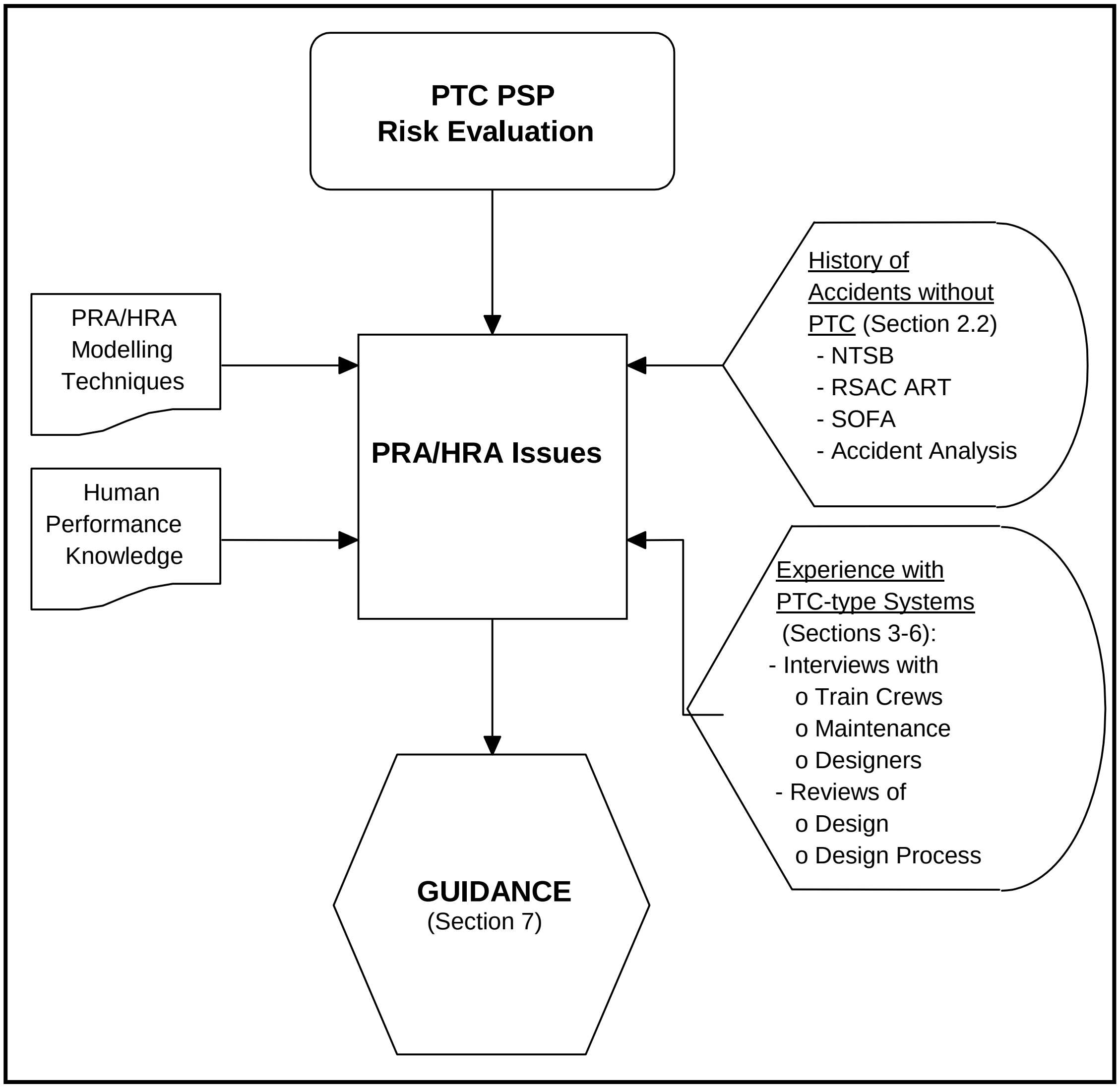


Figure 1. Elements Involved in Framing the PRA/HRA in Support of a PSP

NTSB. In its report on PTC preventable collisions (NTSB, 2002), NTSB traces its history of study and recommendations with respect to PTC systems. Following its first PTC recommendation associated with a collision in 1986, NTSB investigated 100 collisions that may have been preventable if a fully implemented PTC system had been in place.[2]

"The recommendation for a Positive Train Control system has been on the Safety Board's **MOST WANTED** list since its inception in 1990." The current recommendation states, "The National Transportation Safety Board recommends that the Federal Railroad Administration: Facilitate actions necessary for development and implementation of positive train control systems that include collision avoidance and require implementation of positive train control systems on main line tracks. Establish priority requirements for high-risk corridors such as those where commuter and intercity passenger railroads operate" (NTSB, 2002).

Essentially all of the events cited by NTSB in the report involved human error. NTSB promoted the idea that the PTC needs to enforce the existing rules and does not seem to have examined the underlying causes of the human error to determine if the culprit has been human performance or the context in which the humans work.

ART. RSAC established a PTC Working Group and, within that group, an ART to review all accidents in the FRA database to identify PTC preventable accidents (PPA). The team included experienced railroad people from FRA, railroad management, and the labor crafts.

After numerous passes through FRA's accident/incident database, the team agreed upon those accidents that were PTC PPA. However, the team did not characterize the conditions under which these accidents occurred. Work performed by the current authors (Wreathall, Roth, Bley, and Multer; 2003), well after the bulk of ART's work was concluded, clearly demonstrates the value of more thorough characterization of the accidents' causes.

ART members indicated that it would be a massive task to go back through the data to attempt to better characterize the accidents. Additionally, most of the accident reports lacked the kinds of information needed to understand the factors that may have led to human-induced accidents. Nevertheless, several ART members felt that their personal experience with the railroads and their recent reviews would allow them to shed light on the events. Overall, they concluded that the more serious accidents (those involving loss of life and significant property damage) usually involved unsafe human actions caused by one of the following:

- Cognitively challenging situations (e.g., severe weather, such as fog, rain, and ice, garbled radio communications, changing speed restrictions, or confusing equipment indications)
- Poor communications practices (e.g., misunderstandings because communications were not confirmed or ambiguous language)
- Inattention
- Inexperience

---

[2] The notion of a fully implemented PTC system has been incorporated in FRA rule definition through the idea that risk should not increase with the new system in place.

They generally agreed that crews do not get in trouble when few variables exist. Complex context and situations where changes exist (new restrictions, inclement weather, new rules) offer more opportunities for error.

If these judgments are correct, risk assessments should focus on whether the PTC system helps with these particular situations, rather than focusing on the detailed analysis of hardware and software systems already in place. Are the cognitively challenging situations improved? Are the risk consequences of error mitigated? The current PTC system designs focus on mitigating the consequences of the human performance problems–a missed signal, an over-speed event–rather than eliminate the factors that give rise to them. Given that focus, the risk assessment should ensure that the human performance problems do not resurface in other ways, (i.e., in new accidents). Are poor communications eliminated, improved, or covered in another way? Is inattention corrected? Are there new opportunities for failure due to miscommunication or inattention? And are any new cognitively challenging situations created immediately or over time?

SOFA. The SOFA Working Group (1999) examined fatal accidents during switching operations. The goal was to identify contributing factors to these incidents and determine whether a common set of factors existed that played a role. The fraction of events involving human error during switching accidents was significant but lower than estimated by ART members and in the NTSB analysis for accidents on the main line. While conditions for switching operations differ from main line operations, the human-involved failures and the underlying causes were quite similar to those identified by ART for main line accidents. The factors included inexperience, poor communication, and inadequate train resource management.

Analysis of FRA Investigation Files on Accidents. To characterize rail accidents, the authors developed and applied a structure for data analysis from the reports of detailed accident investigations in FRA files. The basic data structure is similar to that developed for the nuclear industry in the ATHEANA human reliability analysis project (Barriere, M., D. Bley, S. Cooper, Forester, (Kolaczkowski, Luckas, Parry, Ramey-Smith, Thompson, Whitehead, and Wreathall, 2000). The authors made additions and refinements to tailor the data structure to the railroad industry, but the focus remains on understanding the context under which people must perform (dispatchers, train crews, and roadway workers). Table 2 summarizes the key elements of the structure.

The current project analyzed five accidents as a trial use of the paradigm outlined above. Appendix E details these analyses. While the number of accidents the authors looked at is small, the results are encouraging and support the judgment of ART described earlier. The level of understanding of each accident is far greater than conveyed in the typical database statistics. Impacts of context on human performance are clear. Implications for the kinds of context that contribute to serious accidents appear to be consistent with results from other industries.

The accident analyses identified the following human performance issues as primarily responsible for creating the cognitively challenging situations that led to unsafe acts:

- Inexperience
- Poor communication
- Inattention
- Physical/environmental factors creating problems for:

  - People
  - Machines
- Systems circumvented
- Problems with automation
- Organizational pressures
- Problems with operating rules
- Maintenance and test issues

Several of these issues were present in each accident. All of these issues occurred in multiple accidents. While the sample is far from complete, it seems significant that these few issues are common across accidents and are consistent with the findings of the ART and SOFA groups. It is also important to understand that the existing designs and operating practice are robust; several of these issues are present whenever the system fails. As has been repeatedly shown in other industries, multiple human and system failures are required for accident to occur. Risk analysts and reviewers should ensure that they consider multiple issues in their work.

Table 2. Structure for Characterizing Accidents

- **Summary of event**
  - Type of accident
  - Identification
  - Train makeup
  - Crew experience
  - Method of operations
  - Consequences
  - Data sources
- **Event characterization**
  - Deviations from expected conditions
  - Any key mismatches between rules, instructions, and performance
  - Most negative influences
  - Most positive influences
- **Work mode transition issues**
  - Mode changes
  - Transfer of control
  - Shifts in authority
  - Skill loss
  - Coming up to speed
  - Primary/backup reversion
  - Fixation
- **Significance of event**
  - Extreme or unusual conditions
  - Contributing pre-existing conditions
  - Misleading or wrong information
- **Information rejected or ignored**
  - Multiple hardware failures
  - Transitions in progress
  - Similar to other events
- **Key parameter and train/process status**
- **An action summary**
  - Timeline
  - Human actions
  - Dependency map of actions
- **An accident diagnosis log showing cues and responses**
- **Unsafe action/context analysis**
  - Operating conditions
  - Performance shaping factors
  - Human information processing

The most significant kinds of information identified in the analysis process described here are not included in existing databases.

Limited Detailed Data. The report focuses on the four sources of information listed above because of the limited depth of information contained in the larger available databases.[3] These sources only support analysis of summary statistics (e.g., how many accidents occur per mile of track, under various kinds of control from verbal authorization to automatic signaling). The authors know what happened but do not know the details of why these accidents occurred or under exactly what specific local conditions they occurred.

The lack of causal data is troubling because it makes calculations of risk suspect or, if carefully prepared, subject to broad uncertainties (Wreathall et al., 2003). If the most severe accidents, those that new PTC systems are intended to protect against, are caused by human unsafe acts, then a thorough understanding of the context under which they occur is essential to meaningful analysis (Barriere, M., D. Bley, S. Cooper, Forester, Kolaczkowski, Luckas, Parry, Ramey-Smith, Thompson, Whitehead, and Wreathall, 2000). Many sources point out that human error is more than a random process or the result of incompetence on the part of personnel; it is often the result of difficult or confusing situations (Wreathall, 2003; Switching Operations Fatality Analysis Working Group, 1999; Dekker, 2002; Reason, 1997).

The authors believe that further examination is essential and that developing a convincing understanding of the causes of serious accidents can greatly simplify understanding the risk benefits of new PTC systems.

To fully characterize the ideal PTC systems, it would be helpful to fully understand the underlying causes of serious rail accidents. If these causes could be characterized down to the level of performance-shaping factors and error mechanisms, evaluating the risk would be more straightforward and understanding how to improve the risk would be clear.

In evaluating risk with and without a PTC system, it would be useful to know how often the crews and dispatchers avoided accidents in difficult conditions. PTC designs under current consideration might not be as effective under severe environmental or other conditions as current crews. In their interviews, operational personnel identified several examples of complex situations that might not be adequately handled by PTC systems. If so, introduction of the PTC system could affect the likelihood of successful crew performance and possibly degrade safety. Unfortunately, no quantitative data sources exist to answer this question. The elicitation process described in the report by Wreathall et al. (2003) could be used to develop an estimate of the likelihood of such conditions arising.

2.2.2 Accidents Involving Roadway Workers

One core function of PTC systems is to improve the safety of roadway workers, particularly from the dangers of trains entering work zones without appropriate authority. As part of this analysis, the report reviewed an FRA roadway worker fatality data set that covered the period from 1986 through 2003.[4] The authors focused on 24 cases that involved roadway workers being hit by a train while working. This included 19 instances of roadway workers being hit by a train that came on the track they were working on and 5 instances of roadway workers being hit by a train that was on an adjacent track. The analysis does not include other fatalities (e.g., fatalities attributable to being struck by maintenance-of-way equipment or that occurred while walking to

---

[3] Accidents during switching operations have been more thoroughly detailed (SOFA Working Group, 1999).

[4] The authors thank Christopher Schulte, FRA, for providing this data set.

or from the work area). The purpose of the analysis was to begin to understand some of the situational factors that appear to contribute to the roadway worker accidents. Several findings emerged from the preliminary analysis, including the following:

- Problems in communication were explicitly identified in 5 of the 24 incidents (20 percent).
- Unusual or unexpected conditions were explicitly identified in 5 of the 24 incidents (20 percent). This included three instances where multiple trains passed in immediate succession and two instances where the trains came from an unexpected direction.
- Roadway workers facing away from the train was explicitly mentioned in 4 incidents (17 percent).
- Dispatchers and/or the train crew not being aware of the roadway workers was explicitly mentioned in 4 incidents (17 percent).

These results reflect similar factors that arose in the analysis of train accidents. Problems in communication, failures in situation awareness with respect to the location and activities of others (trains, roadway workers), and unusual conditions that violate expectations emerged as main contributors to accidents. The results point to the potential value of aids that include the following:

- Facilitate communication among roadway workers, dispatchers, and train crews
- Enhance ability of roadway workers to be aware of approaching trains
- Enhance ability of dispatchers and train crews to be aware of location of roadway workers

Interestingly, this review of fatalities does not identify any cases of fatalities because of a train entering a work zone in violation of its authority. In all cases the fatalities occurred under joint track-and-time operating rules where roadway workers relied on train approach warning and individual train detection for on-track safety. In contrast, current PTC systems should enforce exclusive working limits where trains are not allowed into the working limits without explicit permission from the employee in charge (EIC) of roadway workers. This finding suggests that achieving significant safety benefits from PTC systems that prevent trains from entering work zones will require concomitant changes in operating practice that take advantage of the more positive forms of on-track safety afforded by exclusive working limits, enforced by the PTC system.

A report of the Roadway Worker Protection Task Force draws similar conclusions. The RSAC recently chartered this report to determine best practices for a PTC system as it relates to the protection of roadway workers (Task Force Report, draft, July 2004).[5] The task force examined roadway worker fatalities from 1986 to 2003. It determined that virtually no roadway workers were killed due to an unauthorized train entering working limits.[6] However, by reviewing other sources of historical data (e.g., FRA inspection data, locomotive engineer decertification data, and other miscellaneous sources), the task force determined that known train breaches of

---

[5] Draft Report of the Railroad Safety Advisory Committee Positive Train Control Working Group Roadway Worker Protection Task Force, July 2004.

[6] The exception occurred on May 30, 2003, in Colorado, where a free rolling car entered working limits and killed an employee.

working limits have occurred. The task force identified 10 verifiable incidents between 1997 and 2003. While no known casualties associated with these incidents occurred, they provide evidence of a potential risk to roadway workers of trains entering work zones without authority.

The Roadway Worker Protection Task Force concluded that one of the key features afforded by a PTC system with respect to on-track safety is the system's ability to positively prevent trains from inadvertently entering working limits. While noting that the overwhelming majority of roadway worker fatalities occurred where working limits were not in place, the task force noted that, if an enhanced communication system were available, roadway workers would be more likely to use a more positive form of on-track safety (working limits) and thus benefit from the added protection afforded by PTC systems.

The task force envisions that roadway workers would be equipped with portable terminals that can request authority to occupy track and release authorities. FRA has funded a research and development project to build a model personal remote terminal (PRT). The stated goal of the PRT project is to develop a hand-held remote terminal for use by the EIC of roadway workers to provide a wireless, functional link to the train control system. The PRT will utilize and adapt to a variety of PTC systems to enable roadway workers to more readily obtain more positive forms of on-track safety (working limits) rather than relying on other forms of on-track safety (train approach warning and individual train detection).

The task force concluded that a PTC system, coupled with a PRT device, will greatly enhance communication between all stakeholders (i.e., roadway workers, train crews, and train dispatchers) and increase the capability of roadway workers to request working limits from the dispatcher, request civil speed limits (within working limits and adjacent tracks), and display the location of trains. The report identifies a set of best practices intended to achieve these aims.

These conclusions are consistent with the results of this report's analysis and suggest that PTC capabilities to prevent inadvertent violation of work zones by trains coupled with a PRT that facilitates obtaining and releasing working limits, and corresponding changes in operating rules, should in combination, result in reduced risk to roadway workers.

The above discussion serves to highlight that PTC systems function by enforcing the relevant operating rules. Joint track-and-time rules will always permit trains to enter work zones, and, in this case, the protection of the workers must be the responsibility of the work crew to maintain (e.g., via train approach warning and individual train detection forms of on-track safety). If work is performed under exclusive track-and-time rules, PTC could then act to prevent incursion into the protected work zone.

2.3 PRA/HRA Modeling Techniques

The operating experience emphasizes a need for risk analysis that focuses on human actions, including the following:

- Does the PTC protect against the kinds of human actions that have occurred in the past?
- Is the hardware/software less likely to fail than the dispatcher/crew under all conditions? If not, how do environmental and other conditions affect both the new PTC system and the crew and their interactions?
- Do ways exist in which the system can degrade human performance and vice versa?

- Where are the major uncertainties? Are they due to randomness or lack of knowledge (including experience with the new systems)?

The PRA of new PTC systems can provide an integrated assessment of the safety performance of a rail system with the new PTC system in place. That is, it can answer the question of overall safety, rather than relying on lower level surrogates like “no single failure can fail the system,” “subsystem reliability must meet specific [arbitrary] goals,” or relying on the gut feeling of the regulator that the design represents an improvement. However, because PRA is an open form analysis, the scope must be defined carefully so that the analysis provides convincingly clear results at a reasonable cost.

Thus, PRA is useful because it provides an integrated assessment of system performance (expanding the scope of the analysis over alternative approaches) and because it focuses on the most important issues (greatly narrowing the scope of the analysis). Care must be used in limiting the scope of the analysis to avoid ruling out potential contributors to risk before they have been evaluated. On the other hand, the authors did not require a model of all aspects of railroad operations if some of those aspects are not affected by the new system or if they are not relevant to the questions being asked.

The basic idea of risk assessment is very simple. All risk assessments try to answer the following three basic questions:

1. What can go wrong? That is, what are the scenarios, S_i, that can occur?
2. What is the likelihood, L_i, of the scenario occurring? Here the authors must acknowledge and evaluate all uncertainties.
3. What are the consequences, X_i, of the complete scenario?

The PRA is simply the set of all possible such triplets, S_i, L_i, and X_i, that can occur. The art of PRA is in structuring the model to facilitate calculation, while keeping it simple and clear enough to permit review and understanding of its content. Science and engineering support the search for scenarios and provide the answers to the likelihood of reaching various consequences. A wide variety of modeling and mathematical tools have been developed to support PRA (see, for example, Bley et al., 2002; Barriere et al., 2000; Atwood et al., 2003).

A formal search process is needed to identify possible ways in which the new PTC system (through its possible failure modes or conditions induced by its use combined with failures in other systems) could introduce new failure mechanisms, including creating cognitively challenging situations for crews and dispatchers. Qualitative scenarios must be developed for the events identified in the search. Quantitative likelihoods and consequences are attached to each scenario based on calculation, expert elicitation, and any easily available data (Wreathall et al., 2003).

The results of the interviews with railroad personnel involved in the design and operation of the trial PTC systems in Sections 3-6 provide a significant first step in this search process. From these interviews, the authors learned of problems that have already occurred and of potential problems that are currently causing concern.

For particular PTC systems, analysts must address these questions quantitatively, and in doing so, they must do a particularly good job of identifying potential human interface and interaction problems. These can be addressed judgmentally, even when formal and convincing models are not available, using the methods described in the analysis of the CBTM system (Wreathall et al., 2003).

Because rail systems are so large, varied, and distributed, rail line-specific modeling of all track segments and crew capabilities would be prohibitive. A reasonable alternative would be to develop a number of stylized track segments and crew characteristics that span the space of conditions expected in the field. Then results for a specific line could be obtained by combining a weighted set of stylized situations; additional stylized segments may be required for any new analysis.

For new PTC systems, the risk is expected to be substantially lower because that is the purpose of the new designs. Therefore, the real work of PRA may lie in the search process for the scenarios. Clever ways to structure the search for unexpected conditions that can challenge design assumptions will need to be developed or identified and applied to these facilities. Risk may arise from unexpected ways that the PTC system can end up operating outside its design assumptions. For example, Barriere et al. (2000) developed a search scheme for scenarios that deviate from designers' expectations, and Bley et al. (1992) applied a structured search for construction errors. Ways that the railroad system (the trains, the track infrastructure, the PTC and other control systems, the operating rules and practices, and the people—the train crews, dispatchers, roadway workers, maintenance workers, and management) can end up operating outside its design assumptions could include the following scenarios:

- Where the train crews, dispatchers, and/or maintenance personnel place the equipment (both on-board and way side equipment) in unexpected conditions
- Where gradual degradation has led to unobserved deterioration, fatigue, or physical condition far from that envisioned in the design
- Where crews and dispatchers have become dependent on the systems and they fail to take appropriate action (e.g., in its absence)
- Where external (including environmental) conditions degrade the PTC system, communications, or crew/dispatcher performance

The key to safe operations is a focus on managing the unexpected (Weick and Sutcliffe, 2001). In fact, searching for the unexpected is exactly what PRA is supposed to do. With repeated application to similar facilities, analysts sometimes lose sight of that. In a recent address at a United States Regulatory Commission colloquium (2002), the Director of Research indicated that, in applying PRA to future reactor designs (a situation similar to PTC systems for the railroads), analysts must start with a clean page (i.e., not be biased by expectations from the conclusions of PRAs on old designs and other systems).

To address these potential problem areas, researchers developed a new way to look at human performance and human-machine interactions. New second generation HRA methods focus on context and control (Hollnagel, 1998) and on how the organization (Reason, 1997) and the operating state (Barriere et al., 2000) can set up the operators for failure. The modern approach shifts the focus from human error as the cause of accidents to unsafe actions as a symptom of more systemic problems. The focus in both retrospective event investigation and in prospective HRA shifts to seeking understanding of why operators' actions were locally rational (i.e., why what they did made sense at the time, given the context in which they were operating as opposed to the hindsight of knowing how things turned out and how they might have progressed differently) (Dekker, 2002). The methods for a new type of HRA go beyond standard task analysis and table lookup of average human error probabilities. These methods look for the triggers for desirable and undesirable human performance. The authors' previous report (Wreathall et al., 2003) introduced some of these ideas to PTC-equipped operations.

Closely interwoven with human performance is the new PTC system and the HMI. PTC systems cannot solve the problem alone; they must be matched to the human operators and maintenance personnel. Kletz (1995) cites a number of real-world events showing how advanced digital control systems have failed in ways that proved cognitively challenging to operators, have not been well-matched to human capabilities, or have behaved strangely because of maintenance problems. However, if design of these systems is well matched to human abilities and especially to avoiding the kinds of cognitive problems identified by the new HRA approaches, new PTC systems can avoid many of the difficulties that have faced operators in current facilities. Sections 3-6 provide examples of such concerns in current designs that should be addressed and corrected. Quantitative analysis is not necessary for such mismatches in new systems. Correct them before accidents occur.

2.4 Human Performance Knowledge

This section summarizes some of the key human factors concepts and findings relevant to PTC and its impact on human performance and system reliability. The HRA approaches introduced in Section 2.3, the proper interpretation of accidents (Section 2.2 and Appendix E), and the implications of the interviews about existing PTC systems (Sections 3-6), rely heavily on results from psychology and the behavioral sciences. The earlier report (Wreathall et al., 2003) provides a good introduction to many of the concepts and findings from the behavioral sciences as they relate to human error and the factors that contribute to it. Woods and Christoffersen (2003) provide additional relevant findings in a literature review conducted as part of a related FRA study that is looking at implications of PTC for workload transitions and human performance.

A growing body of literature exists on the factors that contribute to human error and appropriate methods for investigating the role of human error in accidents and their causes (e.g., Dekker, 2002; Reason, 1990; Reason, 1997; Strauch, 2002; Woods et al., 1994). This literature stresses that errors do not occur randomly but rather are the result of error-provoking elements in the situation that include characteristics of the task, the team, the local work environment, and the organizational climate. To understand why errors occur and how to mitigate them, one must investigate the context in which work is done and identify the situations that are likely to be error-provoking.

New systems often have unanticipated effects on human performance, with sometimes negative consequences (Roth et al., 2002). New technologies are generally introduced with the aim of improving overall performance, cost efficiency, and/or safety. These changes in technology can take the form of increased levels of automation, such as in aviation (e.g., Billings, 1997) or new forms of computer support, such as is currently occurring in the health care industry (Patterson et al., 2002). System designers often assume that the introduction of new technologies will produce well-specified, positive impacts on human performance and human reliability. These designers also assume that the new technology will increase performance efficiency or catch and recover from known human errors without otherwise changing operations.

However, experience in a wide range of domains shows that new technologies can impact the field of practice in ways that the system designers did not anticipate (Roth et al., 1997; Woods and Dekker, 2000; Woods and Sarter, 2000; Woods et al., 1997). Increased capabilities are often accompanied by new sources of complexity that include tighter coupling across parts of the system, higher tempo of operations, changes in the availability of information, and mismatches between system assumptions of the demands of work and the actual demands of the work (Woods and Dekker, 2000). These changes can produce unintended and unpredicted impacts on human performance, such as changes in skills and strategies to accommodate the changing environment, new forms of error, and new vulnerabilities to risk (Woods and Dekker, 2000; Patterson et al., 2002; Roth and Patterson, in press). One of the classic examples is the emergence of mode errors in aviation. With the introduction of multiple levels of automation, pilots can lose awareness of the current mode of automation. As a consequence, they can take actions that have (unintended) catastrophic consequences (Sarter and Woods, 1995). The lesson learned from this literature is the importance of searching for potential negative impacts of new technologies on human performance that the system designers failed to anticipate.

Of particular relevance to evaluating the impact of PTC system on human performance is the literature on human interaction with automated systems (Billings, 1996; Christoffsen and Woods, in press; Sheridan, 2002; Woods and Sarter, 2000). Lessons to be learned from this literature include the problems that arise when automated systems are designed to be strong and silent, making it difficult to understand, predict, or control their behavior (Norman, 1990; Sarter and Woods, 1995). Problems include inability of people to calibrate their trust in the automated system to its actual performance capability, at one extreme leading people to distrust the system and turn it off and at the other extreme leading them to overrely on the system beyond what is warranted given its actual level of competence (Parasuraman and Riley, 1997; Sheridan et al., 1999; Moray, 2000).

A consistent finding is that automated systems can be brittle in the face of unanticipated complexity (Woods et al., 1997). This has led to a growing literature on how to design automated systems that act as cooperative team players under the supervisory control of the people interacting with them (Christoffsen and Woods, in press). The goal is to make the total person-machine system more robust when confronted with situations that were unanticipated by the system designers. Design principles for building automated systems that are team players include the following:

- O*bservability*: Allowing the person on the scene to understand what the automated system is doing and why and anticipate what it will do next
- *Directability*: Allowing the person on the scene to redirect it in cases where the automated system’s actions are inappropriate to the situation (Roth et al., 1997)

Another literature relevant to analysis of PTC systems and new opportunities for risk is the human factors literature on maintenance errors (Hobbs, 1999; Reason and Hobbs, 2003). Experience from other industries indicates that maintenance errors can be an important contributor to risk. A growing body of literature exists on the factors that contribute to maintenance errors and the steps that can be taken to reduce maintenance errors. Techniques for mitigating error range from design for maintainability to development of effective training and maintenance manuals to design of supportive organizational structures. Section 4 reviews the primary findings of relevance to the maintenance of PTC systems.

The core concepts and findings from these various human factors resources informed the design of the question sets that were used in the interviews of operations and maintenance personnel. They also helped the authors interpret and understand the implications of what the operations and maintenance personnel said during the interviews as summarized in Chapters 3 to 6.

2.5 Beginning the Search for Potential Problems

Chapters 3 to 6 present the findings of the authors’ discussions with engineers, conductors, maintenance workers, designers, and managers. The fruit of those discussions is a catalog of human performance issues summarized in Chapter 7. That catalog can serve as guidance for analysts performing risk assessment in support of PSP applications. Likewise, the regulators, who must review and evaluate these submittals, might find the issues a useful guide to ensuring completeness and effectiveness of the risk assessments.

3. Engineer-Related Safety Concerns

This section identifies the human factors issues that emerged as part of a review of experiences with PTC systems that are currently in trial operation. This included the Advanced Speed Enforcement System (ASES), the Incremental Train Control System (ITCS), the CBTM system, and the Illinois Department of Transportation (IDOT) system.

3.1 Changes in Operating Practices

Interviews with locomotive engineers and conductors indicated that the introduction of PTC systems impacted how they operated the trains. Changes in train handling resulted from a combination of constraints imposed by the PTC braking profile, increases in information and alerts provided by the in-cab displays, and new sources of workload associated with interacting with the PTC system. The sections below describe changes in operating practices that result from the introduction of PTC systems and the potential safety concerns that they raise.

3.1.1 Impact of PTC Braking Profile on Train Handling and Braking

A consistent finding across the systems examined (CBTM, ASES, ITCS) was that the PTC braking profile was conservative because it required initiation of braking early to insure that train would slow down to the desired target speed under restrictive assumptions (e.g., heavy train or slippery track). This meant that under most conditions it required the train crew to initiate braking at an earlier point than they were normally accustomed to. Section 4.1.1 discusses some of the design constraints that lead to conservative PTC braking profiles, as well as the safety and efficiency implications for overall railroad operation. This section focuses on the implications of conservative PTC braking profiles on the train crews.

The train crews consistently reported that they needed to learn new train handling strategies to be able to stay within the PTC braking profile. The train crews indicated that the PTC systems required that braking must be initiated earlier than they were accustomed to. If the locomotive engineer initiated braking later than the PTC system braking profile required, the system presented a warning (typically first a visual warning, followed some seconds later by an audio warning). If the locomotive engineer did not reduce speed to meet the system braking profile, then the system made a penalty brake application that caused the train to stop. A penalty brake is highly undesirable because it significantly delays train operations and triggers documentation requirements to explain why the penalty brake occurred. As a consequence, locomotive engineers, across the systems in trial operation, consistently reported altering their braking techniques to conform to the requirements of the PTC braking profile.

The PTC braking profiles require that the locomotive engineer start to slow down and achieve target speed significantly ahead of the speed restrictions, which can result in a significant loss of time. The locomotive engineers reported that, if they initiated braking at or before the location where the PTC system required, they could avoid the PTC warning signal (and subsequent penalty brake). However, it resulted in significantly slower operations than when locomotive engineers operated the train without the PTC system. The ASES locomotive engineers estimated that a train could lose at least 4 minutes on a 1-hour commuter trip with ASES when it is not being used.

Some of the locomotive engineers explained that before the introduction of the PTC system, they had developed braking strategies intended to minimize the time required to complete a trip (consistent with staying within authorized speed limits). They set the brakes late to minimize unnecessary loss of speed. This braking strategy is no longer possible with the new PTC systems.

With experience, locomotive engineers are able to develop effective strategies for staying within the braking curve of the PTC system while still operating as efficiently as possible. Locomotive engineers indicated that, as they gained experience with the PTC system, they learned to delay initiation of braking, coming as close to the point of initiating a penalty brake as possible, without actually exceeding that point, to maintain efficient train operation.

One of the ITC locomotive engineers provided an example of a train crew strategy for maintaining operating efficiency while avoiding a penalty brake. Figure 2 provides a picture of the ITCS in-cab display. The display includes target speed and time to penalty (TTP) for the upcoming speed restriction. The TTP starts at 30 seconds. When the 30-second visual warning appears, the locomotive engineer has 30 seconds to reduce the locomotive's speed to fall within the ITCS-specified braking curve to avoid penalty brake application. The 30-second count down continues until the locomotive engineer enters the braking curve. If the time to penalty brake value drops below 10 seconds, ITCS gives an audio warning. When it gets to zero, a penalty brake is initiated. If the train speed gets below the braking profile target value before the countdown reaches zero, then the countdown stops. The ITCS locomotive engineer explained that, if the operators started to slow down as soon as the 30-second countdown appeared and stabilized the value at 27 seconds, they would be ¾ of a mile back from the speed limit location when they slow down. In contrast, if the operators stabilize it at 1 to 2 seconds, they will be 500 feet from it, which is more reasonable.[7] The locomotive engineer indicated that, with experience, locomotive engineers tend to get closer to the edge of a penalty brake to increase train time efficiency.

Figure 2 shows the in-cab display for the ITCS PTC system. The display shows current actual speed and speed limit. It also shows the next upcoming target speed limit, the distance to target, and TTP. The TTP appears 30 seconds prior to predicted penalty brake and counts down until the train speed falls below the braking profile.

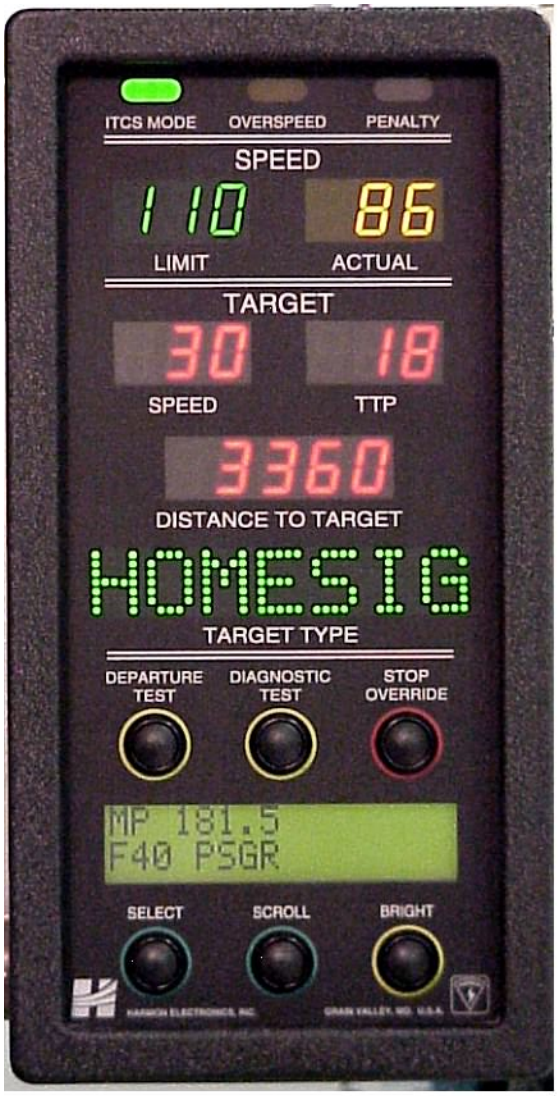
Not only do PTC systems require adapting braking style to conform to conservative braking profiles, but they can also create situations where the train must slow down or stop unnecessarily. New Jersey Transit locomotive engineers who operated trains with ASES described an interesting case that arises in territory where they have ASES with no cab signal.[8] The case involves approach signal updates; Section 4.1.2 describes it more fully. If the locomotive engineer comes to an approach signal, the ASES picks up that signal and requires the train to stop within 500 feet of the next signal. The ASES requires the locomotive engineer to stop at the next signal even if the signal is green when the train reaches it (without the cab signal, ASES has no indication of reading the signal ahead). This system behavior can cause significant

---

[7] The specific braking values are a function of the length of train and type of braking used. In this case, the locomotive engineer was referring to 12 pound blended brake application.

[8] The problem that arises with approach signals will be eliminated once cab signals are added to the speed-enforcement system (SES).

delays, jeopardizing the ability to meet the train schedule. Section 4.1 discusses the spurious enforcements resulting in delays, which can also have safety implications and lead to pressure to disable or defeat the PTC system.



Mode Light

Current Speed Limit

30 MPH Target Speed Limit

Target speed limit enforced in 3360 feet

Actual Speed

18 Seconds Time To Penalty

Target visible only if speed more restrictive

Figure 2. ITCS Display

With experience, locomotive engineers can learn the kinds of situations that cause spurious PTC activation and, in some cases, develop strategies to avoid these situations. The locomotive engineers have developed a strategy for dealing with the special situation described above. They simply slow down ahead of an approach signal until the approach signal turns to a clear to avoid a situation where they enter an approach and have to stop at the next signal even if the signal is green. This is a clever strategy that, while resulting in some slowdown in train movement, is more efficient than having to come to a complete stop when it is unnecessary.

The locomotive engineers pointed out that these strategies to avoid penalty brakes while still maintaining train running time efficiency require significant experience to develop. They stressed that someone who was new or on the extra board would not have developed these skills. As a consequence, he/she would be more prone to experience significant delays and/or initiation of penalty brakes.

Even with experienced locomotive engineers, evidence exists that PTC will result in slower train movement compared to trains operating without PTC. Locomotive engineers described conditions that could arise that would lead to unnecessary slow downs for which they had no control. For example, in the case of ASES, locomotive engineers indicated that, if a problem occurred with the doors, it would cause ASES to revert to enforcing freight speeds for Amtrak passenger trains. This event happened on the order of once or twice a month. It is important to identify the kinds of situations that can lead to spurious PTC enforcement and address them in documentation, training, and safety analyses.

Concerns Raised

The fact that PTC systems require locomotive engineers to adapt their train handling and braking to the requirements of the PTC braking profile raises a number of human factor concerns that could have safety implications. These issues should be considered and addressed as part of safety analyses.

One issue of concern is the performance of individuals who are early in the learning curve in using the PTC system. This includes new hires, experienced engineers who are new to the PTC system, and people on the extra-board who may not regularly use the PTC system. Interviews with locomotive engineers experienced with ASES suggested that it can take engineers approximately a month, operating with ASES on the territory, to learn where to initiate braking and adapt braking strategies appropriately. Similarly, it can require extensive training and experience to learn the variety of conditions that can arise that can cause the PTC to malfunction or initiate a penalty brake unnecessarily and how to avoid or deal with them. Locomotive engineers must have sufficient training and experience to anticipate these situations and learn how to deal with them.

Another concern is that changes imposed by the conservative braking profiles tend to slow train movements, making it harder to keep to the schedule. When multiple trains are on the track, the effect of slowing down a train or requiring it to stop can snowball, resulting in slowing down all the trains behind it. Unless explicit organizational/management recognition of these new sources of delays occurs and support exists for the locomotive engineers when delays arise, it can create new sources of stress and frustration on the part of locomotive engineers. One interviewee gave an example of a locomotive engineer who became frustrated learning to operate an ASES train and eventually bid on another job. The supervising staff pressed him to keep to the schedule, and he experienced difficulty doing so. Railroad management must explicitly recognize the impact of adopting conservative braking profiles on train schedules. Unless explicit organizational/manage-ment support exists, locomotive engineers may perceive themselves to be in a goal conflict situation between the need to operate within the bounds of the PTC system and the need to meet the train schedules. The concern is that, unless the commitment to PTC for safety is clearly communicated by management and reflected in realistic schedules and a supportive training environment, the organizational climate may promote bypassing PTC systems to keep to schedule, which will impact safety.

Implications

Any safety analysis must explicitly consider and address the concerns raised above. These concerns can be addressed through a combination of comprehensive training, improvements to PTC braking algorithms and in-cab displays, and organizational climate that foster a safety culture and avoid creating goal-conflict conditions.

If the predictive algorithm is conservative, it may require the locomotive crews to learn new train handling and braking techniques to avoid predictive enforcement. The following questions may then arise:

- How much and what kind of training will be required to enable locomotive engineers that are experienced in running trains with today's technology to run trains equipped with a PTC system?
- How much and what kind of training will be required to enable new locomotive engineers to run trains equipped with a PTC system?
- How much and what kind of training will be required to enable individuals on the extra-board to run trains equipped with a PTC system?
- How much and what kind of training will be required to enable engineers to anticipate, avoid, and deal with conditions where the PTC system malfunctions or initiates a penalty brake under conditions where it was not needed?

The fact that locomotive engineers will attempt to operate the trains to minimize running time while staying within the bounds of the PTC braking curve has implications for design of the in-cab displays. The in-cab displays currently provide limited cues, including when to initiate braking to stay within the braking curve. If the locomotive engineers initiate braking to avoid warning messages, they are likely to brake too soon, leading to unnecessary time delays. A substantial learning curve exists to develop efficient braking strategies while avoiding a penalty brake application. In addition, the strategies that the locomotive engineers have developed require closely monitoring the in-cab display. A need exists for development of in-cab displays that make it easier to anticipate and stay within the braking curve without having to look closely at the in-cab display so that more attention can be allocated to looking outside the window.

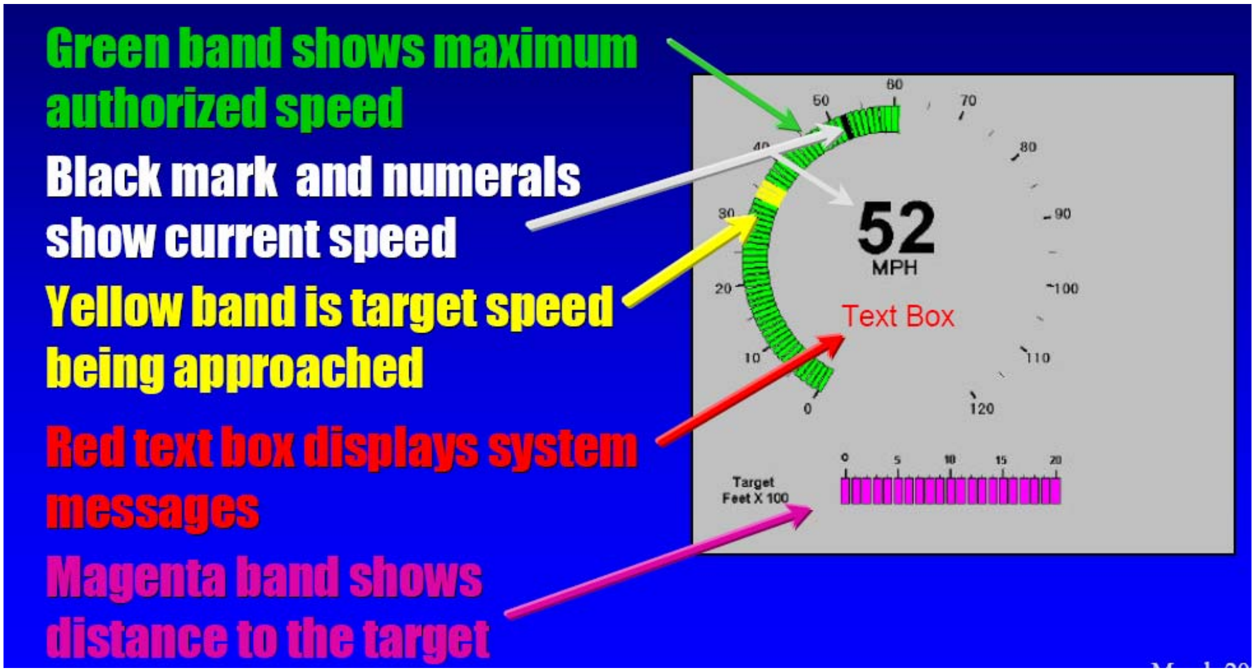
Finally, train schedules must be adjusted to accommodate the potential for slower train performance with PTC systems.

3.1.2 Potential to Shift Attention to In-Cab Displays versus Out the Window

Across the systems examined (CBTM, ASES, ITCS), locomotive engineers reported a need to focus visual attention on the in-cab displays, reducing their ability to look outside the window. Einhorn et al. (in press) reported a similar finding.

Locomotive engineers reported that they needed to carefully monitor the in-cab display to stay within the braking curve and avoid a penalty brake application. Attention allocation arose as a concern when the engineer operated the locomotive within a time window that provided little latitude in schedule deviation and passed through territory with speed restrictions. When the locomotive engineer approaches a block with a speed restriction, the locomotive engineer monitors the in-cab display carefully to stay close to the maximum possible speed while avoiding a penalty brake. In the ITCS system, the engineer monitored the countdown to penalty brake readout (see Figure 1). Locomotive engineers working with ASES reported a similar strategy. Figure 2 shows the ASES in-cab display. In ASES, the engineers attempted to keep the current speed indicator (a black bar) close to the edge of (but still within) the green band that graphically displays the instantaneously changing maximum authorized speed that is calculated from the braking curve. As a consequence, when they get close to a speed restriction, the locomotive engineers focused on the in-cab display and spent less time looking out the window.

Figure 2 shows the in-cab display for the ASES PTC system. The green band shows the maximum authorized speed, the black mark shows the current speed, and the yellow band shows the target speed being approached. If the black mark exceeds the green band, the train is in overspeed. Experienced locomotive engineers attempt to keep the black mark just inside the green band to maintain maximum speed while avoiding a penalty brake.



Green band shows maximum authorized speed

Black mark and numerals show current speed

Yellow band is target speed being approached

Red text box displays system messages

Magenta band shows distance to the target

Figure 3. ASES In-Cab Display

Locomotive engineers indicated that this tendency lessened with experience. For example, ITCS locomotive engineers indicated that, after 3 weeks to 1 month of operating with the system, they spent less time monitoring the in-cab display. However, several of the locomotive engineers reported that, even when locomotive engineers became experienced with the PTC system, they were still not able to look out the window as much as needed.

The locomotive engineers expressed concern that situations occur where they must look out the window to avoid hitting roadway workers, pedestrians at highway-railroad grade crossings, or trespassers. As an example, one locomotive engineer described traveling through a curve where people often trespass. He found himself focusing on the in-cab display to be sure he stayed within the braking curve instead of looking out the window.

The locomotive engineers indicated that they needed to maintain their focus outside the window and be prepared to blow the horn in case they see a trespasser, motor vehicle driver, or roadway worker. They were concerned that with their focus on the in-cab display they might miss unauthorized people on the right-of-way. This issue is a particular problem in territory where many grade crossings exist.

In addition to providing predictive braking, some PTC systems include preview information that enables locomotive engineers to anticipate and prepare for track conditions some distance ahead of the train. Information may include upcoming speed restrictions, location and velocity of nearby traffic, and upcoming distance cues (e.g., mileposts, switches, and stations). The four PTC systems examined, CBTM, ASES, ITCS, and NAJPTC, varied in the amount of preview information they provided. The CBTM system is intended as an overlay system that only activates when an authority is predicted to be violated (see Figure 4). This system does not provide preview information. ASES shows current speed, target speed at the upcoming speed restriction, and instantaneous maximum authorized speed as calculated from the braking curve (see Figure 3).

ACTIVE

WARNING: BRAKING IN 30 SEC

Your Authority Has Been
Violated By CSXT 207

Figure 4. Example of a CBTM In-Cab Display

ITCS provides current speed and target speed. ITCS also provides milepost information, giving the engineer train location (see Figure 2). Of the systems examined, the NAJPTC system provided the most preview information. Figure 5 shows a snapshot of the NAJPTC PTC display that was exercised in a field test conducted in October 2002. As seen, the display indicates the location, length, and current speed of the train. The display also provides 6 miles of look-ahead of the track and depicts upcoming mileposts, track layout, hot boxes, sidings, and crossings.

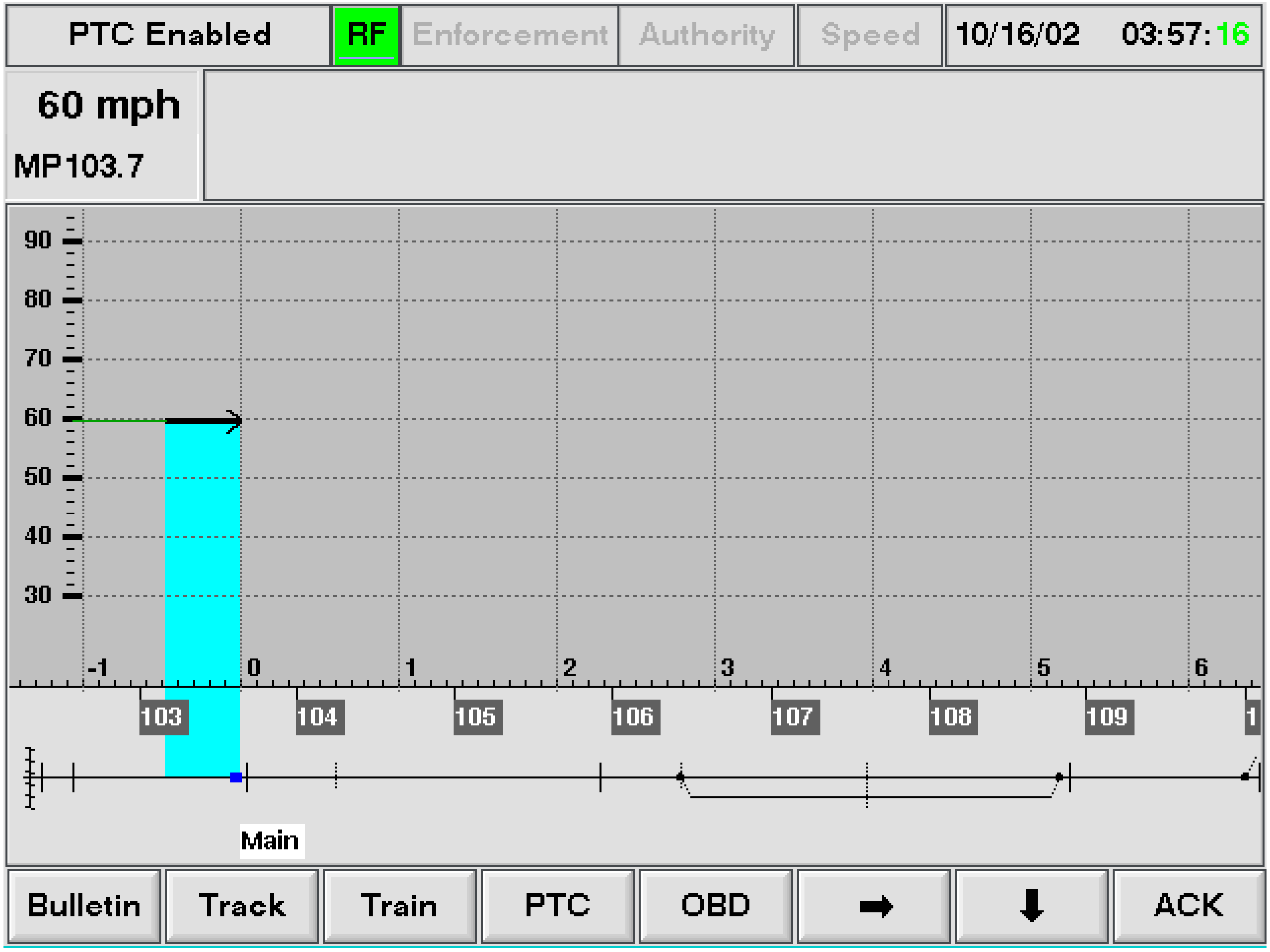


Figure 5. Example of a NAJPTC Display

While providing upcoming track information contributes to the need for locomotive engineers to focus attention on the in-cab displays, feedback from the locomotive engineers interviewed, as well as results of simulator studies, suggests that providing the engineers with preview information is helpful. The evidence suggests that preview information enables engineers to make better (i.e., safer and more efficient) decisions in the time available.

Several simulator studies have demonstrated that displays incorporating preview information can increase safety and efficiency of train operation (Kuehn, 1992; Askey, 1995; and Einhorn et al., in press). Kuehn (1992) showed that displays that incorporated gradient, authority, and speed restriction preview (5 miles ahead of the train) resulted in increased safety, as measured by the number of speed violations and red signal violations, as well as reduction in fuel consumption. Askey (1995) examined the effects of providing varying levels of preview information on locomotive engineer awareness, safety, and efficiency. The study found that, as levels of information display increased, performance improved on a variety of measures, including station-stopping accuracy, schedule adherence, and reaction time to unexpected signal changes. Finally, Einhorn et al. (in press) evaluated preview displays that provided upcoming speed restrictions, location and velocity of nearby traffic, and upcoming distance cues (e.g., mileposts, switches, and stations). The study manipulated the amount of look ahead (1.5 to 3.4 miles and variable look ahead). The results showed that preview displays improved performance on a number of train control tasks, including routine speed control, signal adherence, brake reaction time latency, and schedule adherence. Performance was best for variable preview where the amount of look ahead varied as a function of train speed.

Interviews with locomotive engineers of PTC systems indicated that the engineers perceived preview information as valuable to improve safety and efficiency, independent of the predictive braking aspect of PTC. ITCS locomotive engineers felt that the display of milepost reinforced their mental model of the territory and provided important safety benefits in poor weather with limited visibility. Similarly, Amtrak staff that were interviewed regarding the IDOT system indicated that the IDOT display of the up-coming track and their location on the track would be very useful in helping them operate the train in cases where outside visibility was poor (e.g., in fog or at night). The preview information is expected to aid locomotive engineers in operating trains at higher speeds (e.g., above 79 mph) where there is less time available to process and respond to information outside the window.

Concerns Raised

The PTC system may shift the engineer’s attention from events occurring outside the locomotive cab to in-cab displays. This shift in attention may cause the locomotive engineer to miss key events out the window, creating a new source of safety risk.

Implications

Allocating more attention on in-cab displays at the expense of events outside the window must be addressed in any safety analysis. A combination of more comprehensive training and improved in-cab displays can address this concern. Person-in-the-loop evaluations of the final PTC design can be conducted to establish whether out-the-window performance is substantially impaired by the need to closely monitor the in-cab display.

Interviews with locomotive engineers suggest that a substantial learning curve exists to reach the point where the in-cab display does not serve as a source of distraction, diverting attention away from events out the window. Locomotive engineers must have sufficient experience in running a PTC-equipped train as part of training so that they get beyond the point where close monitoring of the in-cab display is required to avoid a penalty brake application.

A valuable area for research and development is improved in-cab displays that minimize the need to visually attend to the in-cab display to extract important information. It would be desirable to develop alternative display approaches for indicating to the locomotive engineer where train speed is in relation to the desired deceleration rate without having to closely monitor the visual in-cab display. Options to explore include the use of non-visual display modes, such as auditory or tactile displays (Sklar and Sarter, 1999).

Current PTC displays vary widely in the amount of preview information they provide. More guidance is needed on the contribution of preview information on safety. Evidence from simulator research suggests that preview information may have a beneficial effect on safety independent of the predictive braking aspect of PTC. More research is needed to explore the relative risks and safety benefits associated with preview information displays (that may divert attention from out the window) and to develop guidelines for the design of displays that provide valuable preview information without excessively diverting attention from out the window.

3.1.3 New Sources of Workload

The PTC system creates new sources of workload and distraction. Sources of workload and distractions include the need to acknowledge frequent (and often non-informative) audio alerts generated by the PTC system and the need for extensive input to the PTC system during initialization and when error messages occur while operating the train.

3.1.3.1 Audio Alerts as a Source of Workload and Distraction

IDOT and ITCS locomotive engineers raised the issue of too many audio alerts and the need to acknowledge them as a potential workload problem.

IDOT locomotive engineers mentioned a specific example that occurred during a set of test runs. The PTC system includes a train location determination system (LDS) that is able to locate train position within 10 feet. However, on a couple of occasions, the LDS system experienced difficulty identifying the train location. This difficulty triggered an LDS failure alarm. The alarm beeped repeatedly and required the locomotive engineer to press a button several times to acknowledge the alarm. The operational personnel expressed concern that this resulted in a heavy workload. It required two people to handle the situation. One person acknowledged the alarms while the other continued to operate the train. This was an early test of the system, and no consequences of failing to respond to the alert occurred. In an operational system, failure to respond to an alert quickly might result in a penalty brake.

ITCS locomotive engineers mentioned a similar concern with too many audio alerts that need to be acknowledged, creating unnecessary distraction and workload. One engineer mentioned that, during the design process, he had removed some alerts based on recommendations of the locomotive engineers. He indicated that the system provided audio alerts to signal permission to resume speed, as well as upcoming speed restrictions. He suggested that limiting alerts to warning of potential problems (e.g., an upcoming speed restriction that might be missed) and avoiding their use for positive situations (e.g., when a speed restriction is no longer in effect).

Experiences of European railroads suggest that the concern expressed by the locomotive engineers regarding too many non-informative alerts is a legitimate concern that has a real potential for negative safety consequences. Operators may respond to poorly designed audio alerts automatically without fully processing their meaning thus defeating their purpose (Pasquini et al., 2004).

A recent analysis of signals passed at danger (SPADS) in Italian Railways suggests that computerized systems intended to provide in-cab alerts of upcoming stop signals, if poorly designed, can fail to serve their intended alerting function (Pasquini et al., 2004). In the case examined by Pasquini et al. (2004), a locomotive engineer missed a stop signal in spite of an in-cab display system that provided an auditory warning of upcoming stop signals and required an explicit acknowledgement of the alert (via a button push). The analysis conducted by Pasquini showed that, because of the way the alert system was designed, it promoted a tendency to automatically press the acknowledgement button when the alert came on without actually processing the alert message. As a consequence, even though the locomotive engineer received and acknowledged an in-cab alert indicating an upcoming stop signal, he did not know he was approaching a stop signal.

Analysis of the case reveals how poor alert system design can cause a system to lose its alerting function. One problem with the system was that the alerts were generally uninformative. The system attempted to predict the signal aspect for the next block and provide a warning, but in many cases the prediction was inaccurate. Typically, when a train entered a block (block n-1), the system would alert the locomotive engineer that the signal for the next block (block n) would be an approach signal. In most cases, the signal would turn to clear before the train reached the next block. As a consequence, experienced locomotive engineers perceived the system as a noisy distractor that must be silenced as soon as possible. Observation of train crews revealed that, as they approached a block, experienced locomotive engineers tended to look out the window with their fingers on the acknowledge button, ready to press it as soon as the auditory alert came on. They pressed the acknowledge button automatically without looking at the in-cab display that indicated whether the next signal was predicted to be approach or stop. Since the auditory sound was the same for stop and approach signal alerts and the acknowledge button was the same in both cases, the locomotive engineers acknowledged the alert without processing whether the predicted signal aspect for the next block was stop or approach.

This example points to several important principles for design of effective alerting systems. Most importantly, the alerts must be accurate and informative. One of the most frequent problems with alerting systems is that they have a high false alarm rate, which causes users to ignore them. Second, if an audio alert is used in an environment where the user needs to look somewhere other than the display screen (in this case, locomotive engineers need to look out the window), then it is advantageous to use different audio signals to correspond to different alerting conditions (e.g., a different tone for approach versus stop). Third, if users must acknowledge an alert, they are less likely to respond automatically if different actions are required for different alert messages (e.g., a different button push for approach versus stop alerts).

More generally, this example highlights why it is important when doing a reliability analysis to examine how a system is actually used in practice rather than relying on a hypothetical model of how the system is envisioned by the system designers. When the designers developed the system, it appeared to be foolproof. While the designers thought that engineers might miss a signal through lack of attention, they felt that requiring the engineers to acknowledge the alert would insure that they saw the alert message and would act on it. Analysis of how actual experienced locomotive engineers perceived and used the system revealed a very different model of use that was more vulnerable to error.

An alert system that has a high false alarm rate may be disabled, particularly under high workload conditions. Data reported by Einhorn et al. (in press) suggests that this is a legitimate concern with potential for negative safety consequences. The report discusses the problem of alarms as a source of workload and mentions comments made by the locomotive engineers participating in the study. One of the Amtrak engineers complained about the amount of electronic harassment in modern locomotive cabs. He related that many engineers cut out (turned off) the cab signaling and Automatic Train Protection (ATP) in low-speed territory to remove the distraction of the warnings and focus their attention on very fine control of the train’s speed. However, the danger is that they forget to turn it on when they return to high-speed territory.

Concerns Raised

If alerts are poorly designed so that they produce a lot of uninformative alerts that need to be acknowledged, including the following:

- They may act as a source of distraction, causing locomotive engineers to miss important events occurring out the window.
- They may be responded to automatically (pressing the acknowledge button), eliminating their informative value.
- They may be cut out, defeating their safety function.

Implications

Poorly designed alarms can create a source of workload and distraction and should be addressed as part of a safety analysis. This concern can be addressed through a careful user interface design and review process that minimizes uninformative or low importance nuisance alerts. Including system users (i.e., locomotive engineers) early in the design process can help in this regard, as can dynamic, person-in-the-loop tests of the system to establish that it does not impose undue workload and distraction.

3.1.3.2 Initialization/Interaction with PTC as a Source of Workload

PTC systems generally require manually entered inputs at the start of a trip and after a shutdown of the system during train operations. The train crew must enter information that the system will use as parameters for safe operation. These data entry tasks provide another source of workload and distraction. In addition, manual entry errors can have safety implications.

One example relates to initialization of the PTC system at the start of a train trip. The complexity of the information to be entered varies with PTC system. The IDOT PTC system provides an example of a system that involves extensive input. At the start of a trip, the train crew must enter information about the train, its consist, and what track it is on into the PTC system. While the data to be entered is straightforward, the data entry task creates additional workload. As a consequence, operating rules must take this additional workload into account. When the authors conducted the interviews with IDOT PTC operational staff, the detailed operating rules and procedures were still to be developed. The authors raised the question of initializing the PTC system when the train was stopped or running. Amtrak personnel felt that, in the case of Amtrak trains where only one person is in the locomotive cab, the train would need to be stopped.

Another example is the need to re-initialize the PTC system after it has initiated a penalty brake. If the procedure is complex and time consuming, it may not be practical to follow. This issue arose in discussions with New Jersey Transit/ASES locomotive engineers. When a penalty brake occurs, the locomotive engineers must cut out ASES and inform the dispatcher. They are then supposed to restart ASES. A procedure exists for cutting ASES back in, but the procedure is complex, difficult to follow, and time consuming. As a consequence, the locomotive engineers typically do not attempt to cut ASES back in. Instead, with the dispatcher’s permission, they run the train without ASES operating. They are able to do this because the system is still in trial use and not required to operate the train. Once the system becomes fully operational, running a train without ASES activated may no longer be an option.

Concerns Raised

If the added workload associated with interacting with the PTC system is not appreciated by management and accommodated through carefully designed operating rules and procedures, then it can introduce a new source of risk. The safety risk can arise because the workload can serve as a distraction leading to important signals being missed (e.g., if the locomotive engineer is required to initiate the PTC system while the train is running) because it leads to a data entry error or because the PTC system may be cut out or not cut back in when it stops.

Implications

The added workload associated with initializing and restarting the PTC system should it stop in the middle of a trip must be addressed as part of a safety analysis.

Ways to address this concern include design and testing of the user interface to insure that the workload imposed is manageable. This includes minimizing the number of steps and complexity associated with initiating and restarting the PTC system and making error messages and what to do when those error conditions arise easy to understand and follow.

Railroads may need to create or modify operating rules to accommodate the additional sources of workload (e.g., in the case of train runs with one person in the cab that the initiation of the system will be done when the train is stopped).

3.1.4 Potential for Complacency

Another concern that has been raised regarding the introduction of PTC systems is that locomotive engineers will come to rely on the PTC system to alert them of upcoming speed and authority limits and to automatically stop the train should they fail to do so themselves. The concern is that, should the system fail, the locomotive engineers will not perform as well without it as they would have had the system never been installed. Complacency has been used as a label to refer to this problem (Sheridan et al., 1999). It serves as an umbrella term that combines several concerns, including concern that the train crew may not recognize that the PTC system has failed (or is off) and is thus no longer providing the level of support they are expecting; concern that the train crew may be delayed in detecting and responding to PTC system failures; and concern that the crew may lose skill due to lack of practice, and thus may not be able to perform tasks as well when the system is not available as they would have, had they been performing the tasks all along without aid of automation.

The term complacency comes out of the human factors literature; however, it is not a well-defined and universally accepted concept (Moray, 2000). This is partly because it has a pejorative connotation. Complacency seems to blame the person for unreasonably relying on automation and is closely related to the concepts of over-reliance and over-trust. One can define complacency as relying on automation to a greater degree than is warranted by its objective level of performance. As has been pointed out by several prominent researchers, given the many things that people must attend to at any given time, if a system is known to be highly reliable, it is reasonable that people should come to rely on it to function properly without needing to constantly check on its performance (Moray, 2000; Sheridan, 2002). A review of studies of trust in automation suggests that, rather than being overly complacent and trusting in automation, people tend to be less trusting of the automated system’s performance than is deserved by the actual reliability of the system (Moray, 2000).

To make progress the authors must carefully define the term complacency. In the context of railroad operations, complacency refers to the potential for people to become reliant on a job aid that is intended as a back up (like PTC), such that when it fails to work (or does not work as expected), the people are more likely to fail than if the job aid had never been installed. Review of actual incidents and comments by locomotive engineers during the interviews suggests that this is a legitimate concern.

Potential and real examples of complacency have been identified from the operating experience of PTC systems, though none have been identified as leading to an accident (UFF, 2000). Complacency was identified as the most likely cause of one of the major rail accidents in the United Kingdom: the collision of a high-speed passenger train (HST) with a freight train on the approach to Paddington Station (London, UK) at Southall in September 1997. The following describes this incident and how complacency may have played a role.

Example of Event: Southall

While approaching Paddington Station on September 19, 1997, an HST in service from Swansea passed through a sequence of three signals, each of which indicated a need to slow and stop before an interlocking. The signal system was set for an oncoming freight train to cross in front of the HST (Uff, 2000). The engineer did not slow the train at any of the signals and only appeared to react when he saw the freight train crossing in front of him at a distance when it was impossible to stop. The subsequent collision occurred at a closing speed of between 80 and 100 mph and resulted in 7 passenger fatalities and 139 injuries. The engineer of the HST survived with minimal injuries.

The HST, like most other British trains, was equipped with an automatic warning system (AWS) that warned the engineer if he was passing any signal that was more restricting than clear by sounding a warning and displaying a visual indication. By acknowledging the AWS, the engineer can continue to pass the signals; no enforcement of the signals occurs if the warning is acknowledged (and is thus not a PTC equivalent system). However, on the day of the accident, the AWS failed (and was known to be failed) in the leading cab of the HST as it traveled to Paddington Station.

The engineer operated the train appropriately up to the point of the accident, including obeying signals and speed limits. However, when interviewed immediately after the accident, the engineer recalled being preoccupied with getting his bag ready for arrival at Paddington Station—the terminus of the journey about 5 minutes from Southall. He received no warning from the failed AWS of passing the signals set to yellow and red as he approached the interlocking.

The following passage is taken from the inquiry’s report:

> While drivers [engineers] accepted the traditional view that AWS was merely an ‘aid,’ the reality was somewhat different, as the Southall accident has demonstrated. While it must be emphasized that the primary duty of a driver is to keep a vigilant lookout at all times, there must be a tendency for drivers, to an extent, to become dependent on the security of an automatic warning system on the approach to every signal. A full understanding of the effects of such systems depends on studies of human behavior in the particular environment of the driving

> cab, a subject that has so far received only limited attention. It can be concluded, however, that the absence of AWS was a contributory factor to the failure of Driver ------- to respond to signals SN280 or 270 at the crucial time (Uff, 2000).

This accident, plus the SPAD accident at Ladbroke Grove involving a passenger train leaving Paddington Station in October 1999 (Cullen, 2000; HSE, 2000), led the United Kingdom rail authorities to consider the extension of train protection systems (TPS), the equivalent of PTC systems in the United States, to provide much more coverage in the United Kingdom (Uff and Cullen, 2001).

Locomotive engineers interviewed at New Jersey Transit and ITCS felt that complacency was a legitimate concern. At New Jersey Transit they mentioned an anecdotal case where a complacency effect may have contributed to missing a signal in Cab Signal territory. In the case in question, the cab signal cut out. The locomotive engineer was aware that it had cut out. However, he was momentarily distracted (talking with a supervisor) and missed a signal. The locomotive engineers stressed that the individual it happened to was known as a very careful and conscientious locomotive engineer. This anecdote reinforces the point that complacency does not reflect a lack of conscientiousness but rather a tendency to come to rely over time on highly reliable and useful systems.

Concern Raised

If the PTC system is highly reliable by providing useful information that the locomotive engineer relies on, performance may degrade if that information becomes unavailable.

Implications

Locomotive performance under conditions where the PTC system is not functioning must be addressed in any safety analysis. This includes consideration of the potential for complacency effects and what actions have been taken to minimize the potential for complacency effects. Complacency effects include inability to recognize that the PTC system has failed, is off, or is in a different mode such that it is no longer providing the level of support they are expecting; delays in detecting and responding to PTC system failures; and loss of skill due to lack of practice.

Inability to detect whether or not the PTC system is activated and providing protection can be addressed through good user interface design principles to ensure that train crews can rapidly and unambiguously determine whether the PTC system is functioning correctly and what mode it is in.

One way to mitigate against loss of skill is to provide periodic training in controlling the train with the PTC system off, either in a simulator environment or through specific training in revenue service.

In addition, specific operating rules may be required to handle the case of running a train with a non-operational PTC system when the locomotive engineer is normally used to running the train with a functioning PTC system.

3.1.5 Potential for Loss of Control

Locomotive engineers expressed concern that the PTC system takes control away from the person and that the system is not always aware of all the factors that must be considered in braking decisions. In some situations, the automated braking curve generated by the PTC system may be inappropriate. In other cases, it may initiate a penalty brake unnecessarily. If these system actions arise at the wrong time or place, it can have negative safety consequences.

Locomotive engineers pointed out that PTC systems only know about the speed restriction coming up. PTC systems do not take into account all the relevant factors that are important to braking. As a consequence, the PTC system may impose an inappropriate braking curve. For example, locomotive engineers mentioned environmental conditions as one set of factors that that may make the tracks unusually slippery. This includes wet tracks and tracks with leaves on them. One locomotive engineer experienced with ASES explained that wet leaves on the track requires changing braking style entirely. He said that when there are leaves on the track, the operator must slow down much earlier than usual. As a result, the operator will need to enter the braking curve earlier than ASES requires. Equally importantly, the operator cannot slow down as fast as the ASES braking curve requires because slowing down too fast can cause the train to slide, creating the potential for a derailment.

A number of cases have been documented where the PTC system initiates a penalty brake under conditions where it was not warranted and may in fact create a potential for a safety hazard. Some examples mentioned include the following:

- Cases where the PTC system requires the locomotive engineer to reduce speed faster than is physically possible. Locomotive engineers gave several examples of situations where the PTC system received a signal indicating a need to slow down at the last minute, where the request could not be physically met and was unnecessary. For example, if a train is coming to a crossing and communication between the engine and the crossing is lost, ITCS detects this (a poor health indication) and requires that the train slow down to 15 mph. The train could be 45 or 50 feet from the crossing when this happens and unable to reduce speed in time. ITCS initiates a penalty brake creating a potential for a derailment.
- Risk of derailment is of particular concern for long and heavy freight trains. Initiation of a penalty brake takes away the throttle, which is an important source of control for the engineer to use to keep the train cars from bunching up.
- Cases where the PTC system requires the train to slow down when it needs to be picking up speed (e.g., a freight train on upgrades).

The locomotive engineers argued for the importance of being given the authority to suppress a penalty brake under conditions where it is inappropriate and potentially a safety hazard.

Concerns Raised

The main concerns raised relate to loss of control by the locomotive engineer and potential for new sources risk because of inappropriate braking curves and inappropriate activation of a penalty brake.

The PTC systems that this report examines were all in the early development or initial implementation phase. As a consequence, if the locomotive engineer thought that the PTC system was not operating appropriately, it was acceptable for the locomotive engineer to cut out the PTC system and continue operating (after notifying the dispatcher).

If the operating practices are changed so that it is no longer possible to turn off the system if the locomotive engineer judges it to be malfunctioning, then automation-induced accidents may result. Such an accident occurred on January 5, 1996, at the Shady Grove Road station on the Red Line of the Washington, DC metro system (National Transportation Safety Board, 1996). The accident occurred partly because rules prevented the engineers from taking manual control of their train's speed except in an emergency. On that day, trains were experiencing slippery traction and were in some cases over-running stations. The locomotive engineer on the train in question requested to cut out the automatic speed control system and was told he could not do so. An unexpected side effect of over-running the stations was that the automatic speed limits imposed because of the snowy weather were over-written. As a result, the train, under automatic control, approached the Shady Grove Road station much faster than was appropriate for the weather conditions and was unable to stop because of the speed and the poor adhesion to the track. As a result, it collided with a stationary train, and the engineer was killed. Had the locomotive engineer been allowed to over-ride the automation, the accident may have been avoided.

Implications

The potential for automation-induced accidents must be addressed in any safety analysis. This includes an analysis of conditions where the braking curve generated by the PTC system may be inappropriate or where inappropriate initiation of a penalty brake may create a safety hazard. The safety analysis should also address under what conditions the locomotive engineer may over-ride the PTC systems.

Ways to reduce the potential for automation-induced accidents include improving the PTC braking algorithms so that they are closely tailored to the specific conditions of operation. In addition, it is important to put in place mechanism to allow the locomotive engineer to over-ride the automation and supporting operating rules that specify the conditions under which the engineer may over-ride the automation. Situations will inevitably occur that are different than what the system designers anticipated and planned for. It is important to provide some discretion to the locomotive engineer on the scene, to deal with these unanticipated situations.

3.2 Other Sources of New Problems

3.2.1 Reliance on Manually Entered Data

Some PTC systems rely on manual entry of information as part of the system initialization process. For example, some PTC systems require the locomotive engineer to provide information about the train consist, which is used to compute the required braking profile. Some systems require the locomotive engineer to indicate which track the train is on. The manually entered data may be subject to human error. The earlier discussion with locomotive engineers working with IDOT and CBTM focuses on this issue.

Some systems rely on the locomotive engineer to indicate which track they are starting on. Should the locomotive engineer make an entry error, the PTC system would not be able to serve its protective function. For example, the data entry error may indicate that the train is on a different track (a parallel track) than it is on. In most cases, once the train is moving, the system is able to rapidly resolve what track the train is actually on and catch the data entry error; however, IDOT operations staff indicated that some special cases may exist (e.g., situations where there might be 200 miles of parallel track) where the PTC system would not be able to detect the data entry error for extended periods. The IDOT operational staff felt that this was a serious issue, as there could be equipment on the track or a slow order on the track. If the PTC system had incorrect information as to what track the train was on, it would not be able to protect them.

A similar concern relates to the accuracy of the consist information entered into the PTC system as part of the system initialization process. Systems may require the locomotive engineer to manually enter information about the train consist (e.g., number of cars, content, and weight). Other systems, such as the IDOT system, download consist information from existing non-vital data bases and have it confirmed by the train crew as part of the initialization process. However, there was concern that errors in the consist information entered could affect the ability of the PTC system to protect the train. Locomotive engineers expressed concern that the information available to locomotive engineers regarding the content and weight of the consist is not always accurate or up to date. The accuracy of the existing consist databases may not be sufficient to be relied upon by a vital system such as PTC.

The problem is a particularly serious concern in the case of freight trains, where the length and weight of the train can vary greatly and significantly impact the train braking profile. Amtrak passenger trains have less weight variability and can brake more quickly.

Concern Raised

The possibility of human error in data entry may affect the reliability of PTC systems that depend on manually entered data.

Implications

Safety analyses should specifically address the impact of human error in data entry on PTC system reliability. Human factors design principles should be followed to reduce the possibility of data entry errors and facilitate detection and correction of errors. If locomotive engineers are required to enter information or if the information is extracted from existing databases (e.g., train consist information), then processes should be put in place to insure that the information is accurate and up-to-date.

Benefits may exist in exploring the possibility of having the PTC system actively estimate train length and train weight rather than relying on non-vital consist databases that may not be up to date or accurate.

3.2.2 Mode Transitions

Another area of concern relates to changes in modes of operation. Locomotive engineers may have difficulty transitioning between train operation with PTC and train operation without PTC.

Mode transitions fall into several types. One type of mode transition relates to operating a train that is equipped with PTC, but that, depending on conditions, has the PTC system active or not. PTC may not be operational on a PTC-equipped train because the train is outside of PTC territory or because the PTC system is malfunctioning. In the interviews, employees gave numerous examples of PTC-equipped trains that crossed in and out of territory where PTC coverage was available. For example, a freight train locomotive engineer operating an ITCS-equipped train mentioned that, when the train went off territory (e.g., in a business yard), the ITCS coverage stopped. The system did not come back on until the train returned to the main line and passed a control point. The train can travel up to 2.5 miles on the main track before the system came on. These interviews also revealed numerous situations where the PTC system became inactive because of a malfunction.

One concern with these kinds of mode transitions was that the locomotive engineer might fail to notice that the PTC system was inactive and no longer providing protection. Alternatively, the locomotive engineer may recognize that the PTC system was unavailable but fail to increase vigilance sufficiently to compensate for the lack of PTC protection. These concerns were similar to the concerns raised in the earlier section on complacency. The locomotive engineers will not perform as well when the PTC is not activated as they would have had the system never been installed because they have come to rely on it.

Interviews with locomotive engineers suggest that the possibility of failing to realize that the PTC system is no longer operational is likely to be low. Typically a prominent visual cue occurs, indicating when the PTC system is operational. Locomotive engineers reported no trouble telling whether the PTC system was active or inactive. The question of whether locomotive engineers come to rely on the PTC system, and therefore perform less well when it is unavailable than they would have had it never been available, is unclear. The earlier section on complacency addresses these issues.

A second, related mode-transition issue involved locomotive engineers that operated on both PTC territory and non-PTC territory. Examples include locomotive engineers working on the extra-board that might be called to operate PTC-equipped trains on PTC territory, as well as non-PTC equipped trains on a different territory. The concern is how easily the locomotive engineer can switch between the two types of operation and whether any negative transfer occurs in going from operating PTC-equipped trains to non-PTC equipped trains and vice versa.

Concern Raised

Locomotive engineers may have difficulty transitioning between train operation with PTC activated and train operation without PTC, resulting in decreases in reliability at points of transition.

Implications

Safety analyses should explicitly address the types of mode transitions that are likely to arise in operation and the steps taken to reduce the possibility of problems at mode transitions.

Mode transitions that need to be considered include the following:

- PTC-equipped trains transitioning into and out of PTC territory
- PTC-equipped trains running on PTC territory without PTC activated (e.g., due to a malfunction)
- Locomotive engineers who normally operate on non-PTC territory operating on PTC territory and vice-versa (e.g., locomotive engineers on the extra-board)

As in the case of complacency, performance impacts of mode transitions can be minimized through a combination of user interface features that provide unambiguous cues as to whether the PTC system is active or not and training that provides practice in running trains with and without PTC. This includes comprehensive initial training as well as periodic refresher training.

3.2.3 Impact on Teamwork Processes

Another issue to consider is the impact of the PTC system on teamwork processes among members of the train crew, including the locomotive engineer and the conductor. If the display is poorly designed or poorly located, it can interfere with the ability of team members to serve as a mechanism to catch and recover from errors. For example, in cases where there are two people in the cab (e.g., a locomotive engineer and a conductor), the second individual is charged with serving as a redundant check/reminder to the locomotive engineer running the train. This includes calling out signals as they are seen and providing reminders of upcoming speed restrictions. If the PTC display is placed in a location so that only the locomotive engineer can see the display, it reduces the ability of the second individual in the cab to provide a redundancy check. Pasquini et al. (2004), reviewing an Italian cab signal system, reported that the location of the cab signal interface did not allow the second locomotive engineer in the cab to read off the alert messages, thus reducing his or her ability to detect when a locomotive engineer was about to violate a signal. A similar issue was raised during the interviews with locomotive engineers and conductors regarding the CBTM system. Several of the individuals interviewed argued that it would be helpful to place CBTM displays on the conductor’s side, as well as the side of the locomotive engineer, so that the conductor could better support the locomotive engineer.

Concern Raised

If a system is poorly designed or poorly located, it can disrupt teamwork and interfere with the ability of team members to catch and recover from errors.

Implications

Safety analyses should specifically address who will be the primary user of the PTC system and what role, if any, other crewmembers are expected to play, with respect to monitoring and acting upon PTC displayed information. If crewmembers other than the locomotive engineer are expected to read and respond to PTC messages (e.g., to serve as a redundancy check), then the display must be placed in a location where they can easily see it.

3.2.4 Interaction with Operating Rules

Introduction of new PTC systems will necessitate changes to operating rules. New operating rules must be written to cover procedures required to operate the PTC system and handle different contingencies that can arise. Modifications to existing procedures may also be needed to accommodate new PTC capabilities and constraints.

New rules and procedures will need to be associated with the introduction of the new PTC system. An example is specification of procedures for when and how to initiate the PTC system (e.g., is it done while the train is stopped or can it be done when the train is moving?). The various failure modes that can arise must be defined, and operating rules must be written to cover those contingencies. Interviews with ASES and ITCS locomotive engineers indicated that PTC error mode indications can be difficult to understand, and the procedures for re-initializing PTC after a failure has occurred can be complex and time consuming. The operating rules must be easy to understand and practical to follow.

Cases may occur where the behavior of the PTC system is inconsistent with the requirements in the rulebook. In those cases, the railroad will need to reconcile the behavior of the PTC system and the rulebook. This may involve adjustments to the rulebook to accommodate new capabilities provided by the PTC system. One of the ITCS locomotive engineers provided an example where an inconsistency existed between the rules as specified in the rulebook and how they were being enforced by the PTC system. The rule in question dealt with dark signals where the signal light is out. Northeast Operating Rules Advisory Committee (NORAC) rules specify that the train should stop and contact the dispatcher. ITCS, however, did not enforce this rule because ITCS is able to infer the signal, even though the signal light is out, because it senses the signals up to two blocks ahead. The PTC system and the rulebook must be reconciled to not place locomotive engineers in a dilemma situation where they must decide whether to follow the rulebook or assume that the PTC system takes precedence. In this particular case, the locomotive engineer suggested that the information provided by ITCS regarding the signal is reliable whether or not the signal light is there. As a consequence, he felt that it would be appropriate to modify the NORAC rule so that it does not require a train equipped with PTC to necessarily stop at a dark signal.

Concern Raised

If rulebooks are not updated to accommodate the new capabilities of PTC systems and to provide practical procedures for handling the different contingencies that can arise, then inconsistencies may emerge between the procedures specified in the rulebook and actual operation.

Implications

Safety analyses should address interaction of PTC with operating rules. This includes specification of new operating rules that have been developed to cover operation of trains equipped with PTC under different contingencies (e.g., initialization of the PTC system, malfunctioning of the PTC system, or running a PTC-equipped train when the PTC system is disabled). Ideally, the rules should have been developed with input from operations staff (e.g., locomotive engineers), and the comprehensibility and workability of these rules should have established through field tests.

Safety analyses should also address the impact of the PTC system on existing rules and how inconsistencies between existing rules and PTC operation, if any, have been reconciled.

3.2.5 Issues Impacting Freight Operations

Freight operations impose more of a challenge for the application of PTC than passenger trains. Freight trains are longer and heavier, complicating braking decisions. ITCS and ASES locomotive engineers expressed concern that simple, conservative braking profiles that may work in the case of passenger trains may not work well in the case of freight trains, reducing efficiency of freight operations and in some cases impacting safety.

Freight braking has more dynamic variables must be considered in determining when and how to brake. Considerations that enter into braking decisions of locomotive engineers include the following:

- Number of cars (can be up to 200 cars in a train)
- Mixture and distribution of loaded and empty cars

- Adhesion factors on the brake shoes and the wheels
- Terrain grade and undulation

The IDOT, ITCS, and ASES locomotive engineers interviewed all felt that the PTC systems applied more easily to passenger train operation than to freight operations. One concern related to the use of a single or limited number of braking profiles for freight trains that were overly conservative, requiring the locomotive engineer to begin braking earlier than he/she would normally begin to apply the brakes. The locomotive engineers indicated that, in some instances, the braking requirements were inappropriate, impacting efficiency and in some cases safety. A major concern related to hilly territory where braking prematurely could make it difficult to get up the hill, could result in stopping at an inappropriate location (e.g., a grade crossing), or could result in loss of air brakes. An example given was a case of a steep grade where, in order to stay below the braking curve, the locomotive engineer needed to repeatedly apply the air brakes to the point where eventually not enough air was left in the brake line to stop the train at the end of the authority.

Another related issue is that freight trains use dynamic brakes, as well as air brakes, for slowing down a train. However, PTC systems generally do not sense dynamic braking. As a consequence, freight train operators must modify their braking techniques when operating PTC-equipped trains. An ITCS locomotive engineer mentioned that Norfolk Southern generally encouraged freight train engineers to use dynamic braking for slowing trains down whenever possible. Air brakes were primarily to be used when stopping a train. However, the ITCS system requires the use of air brakes to stay within the ITCS braking profile. As a consequence, the railroad modified the rulebook to deal with this situation. A special set of instructions were issued for engineers in the freight railroads that operate over Amtrak lines indicating that they are to use air brakes over dynamic brakes. This example brings up several issues discussed in earlier sections, including the following:

- A need for locomotive engineers to modify their braking strategies (a training and practice issue)
- An interaction between PTC operation and existing rulebooks requiring a need to modify existing rule books to deal with special cases that arise with PTC systems
- A type of mode transition involving a change in the operating rules that apply as a freight train locomotive engineer moves in and out of Amtrak territory

Concern Raised

Freight train braking decisions are complex, involving multiple, dynamically changing variables. PTC systems that use one-size-fits-all conservative braking profiles may result in reduced efficiency of freight operations and could in some cases impact safety.

Implications

Safety analyses should address the special concerns that arise with freight operations. This includes establishing, through field tests, that the PTC systems are able to handle trains of variable length and distribution of empty and loaded cars, on terrain of different grades and curvature.

3.3 Training

Introduction of PTC systems impose new training requirements for locomotive engineers. First, training is needed to understand how the PTC system works (technical theory). Second, training is needed to understand how to operate the PTC system under different conditions (e.g., how to initialize it, what the different PTC displays mean, what error modes might arise, and what to do in those different conditions) and the applicable rulebook operating rules (PTC operations). Third, hands-on experience is required to learn the new train handling and braking strategies required to operate a PTC-equipped train to run efficiently while staying within the PTC braking profile (hands-on train handling).

Interviews with ITCS and ASES locomotive engineers indicated that current training typically involves a combination of classroom instruction on how the PTC system works followed by several trips with an experienced engineer. The interviews showed that the classroom training gave the engineers a solid foundation on how the equipment worked but that more hands-on experience was needed in running a PTC-equipped train.

Several locomotive engineers indicated that one of the limitations of current training is that it does not provide sufficient opportunity to develop the new train handling and braking skills required to operate a PTC-equipped train. It also does not provide sufficient experience with non-routine situations (e.g., different malfunctions) and how to deal with them. One of the locomotive engineers suggested providing an opportunity for trainees to operate a PTC-equipped train in a more controlled environment (e.g., run a test train or a train simulator) where they would be able to practice train-handling skills without concern of the consequences of inadvertently initiating a penalty brake. Another advantage of running in a controlled environment such as a test train is that it would be possible to simulate different types of rare conditions that can arise so that the trainee could learn what displays would come up (e.g., what error codes appear) and how to handle the situation.

Another issue raised with respect to training is the need to train crews to run the trains without the PTC system on so that, if the system ever fails, the engineer will still be able to run the train safely. A concern raised was that the locomotive engineers might become dependent on the PTC system to the point where they would not be able to run the train safely without it.

It may be possible to selectively turn off some of the features of the PTC in-cab display to provide practice in running the train without them. For example, one of the lead engineers of the IDOT display suggested that some of the PTC interface features, such as the 6-mile track look ahead display on the bottom of the screen, could be selectively turned off. While the track look ahead is likely to be a very useful feature for supporting situation awareness of the locomotive engineer, especially when outside visibility is low (e.g., in fog or at night), it may be useful to turn it off during some portion of training to insure that the train crews develop their own mental models of the track so that they are able to operate safely in cases where the PTC system is unavailable. Train crews may want to operate with the PTC system inactivated for selected trips during revenue service to maintain their territory knowledge as well.

Concerns Raised

Several concerns associated with insufficient training exist. One concern is that, if a locomotive engineer does not have sufficient experience in operating a PTC-equipped train, increased risk due to inappropriate train handling or braking may exist. Increased risk due to the inability to recognize unusual circumstances and know what to do may also exist (e.g., if a PTC error code appears).

Another concern relates to train operations in cases where the PTC system is unavailable (e.g., because of a malfunction). The concern is that, if train crews are inexperienced in operating a train without PTC, their performance may degrade, leading to increased risk.

Implications

Safety analyses should address the kind of training to be provided to train crews who will be operating PTC-equipped trains. This includes the following:

- New engineers
- Experienced engineers who are learning to run a PTC-equipped train
- Transferring in and occasional staff, such as crews on the extra-list who may only occasionally operate a PTC-equipped train

Training should include sufficient hands-on experience in running a PTC-equipped train to develop the necessary train handling and braking skills required to operate a PTC-equipped train so as to be able to run efficiently while staying within the PTC braking curve. Training should also provide sufficient exposure to unusual conditions to insure that the locomotive engineer will be able to recognize and know what to do should they arise.

Training should also cover operation without the PTC system to insure that the train crews can run trains safely in conditions where the PTC system is non-operational. This may require periodic refresher training in running a train with the PTC system inactive.

4. Maintenance-Related Safety Concerns

Section 2 focused on issues related to the performance of train crews and their potential impact on the reliability and safety of PTC systems. Another important contributor to system reliability and safety is the performance of system maintainers. This includes the performance of signalmen who maintain the wayside equipment, maintenance-of-way workforce, as well as the performance of cab mechanics who maintain the in-cab PTC systems.

Experience from other industries indicates that maintenance errors can be an important contributor to risk. Hobbs (1999) reports that approximately 15 percent of major aircraft accidents involve maintenance error. In the nuclear power plant industry, maintenance errors account for approximately half of human performance problems associated with potentially serious events (Reason and Hobbs, 2003).

Based on a review of maintenance accidents and incidents across a variety of industries, Reason and Hobbs (2003) identified the following factors that repeatedly emerge as contributors to maintenance errors:

Manuals and Procedures: Guidance documents, such as manuals and written procedures that are ambiguous, inaccurate, incomplete, or too technical, are likely to promote errors. Procedures that are unworkable or unrealistic are likely to lead to procedure violations and workarounds. In the nuclear industry, nearly 70 percent of all human performance problems have been traced to poor manuals and procedures.

Training and Experience: Lack of training or insufficient training or experience can result in error due to lack of knowledge or skill.

Tools and Equipment: Lack of appropriate tools and equipment is one of the most commonly cited contributing factors to maintenance performance problems.

Coordination and Communication: Problems in communication and coordination (e.g., between different crafts or across shifts) is another leading contributor to maintenance error. In an Australian survey of aircraft maintenance, 12 percent of maintenance errors involved problems, such as misunderstandings, poor teamwork, or incorrect assumptions (Reason and Hobbs, 2003).

Time Pressure: Maintenance personnel often face pressure to get a system (e.g., aircraft, locomotive, or power plant component) back in service as quickly as possible. Time pressure can cause individuals to hurry or take shortcuts, resulting in errors. In an Australian survey of the aircraft maintenance personnel, time pressure was the most frequently mentioned factor leading to incidents. In addition, 32 percent reported that, on occasion, they had not done a required functional check because of lack of time (Hobbs, 1999).

Physical Ergonomics: Another source of problem that has been reported in the general literature on maintenance errors relates to the physical ergonomics of a system, the design of the physical aspects of the equipment, and the physical environment in which the maintenance activities take place. If the equipment that needs to be maintained is hard to reach, hard to grasp, or hard to see and requires the person to get into or maintain awkward physical positions, it can lead to physical fatigue, injury, and maintenance error (Reason and Hobbs, 2003).

Fatigue: Working while fatigued can lead to error. After 18 hours of being awake, mental and physical performance on many tasks is affected as though the person had a blood alcohol concentration of .05 percent (Reason and Hobbs, 2003).

As part of the present study, the authors interviewed system maintainers of ASES and ITCS to explore potential maintenance-related safety concerns. The authors conducted interviews with signalmen who install, test, and maintain the wayside equipment and mechanical department personnel who install test and maintain the in-cab systems. The interviews explored the extent to which the types of factors that have been previously identified to impact maintenance performance apply to the maintenance of the PTC systems. The interviews also probed for any additional safety-related factors associated with the maintenance of advanced train control technologies. The sections below summarize the primary maintenance-related safety concerns that emerged.

4.1 Availability and Quality of Support

4.1.1 Training

The quality of the training provided is important in enabling maintenance personnel to maintain new equipment. The maintenance personnel all felt that the training they were provided was insufficiently in-depth. In some cases, training was relatively brief (on the order of 4 hours) and involved a basic introduction given by a vendor representative that covered how the system worked and what it was supposed to do when it worked appropriately. The maintenance personnel all agreed that the training did not go into enough detail on how to diagnose and fix problems that arose.

The signalmen, who worked on the ITCS, reported that, at around the time ITCS was being installed, they received a grant from FRA for a general course in electronics. The course was given at a local technical college. It was 40 hours in duration and was designed to provide them with a basic level of knowledge in electronics. The signalmen reported that the course was extremely beneficial in enabling them to troubleshoot and maintain the ITCS wayside equipment, even though it did not cover ITCS equipment specifically.

One of the concerns that the ITCS signalmen raised was how to train new people who come on board who did not have the benefit of taking this basic course in electronics.

Concern Raised

Inadequate training of maintenance personnel can contribute to maintenance errors that reduce system safety and reliability.

Implications

Safety analyses should specifically address the training provided to maintenance personnel. This includes initial training when new systems are first installed, as well as ongoing training of new maintenance personnel as they come in.

The general shift to digital signal equipment from traditional relay-based equipment means that maintenance personnel will need training in the fundamentals of digital technology and its maintenance.

4.1.2 Availability and Quality of Maintenance Manuals

It is important to provide manuals that provide comprehensive guidance in how to diagnose and fix equipment problems that occur.

The maintenance personnel generally agreed that the manuals provided were incomplete, difficult to understand and follow, and not tailored to the task of troubleshooting the PTC equipment. The maintenance personnel reported that they experienced trouble with the reliability of the PTC systems and had difficulty localizing the source of the problem (e.g., was it because of a problem with the in-cab equipment, the wayside equipment, or both? Was it due to something the locomotive engineer did or did not do?). The manuals lacked sufficient guidance to isolate and repair these problems. Error codes that came up on equipment displays were often cryptic so that it was impossible to identify the fault. The manuals did not always provide sufficient help to understand the fault and what needed to be done to correct the fault.

One of the manuals (a manual for maintaining wayside equipment) specified bit level diagnostics down at the machine language level. The error codes provided diagnostics at the software level (e.g., a registered overflowed) rather than at the level required to troubleshoot the equipment. The manual appeared to be based on a final design review document that provided information intended to help troubleshoot the software design. The manual was not written specifically to be used by signal maintainers to troubleshoot the equipment.

The maintenance personnel also discussed the issue of the PTC systems continuing to be in the process of changing and that the manuals were not kept up-to-date. As a result, if the new software gave an error code, it may not have been reflected in the manual.

Concern Raised

Inadequate maintenance manuals can contribute to maintenance errors.

Implications

Safety analyses should specifically address the development, evaluation, and upgrade of maintenance manuals.

Manuals must be specifically written to support installation, testing, and maintenance of PTC equipment. The manuals should be comprehensive. They must cover all error codes that can appear and provide specific procedures for troubleshooting and correcting PTC system malfunctions. The manuals should also provide detailed procedures for differentiating problems that are because of in-cab equipment from problems that are due to wayside equipment.

User evaluations should be performed to establish that the manuals are complete, easy to understand, and followed by the maintainers that are supposed to use them. These tests should be conducted using actual system maintainers as test participants, and their feedback should be used to correct any problems identified.

Processes should be put in place for upgrading maintenance manuals when changes to the PTC system are made.

4.1.3 Quality of Support from Vendors

One point raised by the maintenance personnel interview was the quality of technical support from the vendors of the wayside and in-cab equipment. Vendors were responsible for initial training, preparation and updating of manuals, upgrading of equipment, and technical support in cases where problems arose that could not be solved.

In the case of all the groups interviewed, perceived problems existed in the equipment's reliability. In many cases, the error codes that came up were cryptic, and the manuals did not provide sufficient guidance to isolate and correct the fault. As a consequence, the maintenance personnel needed to contact the vendors for help in tracking down the source of the malfunction.

The groups interviewed had mixed reactions with respect to the quality of the technical support provided. The ITCS signalmen reported that they received good technical support from the vendor. They indicated that the vendor representatives were easy to reach and knowledgeable. Other groups indicated that the technical support from the vendors was not always sufficient. In some cases, the vendors indicated that the reliability problems exhibited by the system were difficult to diagnose and correct, even for the vendors. They indicated that everyone, vendors included, was in learning mode.

Concern Raised

Inadequate technical support by vendors can contribute to maintenance errors.

Implications

The quality of the technical support provided by vendors is important. This includes providing effective training, developing good maintenance manuals, and making available knowledgeable support personnel to aid in troubleshooting complex problems.

4.1.4 Availability of Testing Equipment

Lack of appropriate tools and equipment is one of the most commonly cited contributing factors to maintenance performance problems across industries. One of the primary tools for test and maintenance of advanced digital technology systems, such as PTC, are portable computers that serve as portable test terminals. These are carried into the field and used to test and upgrade software in both the wayside and in-cab systems.

The maintenance personnel mentioned a shortage of portable computers as a factor that limited productivity and turnaround time. Signalmen who used portable computers to perform transponder tests and mechanical department personnel who used portable computers for equipment testing mentioned this shortage in their interviews.

Concern Raised

Lack of appropriate test and maintenance equipment can impact the ability to detect and correct system malfunctions in a timely manner. This can impact system reliability.

Implications

It is important to insure the availability of test and maintenance equipment. This includes portable computers that are used out in the field to test and maintain wayside and in-cab systems.

4.1.5 Communication and Coordination

Problems in communication and coordination (e.g., between different crafts and across shifts) contribute to maintenance errors across industries. The maintenance personnel confirmed the importance of communication and coordination for timely and accurate diagnosis of PTC equipment problems.

Close communication and coordination are often required between personnel in the signal and mechanical departments to track down the source of abnormal PTC system behavior. In many cases, the system exhibited problems that occurred intermittently and thus difficult to track down. In those cases, close interaction was required between signalmen and mechanical department personnel to determine whether the problem was due to a malfunction of on-board cab equipment or wayside equipment. Both the ITCS and ASES maintenance personnel groups interviewed indicated that close communication and sharing of information existed between the two crafts in troubleshooting PTC systems.

Maintenance personnel also indicated that information from the train crew was also valuable in attempting to troubleshoot a PTC system malfunction. They suggested that it would help to have better documentation from the locomotive engineer explaining the context surrounding a malfunction (e.g., exactly when and where the malfunction occurred and what he or she saw out the window). Some information can be downloaded from the PTC system, but things such as what the crew saw out the window (e.g., wayside signal aspects) can only be obtained from the train crew.

In some cases, the maintenance personnel indicated that train crews needed to fill out forms explaining malfunctions that occurred during a trip but that the maintenance personnel did not always get a copy of the form.

In some cases, the maintenance personnel called the locomotive engineer on the radio to find out where the problem occurred and the context in which it occurred. Sometimes it was hard to track down the locomotive engineer (e.g., because of rest days). In some cases, days went by before the maintenance personnel spoke with the locomotive engineer, by which point the locomotive engineer may have forgotten the details of what happened.

Concern Raised

Problems in communication can result in delays in tracking down and correcting system malfunctions. These problems can also contribute to maintenance errors that reduce system safety and reliability.

Implications

Communication and coordination among different crafts is important to rapidly track down and correct system malfunctions, particularly in cases where the system malfunction is difficult to reproduce and localize. Procedures should be put in place to ensure that train crews document the contextual details surrounding a malfunction that are not automatically recorded by the system and are important to tracking down the source of a problem and that this information is passed to the maintenance personnel.

Sharing of information and joint troubleshooting by the signalmen and mechanical departments should be encouraged.

4.1.6 Physical Ergonomics

Another source of problem that has been reported in the general literature on maintenance errors relates to the physical ergonomics of a system: the design of the physical aspects of the equipment and the physical environment in which the maintenance activities take place. Interviews with the maintenance personnel revealed instances of poor physical ergonomic design.

The mechanical department described one case concerning the maintenance of the ASES cab signal system. Performing the 60-day inspection of the cab signal system required an employee to go into the cabinet, remove the door, and kneel down to read data values off of a display and record them by hand. The employee had to stay in this kneeling position and write down values for 15 minutes, leading to physical fatigue and potential for error.

Signalmen working on the ASES system described another instance of poor physical ergonomics. They mentioned that testing a transponder can be time consuming, taking up to 30 minutes to obtain transponder test readings that involve reading and manually recording long strings of characters off of a difficult-to-read display. An alternative is to dismantle the transponder and perform the test back in the shop where the physical test conditions are better, but it can take 20 minutes to dismantle the transponder. Improved physical ergonomics that would include easier-to-read displays, less need to manually record long strings of characters, and easier mechanisms to dismantle the transponder would make the test process faster and more reliable. Multer et al. (1998) provide guidelines that should be considered in designing railroad equipment for maintenance needs.

Concern Raised

Poor physical design of systems can contribute to fatigue, injury, and maintenance errors.

Implications

The physical ergonomics of the system should be considered as part of the development and evaluation of new PTC systems. This includes consideration of the physical ergonomics associated with equipment testing and maintenance.

4.2 New Sources of Workload

A byproduct of the introduction of new technologies, such as PTC systems, is the potential to introduce new sources of workload for maintenance and operation personnel. Some sources of workload relate to new tasks required to operate the system, for example, entering temporary speed restrictions and work zones into the system. Other sources relate to new tasks associated with inspecting, troubleshooting, and fixing the PTC systems. In the case of both ASES and ITCS, the maintenance personnel reported that they experienced problems in system reliability that required significant maintenance personnel time to track down and correct. Unreliable systems can divert maintenance attention and resources from other safety areas.

Concern Raised

New systems can introduce new sources of workload that can divert attention and resources. This can result in increased error or sources of risk in other safety areas.

Implications

Safety analyses should identify additional sources of workload associated with the operation and maintenance of the new PTC system. The potential for increased error or risk in other safety areas should be addressed.

4.3 New Technology Issues

The new PTC systems incorporate digital technologies that differ from more traditional relay logic systems. This imposes new human performance requirements (e.g., new knowledge and skills), as well as introducing new opportunities for improved performance (e.g., better diagnostics). This section explores some of the human performance issues that relate to the introduction of digital technologies.

4.3.1 New Training Requirements

The PTC systems use advanced digital technologies that require new knowledge and skill to maintain. In addition to training on the specific system (e.g., ITCS), the maintenance personnel needed more general knowledge of electronic systems and how to troubleshoot them. The signalmen working on ITCS provided one successful model. They requested and received an FRA grant to develop a general electronics maintenance course that was offered at a local community college. The signalmen felt that the general knowledge they gained from this course enabled them to understand how ITCS worked and troubleshoot it more effectively. This training experience was so successful that it prompted one of them to go back and get a degree in electronics at a community college.

Concern Raised

Test and maintenance of PTC systems require general knowledge of electronics that maintenance personnel who have worked on traditional relay logic systems may not possess.

Implications

In addition to system-specific training, it may be necessary to insure that the maintenance personnel have the necessary general electronics background knowledge needed to test and maintain new digital-based systems. This can be achieved through personnel selection or training.

4.3.2 Self-Diagnostics

In the age of microelectronics, software has the capability to self-diagnose. Systems should provide easy-to-understand explanations of the malfunction and easy-to-follow procedures for how to fix it. This behavior can facilitate testing and maintenance of systems, reducing the potential for error.

Maintenance personnel working on ASES and ITCS suggested that the systems did not include adequate self-diagnostics. The maintenance personnel indicated that the error codes that were generated were cryptic and required reference to a manual to decode. In some cases, the manual did not include the error codes.

Concern Raised

Cryptic error codes and incomplete documentation can make it difficult to diagnose and repair system malfunctions. This can lead to delays in getting a system back online and safety-related errors.

Implications

Future PTC systems should include better self-diagnostics that provide easy to understand explanations of the malfunction and easy to follow procedures for correcting the problem.

4.3.3 Software Version Control

Another issue that arises with the introduction of digital technology is the need for software version control. Over the life of a system, new software versions will be released to correct problems identified in prior versions and/or introduce improvements. A process must be in place to insure that PTC systems have the latest version of software installed. Failure to put in place a process for software version control can result in a wrong version being installed, possibly leading to problems in system reliability.

While the maintenance personnel did not identify any cases where an incorrect software version led to reliability problems, one of the maintenance personnel did mention a case where a vendor sent a system that had been repaired back to the maintenance department with the wrong software version installed.

The maintenance personnel also mentioned that locomotives differed in the version of the software installed. Since upgrades were being made to system software on a regular basis, multiple versions of the software installed on different locomotives occurred. The existence of multiple versions of software in the field at the same time can complicate system troubleshooting and maintenance. It can also create the possibility that an older version of software that is less reliable or that has unanticipated negative interaction with newer systems will be inadvertently installed leading to problems in system reliability.

Concern Raised

Failure to put in place a process for software version control can result in multiple versions of software in the field at the same time, complicating system troubleshooting and maintenance. Inadequate software version control can also result in the wrong version being installed, impacting system reliability.

Implications

A process must be put in place to insure software version control and testing.

4.4 New Sources of Risk Exposure

Another issue to be considered in assessing the impact of a new technology on risk is whether any added exposure to risk associated with operating and maintaining the equipment exists.

One area of risk exposure that emerged from the interviews was the time signalmen spent on the tracks testing wayside equipment. Unreliable equipment requires signalmen to spend more time on the track troubleshooting the equipment. The increased time spent working on the tracks increases their exposure to risk. Both ITCS and ASES signalmen reported problems in reliability of the wayside equipment. ASES signalmen indicated that transponders tend to be unreliable. A problem can also occur with the reliability of the test equipment used to test the transponders. If the battery on the test equipment is low, then the readings off of the transponder may become unreliable. The signalmen reported that they are currently responding to a lot of false alarms. False alarms are cases where locomotive engineers report a problem, but when signalmen go out to test the transponders, they do not find a problem. Cases occur where they replace the transponder, but the locomotive engineers continue to experience the problem. The more time signalmen need to work on the track to deal with unreliable equipment and false alarms the more exposure to risk they have.

Concern Raised

New technologies can result in added exposure to risk. In particular, unreliable equipment that requires signalmen to spend more time on the track troubleshooting wayside equipment can increase their exposure to risk.

Implications

Safety analyses should explicitly consider any added exposure to risk that result from operating or maintaining the systems. In particular, safety analyses should explicitly address issues relating to the reliability of the equipment and impact on risk to the maintenance personnel responsible for testing and fixing the equipment.

5. System Operation-Related Safety Concerns

PTC systems have the potential to impact the operation of railroad systems in several ways. First, trains run on networks, such that delays or other operational problems on one train can spread to delay or create congestion on other trains in the system. The more congested the system, the greater the potential for coupling between delays of the trains. PTC itself may not necessarily create tighter coupling but be an additional source of delays whose effects then spread across the system.

Second, operation of trains that have PTC systems occurs generally in areas where other traffic control systems are also used, such as automatic block systems or direct traffic control systems. Train crews must comply with the more normally used control systems, and the PTC system enforces them (although exceptions exist where PTC is the only control system). The integration of the different systems must be considered such that no conflicts occur, such as the PTC system providing one set of orders to the engineer and another control system providing different orders. An example of this is with the Northeast Corridor (NEC) Advanced Civil Speed Enforcement System (ACSES) PTC system, where cab signaling and PTC systems can display different speed limits at the same time.

Third, as more railroads add PTC capabilities, interoperability becomes important, particularly as locomotives travel on multiple PTC-equipped territories using different technologies. However, interoperation is not yet a design feature of the current PTC systems.

5.1 Impact on Operations

PTC systems can impact the overall safety and productivity of a railroad since the delays or stoppages by one train in the system can spread to create blockages for other trains, and these can have impacts beyond the simple delays to a single train. This is particularly true for high-density operations, such as the NEC and for commuter operations (because of scheduling constraints), but other locations may exist where system delays and interruptions can be significant. For example, if a long heavy coal train were to stall on an upgrade while the traffic density may be low, the inconvenience of having to repeatedly send out helper locomotives could be a source of operational frustration.

While problems like these may not be in themselves safety concerns, they can become sources of pressure for operators to find ways to overcome these problems. Some of these may lead to the system being switched out (and therefore the expected level of protection from its operations being reduced) or other ways of bypassing the enforcement components of the PTC system.

In this review of PTC systems, the authors identified two instances of these kinds of problems, including delays from the use of conservative braking algorithms and delays because of approach signal operations. In addition, the authors identified delays due to the unreliability of the PTC equipment as a source of disruption that may impact other equipment. As the railroads gain experience with PTC operations, other sources are likely to emerge.

5.1.1 Conservative Braking

The authors identified the use of conservative braking algorithms as significantly impacting train system operation in most, if not all, PTC systems now in use. One of the goals of PTC systems is to enforce rules of operation (speed limits, limits of authority, and work zones) in the face of failures by train crews to comply with these rules. In most cases, if the PTC system logic identifies that a rule has been (or is about to be) broken, it enforces a penalty brake to ensure safety. This gives rise to two potential problems.

First, the PTC logic that determines the need for a penalty brake usually compares the actual train speed with a calculated speed (based on a braking curve) to ensure the train will stop at or before a designated point. If the train speed is above the brake-curve speed (or the speed limit), then the penalty brake will be applied and bring the train to a halt. The problem is associated with the selection of the braking curve. Typically, the braking curve for passenger operations is just one curve that is applied regardless of weather conditions (whether or not the rails are wet and slippery or icy) and therefore is usually designed to be conservative—that is, it assumes that adhesion is poor. Additionally, in some systems, only partial effectiveness of the brake system is assumed in the design of the braking curve since the PTC system will be enforcing safety rules. In freight operations, the onboard processor may calculate the braking curve by using the train consist information, which includes a heavy long coal train that must be handled differently from a short intermodal freight train. But again, the braking curves are not adjusted for weather or typically for grade.

The effect of this use of conservative braking curves is that trains must be slowed earlier (sometimes much earlier) by the engineer to avoid a penalty brake, compared with train operations without PTC. For example, in the case of the New Jersey Transit ASES, engineers estimated that to use that system’s conservative braking adds about 4 minutes to the 1-hour commuter trip from Spring Valley to Hoboken on the Pascack Valley line (a 7 percent increase in trip time).

The conservative braking curve forces engineers to operate trains in what they consider to be less skilled ways. Part of an engineer’s responsibility is to know how to control train speeds under a variety of conditions. Because the PTC system is enforcing a one-size-fits-all braking practice, engineers feel that their skills in this area are no longer important. The PTC system limits the locomotive engineer’s flexibility to adapt to conditions outside the scope of the braking algorithm.

Second, the application of a penalty brake will stop the train regardless of location. It may stop on a grade crossing; it may stop on an upgrade; it may stop inside an interlocking. All of these events can create delays, not only to the equipped train but also to other system users from vehicles at grade crossings to holding up following or crossing trains on grades or interlockings. When stopped at a grade crossings or interlockings, the delays should only be temporary. However, stops on an upgrade with a heavy freight train could lead to extensive delays while helper equipment is sent out to restart the train.

Train delays may reinforce the tendency for engineers to pay closer attention to the displays inside the cab rather than outside the cab, with the increased potential for accidents to trespassers, workers, or vehicles on the tracks (see the discussion in Section 3.1.2).

5.1.2 Approach Signal Update

A second source of delays can occur on some PTC systems where only periodic updating of the signal or other information along a train journey occurs. This issue was raised for ASES, though it may exist in other settings that rely on transponders on or near the track to provide information to the train.

Dr. Alan Bing (ICF, Inc.) provided the following description of the delays associated with approach signals on ASES. Figure 6 shows the scenario for explaining train delays associated with approach signals in ASES.

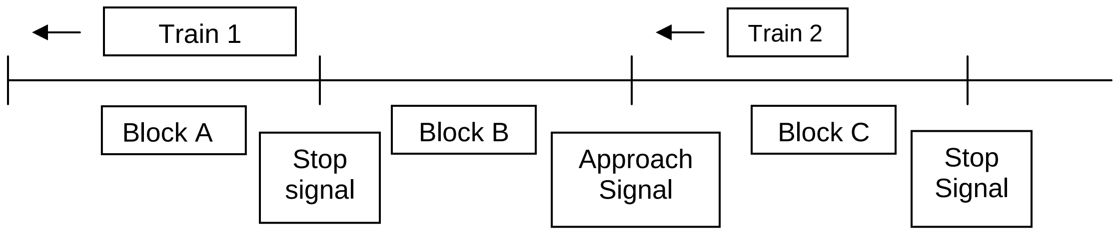


Figure 6. Scenario for Explaining Train Delays Associated with Approach Signals in ASES

Consider a length of track with three signal blocks, A, B, and C, as shown in the diagram above. trains 1 and 2 occupy signal blocks A and C, respectively. Signals and ASES transponders are located at the beginning of each block. Because train 1 is occupying block A, the signal protecting the entry into block A shows a stop indication. This means that the signal controlling entry to block B must show an approach indication, telling the engineer of train 2 that he or she must stop at the beginning of block A after passing through block B. The transponder at the approach signal transmits a message to train 2 with instructions to stop at the entry to block A and giving the distance to that point. The ASES onboard computer will enforce a braking curve to ensure that train 2 stops at or before the entry to block A. With ASES without cab signals, no way exists to change the controlling command in the ASES onboard computer until train 2 moves over another transponder. Therefore, train 2 must be brought to a stop at the entry to block A even if train 1 leaves block A, and the signal at the entry changes from stop to approach, with the adverse effects on the schedule.

New Jersey Transit engineers try to avoid the problem of an enforced stop after passing an approach signal by slowing down in block C before the approach signal and waiting until train 1 has left block A, and the signal at the entry to block B changes from approach to clear. This will result in a slight delay, but this delay is shorter than going into block B and having to stop.

The problem goes away when cab signals or other means of continually updating the PTC system are installed because train 2 then receives continuous data on the status of the entry signal to block A, and the controlling ASES command will be updated as soon that signal changes.

5.1.3 Lost Signals

Many PTC systems rely on continuous communications with various data sources, such as a global positioning system for locating trains and equipment on the track. Delays often result once a signal is lost, particularly when the affected train must now operate at a reduced speed when operating in a congested area. In an extreme case, a passenger train’s speed may be reduced to freight speeds under some failure conditions for ASES.

5.1.4 Spurious Enforcement

Train crews who were interviewed at each PTC system visited reported that, even after the system has been in operation for an extended period of time, there remain relatively frequent spurious enforcements on the systems. These events occurred while the authors visited both the ASES and ACSES and were reported for all the others. Since the system was in a trial or experimental mode, operating rules allow the system to be bypassed so that extended delays did not result. When a spurious enforcement took place, the system applied the penalty brake after which the engineer reset the system. However, once in revenue service, recurrent spurious enforcements will lead to pressure to disable or remove the system, particularly when they occur in congested areas.

Of particular concern would be the potential for unauthorized tampering with the system. FRA may wish to consider the extent to which the systems are tamper-proof, or tampering can be detected readily by the management.

5.2 Integration with Existing Systems

All PTC systems currently in operation are used as an overlay to provide an additional level of enforcement to operations controlled by more traditional train control systems, like absolute block systems (ABS) or direct traffic control (DTC) systems. The IDOT system differs from other PTC systems because it serves as an active (vital) for the higher speeds of operation. The use of PTC systems in conjunction with other systems raises several issues associated with their integration.

5.2.1 Integration of Cab Displays

Some railroads integrate the PTC system with existing in-cab displays, particularly ACSES and ASES. Others, such as the CBTM system, completely separate the PTC-related information from the main train control displays. To varying degrees, the integration of these systems makes their operation more prominent to the engineers. For example, ASES provides an integrated display of the train speed and relevant speed limits, whether mandated by cab signaling or the SES component of ASES. The NEC ACSES has a speed display unit that shows the current train speed and restrictions associated separately with cab signaling and the ACSES PTC system. The engineer must comply with the more restricting of the speed restrictions when the two displays differ (a not unusual condition). Train crews did not identify this separation of displays as a specific source of problems, but it has the potential to create a problem, particularly if an engineer is focused on one display, and the other system enforced train movement at an inappropriate location.

5.2.2 Operational Integration

Operational integration refers to the ways in which train operations across a system can be affected by the addition of a PTC system.

Within an organization, conflicts may exist in the handling of operations with the incorporation of the PTC system. For example, train delays can occur from operation of the PTC system, yet the line management may not appreciate these effects are a systemic property and press crews to maintain the before-PTC schedule. Groups more familiar with the effects of the PTC system may suggest modifications to the train schedules to allow for the effects of the PTC system and reduce the pressure on the crews to work around the system. This can leave train crews in the middle of the conflict as people who must resolve this conflict. This pressure can, for example, exacerbate the crew's complaints about the conservative braking and the frustration from the unexpected penalty brake applications.

Section 5.1.2 discusses a specific problem associated with using a PTC system in conjunction with cab signaling, where unnecessary train delays can occur.

5.2.3 Varied Experience of Staff

As PTC systems become adopted gradually, either during the initial testing period or during the typical progressive rollout of the system in different territories, train crews will vary in their levels of expertise. Some staff will become experts, and others will acquire little or no experience. This can become an operational concern when staff that act as relief (extra board) engineers are assigned to the PTC equipped territory and have only novice levels of experience. The seniority system typically used for work assignments may make it difficult to rotate the assignments to ensure that relief engineers have appropriate levels of experience beyond their mandatory training (which may be as little as a few hours of classroom plus one or two familiarity rides). Experienced engineers identified several of the issues associated with PTC operations (such as constantly monitoring the displays rather than looking outside the cab) as particularly problematic for new and inexperienced engineers.

FRA may wish to consider how the railroads will maintain appropriate levels of expertise as the system becomes used in smaller areas of operation during the rollout phase of deployment and what that level of expertise should be.

5.3 Interoperability Issues

Interoperability issues related to PTC systems can encompass several potential human factors issues. These include the movement of personnel between equipped and non-equipped trains, the movement of equipped trains between covered and non-covered areas, and the use of trains equipped for one PTC system into territories equipped for other PTC systems. This report will address each of these areas. A parallel project for FRA, to examine workload and work mode transitions, has prepared a draft report to discuss these and related issues in greater detail (see Woods and Christoffersen, 2003).

5.3.1 Personnel Movement Between Equipped and Non-Equipped Trains

The roles of the PTC systems in use and under development vary considerably as to their interactions with engineers (see Section 2.1.2). Some, like the CBTM system, are virtually invisible during normal service and only appear via a warning when enforcement is possible (see Figure 3). Other than the complacency concern discussed in Section 3.1.4 above where engineers become complacent in the protection provided by the system, it is unlikely that the movement of personnel between the equipped and non-equipped trains would adversely influence safety.

Other PTC systems provide a more visible role in normal operations, such as the speed indications provided by ASES (see Figure 2) and, in the extreme, the IDOT system's role as a necessary system for high-speed operations (see Figure 4). A conceptual trade-off exists between the role these systems play and their visibility in the locomotive cab. The more visible their role normally is, the more obvious their absence will be when operating non-equipped trains. In two systems currently used (ASES and ACSES) and one under development (IDOT), the equipment provides the normal speed indication and therefore is prominently displayed in the cab. In two systems in use (ITCS and ASES) and the IDOT system under development, the systems provide information about upcoming restrictions or objects (e.g., grade crossings) that can help in operating in poor visibility. The potential exists for engineers to become reliant on this information and therefore perform less well when required to operate a train that is not equipped with that in-cab display. Section 2.1.4 addresses related concerns that deal with loss of skill and complacency issues.

An additional concern can be the limited experience of engineers who only occasionally operate PTC-equipped trains, such as the relief (extra board) engineers who provide backup service for vacation and sick coverage and therefore may only operate equipped trains for a few weeks a year. This level of experience may not be sufficient to maintain a substantive degree of expertise in using the system. Section 2.3 discusses the issue of training requirements for operating PTC-equipped trains. FRA may wish to review how railroads will maintain expertise across all users, including those who only operate equipped trains in an occasional relief capacity.

5.3.2 Train Movements

Several of the PTC systems in use now provide service only for part of the routes that equipped trains serve, most notably ITCS and ASES. Both of these systems indicate when the system is providing coverage. In addition, the railroads will likely deploy new systems by gradually increasing areas of coverage. As such, it will be an aspect of systems operations that equipment will be operating in and out of PTC-covered territory. Equipped trains moving in and out of covered areas provides the potential for inadvertent reliance on the system in an area where coverage is not provided. As discussed in Section 2.2.2 on mode transitions, performance impacts can be minimized through a combination of user interface features that provide unambiguous cues as to whether the PTC system is in operation or not and training that provides practice in running trains in and out of PTC-covered territory. FRA may wish to review the effectiveness of the indications as to whether the system is providing coverage.

5.3.3 Movement Between Different PTC Systems

At present, very limited interoperability built into the current PTC systems exists. Perhaps the only area where this could occur is in the NEC where ASES-equipped trains may operate in the ACSES-covered area. ASES was designed to provide a compatible service with ACSES when operating in NEC. If properly designed and implemented so that the systems are entirely compatible, the shift from ASES- to ACSES-covered territory should be completely seamless from the train crews’ perspective. The PTC system and in-cab displays should continue to operate in exactly the same manner. (As of the visit to New Jersey Transit, trials were about to start testing the compatibility.)

For all other systems, operating a train equipped with PTC system A on territory equipped with system B would be the same as operating on non-equipped territory. No current design goal for PTC equipment to be interoperable exists, and in general the technologies are sufficiently different that accidental cross-coverage is unlikely. However, for any particular system, FRA may wish to check that no other PTC systems are in use or known to be in development where cross-coverage may occur.

In addition to compatibility of the PTC hardware, compatibility of the operating rules and operating conventions across the territories over which the PTC equipped trains will operate must be considered. Differences in operating rules across territories may create opportunities for confusion and error as trains transition from one territory into another. Section 2.2.4 discusses the possibility of interaction between PTC operation and existing operating rules. Differences in operating rules across territories, especially rules relating to PTC operations must be carefully examined. Potential differences in operating rules or operating conventions across territories should be identified and reconciled to avoid potential for confusion or error.

6. Systems Development and Implementation Process

An earlier report specifically associated with the CBTM PTC system addressed issues associated with the development and implementation of a new PTC system (Wreathall et al., 1993). However, the lessons are generally considered to apply to all PTC systems. The sections below summarize the points.

This section provides guidance to FRA on topics it may wish to review for evidence that the design processes used for the PTC systems submitted for approval have included appropriate use of these techniques.

6.1 User Involvement in the Design Process

It is essential in any human-factors development program that users be involved in the design process early and continue to be involved in evaluating and improving the design as it progresses (Nielsen, 1994). Interviews with users of all the systems currently in use shows that everyone with operating experience knows that, with their input very early on, the designs would be more effective, development and deployment would take less time, and acceptance by the users would be better. Yet in each case, only limited involvement by user groups (typically by one or two former engineers) has been made.

Without such an involvement, often users have to adapt to weaknesses in the design, with a negative impact on the overall reliability and an increase in the user work-related stresses when using the system. Simple examples seen in some of the PTC systems reviewed include displays that cannot be easily read from the locomotive control stand, audible warnings that cannot be heard during normal train operations, and incomprehensible error codes found in software and hardware. These design weaknesses could result in increased frequencies of apparently random penalty brake applications and increased distrust of the reliability of the system. In turn, this may create the potential for the system to be disabled.

6.2 Person-in-the-Loop Testing

Person-in-the-loop testing is the process by which developers continue to include representatives of user communities in the system tests as the design progresses, rather than simply performing hardware and software tests in an isolated manner. The idea behind testing is that there should be no user-related surprises when the system goes into operation. Tests that explicitly evaluate the ability of train crews to understand and use the in-cab displays being designed and to operate a train with the PTC control algorithms under development should be conducted throughout the PTC development process to provide rapid feedback to inform the design process. In practice, the railroad may implement person-in-the-loop testing. However, this testing frequently takes place during the latter phases of the system implementation, as the systems become installed in locomotives. Making changes at this stage is more expensive, more likely to delay the rollout of the system, and less likely to remove (rather than moderate) user problems. Performing person-in-the-loop testing early in the design process makes easier to adjust the design before irreversible or costly decisions have been made.

The most frequently cited example for PTC systems is the use of a conservative braking algorithm, discussed in Sections 3.1.1 and 5.1.1. While such an operational issue may not be resolved by simple solutions, its existence can be anticipated in the design trials, and various countermeasures can be developed and tested, such as adjustments to the braking profiles or changes to the in-cab displays. Changes that must be made after the design is complete and in operation often represent significant compromises and are only partially effective. These changes may be less reliable compared with a system that has continued to incorporate feedback from users through the design process.

6.3 Gradual Implementation Process

Even if the system design evolves using feedback from person-in-the-loop testing with user groups (discussed above), surprises can still occur as the system becomes deployed in operational settings. Examples include the following:

- Finding areas where signal strength to the PTC system is suddenly weak (most PTC system users described this experience)
- Operational settings where equipment difficulties exist (such as the approach signal problem)
- Maintaining a minimum train speed in particular locations to prevent power phase through pantograph and catenary equipment
- Locations where frequent changes in speed limits occur (and engineers become preoccupied with PTC displays) are also often areas where there are frequently trespassers (e.g., urban locations)
- Maintenance staff or equipment may be needed to overcome initial weaknesses in the design

To avoid these and other new problems causing loss of credibility of the PTC system and pressure to remove or isolate it, the deployment of the system should be done gradually and preferably in locations where the consequences can be isolated from the entire operating system. Solutions can then be developed before the PTC system is deployed more widely.

FRA may wish to review the expected deployment process to ensure that the initial locations will allow the learning to proceed without pressure to remove or disable the PTC system, with the associated loss of safety improvement.

7. Implications for Review of New PSPs

NTSB proposed PTC systems as a way to reduce the negative impact of human error and improve safety. The actual implementation of PTC systems must provide productivity benefits, as well as safety improvements, to be considered a success. The railroad industry has begun experimenting with PTC in different forms to evaluate how to make the best use of this technology. The systems vary from overlay systems that provide an additional level of protection on top of the existing train control method (e.g., CBTM) to significantly more complex systems that replace the current method of train control (e.g., NAJPTC). While each system addresses one or more of the core safety functions of a PTC system (to prevent train collisions, prevent speed violations, and protect roadway workers), how they implement the system has human performance implications. A question to answer in the preparation of a PSP is: what human performance problem are you addressing? PTC provides a new barrier to preventing unsafe events. What unsafe events related to human performance does the system address? The PSP should describe the aspects of human performance that the PTC system should prevent. This report has identified many of those human performance problems; a search for even more could be valuable.

PTC systems will add complexity to current railroad operations. Railroad employees will adapt to these changes in ways that were unanticipated by the designers. These unanticipated changes will introduce new failure modes that must be considered in evaluating the risk of the new system. Testing could provide firm indications of these effects. Lacking such tests, analysis and probative investigations as the authors have performed can identify many possibilities. Sections 3-6 lay out the human factors concerns identified as a result of reviewing the literature, analyzing potentially PTC preventable accidents, and interviewing employees at several railroads trying out new technologies with elements of PTC. The authors identified the human performance considerations associated with these concerns and how they may affect safety, as well as their implications for risk. Table 3 summarizes the key elements from Sections 3-6 to provide the reader with a checklist to consider when preparing or evaluating a PSP.

Because these suggestions are based on a limited review of serious accidents and discussions with experienced railroad personnel, these findings should not be viewed as a complete review of all possible human performance issues that may arise in the use of PTC systems. The findings could be improved by a more thorough review of accidents[9] and by convening an expert group to review and challenge the findings.

Each PSP risk analysis group could also convene an expert group to focus on the following activities as part of their search risk-relevant issues resulting from deployment of their new PTC system.

- Demonstrate reduction of the most serious accidents.
    - Because most of the fatal accidents involve unsafe human acts (primarily slips, lapses, and circumventions), demonstrate that the new PTC system reduces the likelihood or severity or both of such events.

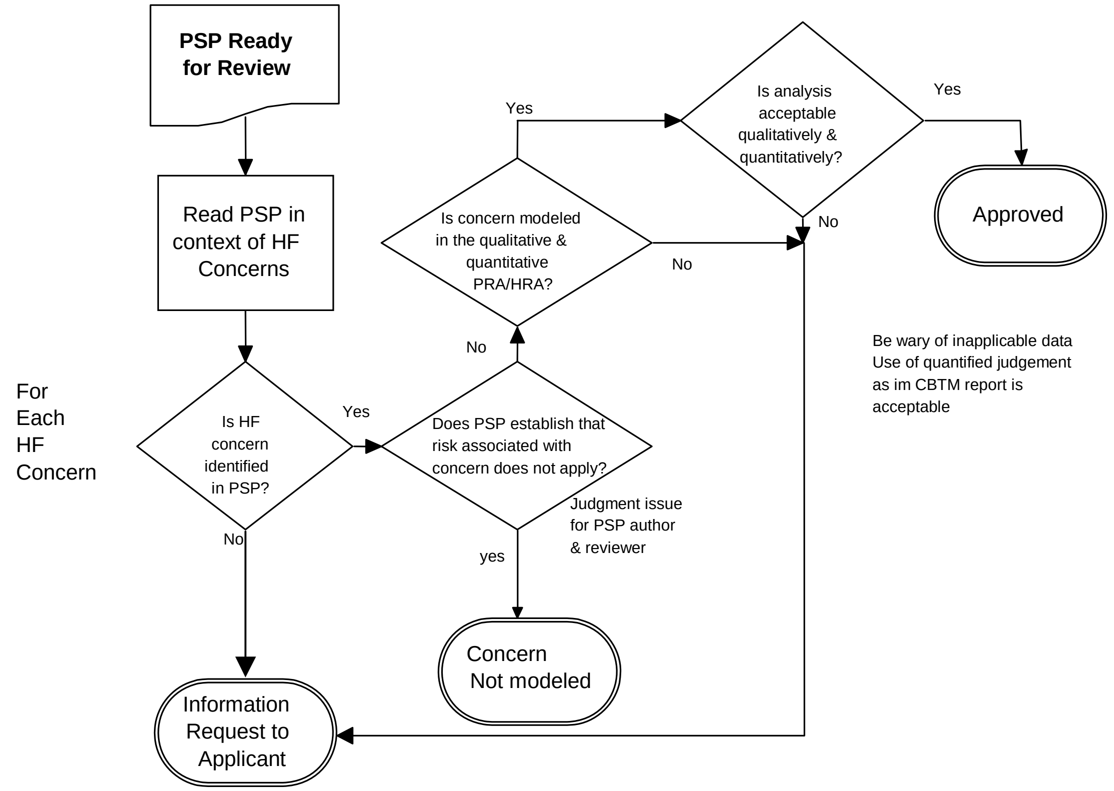
---

[9] A study extending the review described in Section 2.2.1 and documented in Appendix E to cover all events in FRA accident investigation files is recommended.

    - Demonstrate that the new PTC system reduces the likelihood or severity or both of events conducted under difficult operating conditions.
    - Perform a systematic search for possible situations that could follow from deployment and use of the new system, situations that could involve the human performance concerns outlined in Table 3.
- Provide a quantitative analysis, including uncertainty, of these two key aspects of new PTC operation to compare the risk with and without the PTC system. Develop and apply stylized track segments and crew characteristics to mock up the rail system under consideration. Justify that that these stylized segments can represent your rail system.

The summary of human factors concerns provided in Table 3 is more than a summary of the findings of this investigation. It is intended as a guide to railroad personnel preparing PSPs and FRA personnel who must review and evaluate them. Details of its best use will evolve with practice. At this time, the table should be used as a learning tool to be studied by analysts and reviewers before they begin their efforts and as a checklist during the actual analysis/review process. Has each concern been considered? Is it applicable to the current system? Have its implications been followed (analyzed) and addressed to an acceptable extent?

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment



Roadmap for Use of Human Factors Concerns Table

This roadmap shows how to use the Human Factors Concerns Table in the development or review of the PSP risk assessment.

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	Engineer-Related Safety Concerns	
The PTC braking profile may impact how train crews operate the train.	If the PTC braking profile is conservative, it may require the locomotive crews to learn new train handling and braking techniques to avoid unnecessary PTC penalty brake application while still operating efficiently. Of particular concern is the performance of individuals who are early in the learning curve to use the PTC system. This includes new hires, experienced engineers who are new to the PTC system, and people on the extra-board who may not regularly use the PTC system. Potential impacts include inadvertent activation of a penalty brake that creates risk (e.g., train stops at inappropriate location or train derails)	PRA/HRA qualitative analysis must evaluate possible impacts of conservative braking algorithms on crew performance.[*]

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	and possibility that crews will disable or circumvent the PTC system. Concerns with conservative braking algorithms are especially high in the case of freight operations where train braking decisions involve more dynamically changing variables than passenger train operations. Human performance problems associated with conservative braking curves can be reduced through a combination of comprehensive training, improvements to PTC braking algorithms and in-cab displays, and an organizational climate that foster a safety culture and avoid creating goal-conflict conditions.	
In-cab displays may require close monitoring, reducing the train crew's ability to monitor out the window.	PTC system may shift the train crews' attention from events occurring outside the locomotive cab to in-cab displays. This shift in attention may cause train crews to miss key events out the window, creating a new source of safety risk. Problems can be reduced through a combination of more comprehensive training and improved in-cab displays. Person-in-the-loop evaluations of the final PTC design can be conducted to establish whether out-the-window performance is substantially impaired by the need to closely monitor the in-cab display.	Any safety analysis must address allocating more attention on in-cab displays at the expense of events outside the window.
PTC systems may generate uninformative alerts that become a source of workload and distraction.	If alerts are poorly designed so that they produce a lot of uninformative alerts that need to be acknowledged, the following may occur: • They may act as a source of distraction causing locomotive engineers to miss important events occurring out the window • They may be responded to automatically (pressing the acknowledge button), eliminating	Poorly designed alarms can create a source of workload and distraction and should be addressed as part of a safety analysis.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	their informative value • They may be cut out, defeating their safety function Problems can be avoided through a careful user interface design and review process that minimizes uninformative or low importance nuisance alerts.	
Initiation/interaction with PTC may create a source of workload and distraction.	PTC systems generally require manually entered inputs at the start of a trip and after a shutdown of the system during train operations. The added workload associated with interacting with the PTC can introduce new sources of risk. Sources of risk include: distraction leading to important signals being missed, data entry errors, and a possibility that the PTC system will be cut out or not cut back in, eliminating its safety benefits.	A safety analysis must address the added workload associated with initializing and restarting the PTC system should it stop in the middle of a trip.
Potential for complacency/over-reliance.	Locomotive engineers may come to rely on the PTC system to alert them of upcoming speed and authority limits and to automatically stop the train should they fail to do so themselves. As a consequence, should the system fail, the locomotive engineers may not perform as well without it as they would have had the system never been installed.	A safety analysis must address locomotive performance under conditions where the PTC system is not functioning. This includes consideration of the potential for complacency effects and what actions have been taken to minimize the potential for complacency effects.
Potential for loss of engineer's control.	PTC systems that generate penalty brakes without the possibility of a manual over-ride by the locomotive engineer are taking the locus of control away from the person on the scene, who may be aware of important safety factors that are not taken into account by the PTC braking algorithms. In some situations, the automated braking curve generated by the PTC system may be inappropriate. In other cases, it may initiate a penalty brake	Any safety analysis must address the potential for automation-induced accidents. This includes an analysis of conditions where the braking curve generated by the PTC system may be inappropriate or where inappropriate initiation of a penalty brake may create a safety hazard. The safety analysis should also address under what conditions the locomotive engineer may over-ride the PTC systems.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	unnecessarily. If these system actions arise at the wrong time or place, it can have negative safety consequences. The safety concerns are particularly great in the case of freight operations where braking decisions are complex involving multiple, dynamically changing variables. PTC systems that utilize one-size-fits-all conservative braking profiles may result in reduced efficiency of freight operations and could in some cases impact safety.	
Reliance on manually entered data.	The reliability of PTC systems that depend on manually entered data may be affected by the possibility of human error in data entry.	Safety analyses should specifically address the impact of human error in data entry on PTC system reliability.
Impact of mode transitions.	Locomotive engineers may have difficulty transitioning between train operation with PTC and train operation without PTC, resulting in decreases in reliability at points of transition. Mode transitions that need to be considered include the following: • PTC-equipped trains transitioning into and out of PTC territory • PTC-equipped trains running on PTC territory without PTC activated (e.g., because of a malfunction) • Locomotive engineers who normally operate on non-PTC territory operating on PTC territory and vice-versa (e.g., locomotive engineers on the extra-board) The concern is that the locomotive engineer may fail to increase vigilance sufficiently to compensate for the lack of PTC protection. As in the case of complacency, the concern is that the locomotive engineers will not perform as well when the PTC is	Safety analyses should explicitly address the types of mode transitions that are likely to arise in operation and the steps taken to reduce the possibility of problems at mode transitions.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	not activated as they would have had the system never been installed because they have come to rely on it. Performance impacts of mode transitions can be minimized through a combination of user interface features that provide unambiguous cues as to whether the PTC system is active or not and training that provides practice in running trains with and without PTC. This includes comprehensive initial training, as well as periodic refresher training.	
Impact on train crew teamwork.	If a system is poorly designed or poorly located in the cab, it can disrupt teamwork and interfere with the ability of train crew members to catch and recover from errors. If crewmembers other than the locomotive engineer are expected to read and respond to PTC messages (e.g., to serve as a redundancy check), then the display must be placed in a location where they can easily see it.	Safety analyses should specifically address who is expected to be the primary user of the PTC system and what role, if any, other crewmembers are expected to play, with respect to monitoring and acting upon PTC displayed information.
Interaction with operating rules.	If rulebooks are not updated to accommodate the new capabilities of PTC systems and to provide practical procedures for handling the different contingencies that can arise, then inconsistencies may emerge between the procedures specified in the rulebook and actual operation. This can create opportunity for unsafe action because of misunderstanding rules and policies. The potential for problems is particularly great in situations where rulebook specifications and/or conventions of practice differ across the different territories the PTC-equipped train passes.	Safety analyses should address interaction of PTC with operating rules. This includes specification of new operating rules that have been developed to cover operation of trains equipped with PTC under different contingencies (e.g., initialization of the PTC system, when the PTC system malfunctions, running a PTC-equipped train when the PTC system is disabled). Ideally, the rules should have been developed with input from operations staff (e.g., locomotive engineers), and the comprehensibility and workability of these rules should be established through field tests.
New training requirements.	If a locomotive engineer does not have sufficient experience in operating a PTC-equipped train, there may be increased risk because of inappropriate train handling or	Safety analyses should address the kind of training to be provided to train crews who will be operating PTC-equipped trains. This includes

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	braking. There may also be increased risk because of added workload and distraction. Increased risk may also occur because of inability to recognize unusual circumstances and know what to do (e.g., if a PTC error code appears). Another concern relates to train operations in cases where the PTC-system is unavailable (e.g., because of a malfunction). The concern is that, if train crews are inexperienced in operating a train without PTC, their performance may degrade leading to increased risk. Training should include sufficient hands-on experience in running a PTC-equipped train to develop the necessary train handling and braking skills required to operate a PTC-equipped train to be able to run efficiently while staying within the PTC braking curve. Training should also provide sufficient exposure to unusual conditions to insure that the locomotive engineer will be able to recognize and know what to do should they arise. Training should also cover operation without the PTC system to insure that the train crews are able to run trains safely in conditions where the PTC system is non-operational. This may require periodic refresher training in running a train with the PTC system inactive.	the following: • New engineers • Experienced engineers who are learning to run a PTC-equipped train. • Transferring-in and occasional staff, such as crews on the extra-list who may only occasionally operate a PTC-equipped train.
	Maintenance-Related Concerns	
Availability and quality of training.	The general shift to digital signal equipment from traditional relay-based equipment means that maintenance personnel will need to train in the fundamentals of digital technology and its maintenance. Inadequate training of maintenance personnel can contribute to maintenance errors that reduce	Safety analyses should specifically address the training provided to maintenance personnel. This includes initial training when new systems are first installed, as well as ongoing training of new maintenance personnel as they come in.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	system safety and reliability.	
Availability and quality of maintenance manuals.	Maintenance manuals that are incomplete, difficult to understand, or use can contribute to maintenance errors. Manuals must be specifically written to support installation, testing, and maintenance of PTC equipment. The manuals should be comprehensive. The manuals must cover all error codes that can appear and provide specific procedures for troubleshooting and correcting PTC system malfunctions. They should also provide detailed procedures for differentiating problems that result from in-cab equipment from problems that are due to wayside equipment. User evaluations should be performed to establish that the manuals are complete, easy to understand, and follow by the maintainers that are supposed to use them. These tests should be conducted using actual system maintainers as test participants, and their feedback should be used to correct any problems identified. Processes should be put in place for upgrading maintenance manuals when changes to the PTC system are made.	Safety analyses should specifically address the development, evaluation, and upgrade of maintenance manuals.
Availability and quality of technical support from the system vendor.	Inadequate technical support by vendors, who are difficult to contact or lack relevant knowledge, can contribute to maintenance errors. Risk because of maintenance errors can be reduced by providing effective training, developing good maintenance manuals, and making available knowledgeable support personnel to aid in troubleshooting complex problems.	Safety analyses must address the quality of the technical support provided by vendors.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
Availability and reliability of testing equipment.	Lack of appropriate test and maintenance equipment can impact the ability to detect and correct system malfunctions in a timely manner, which can impact system reliability. Problems in test equipment reliability can also impact system reliability.	Safety analyses should address the availability and reliability of testing equipment.
Communication among crafts and across shifts.	Problems in communication within and across crafts (e.g., between locomotive engineers, cab mechanics, and signal maintainers) can result in delays in tracking down and correcting system malfunctions. These problems can also contribute to maintenance errors that reduce system safety and reliability.	Safety analyses should address the quality of communication among crafts and across shifts.
Physical ergonomics.	Poor physical design of systems can contribute to fatigue, injury, and maintenance errors. The physical ergonomics of the system should be considered as part of the development and evaluation of new PTC systems and should be addressed by safety analyses. This includes consideration of the physical ergonomics associated with equipment testing and maintenance.	Safety analyses should address the physical ergonomics associated with equipment testing and maintenance.
New sources of workload for roadway workers and maintenance personnel.	New systems can introduce new sources of workload that can divert attention and resources. This can result in increased error or sources of risk in other safety areas.	Safety analyses should identify additional sources of workload associated with the operation and maintenance of the new PTC system. The potential for increased error or risk in other safety areas should be addressed.
New training requirements.	Test and maintenance of PTC systems require general knowledge of electronics that maintenance personnel who have worked on traditional relay logic systems may not possess. Lack of knowledge can result in maintenance errors that increase risk. In addition to system-specific training, it may be necessary to insure	Safety analyses should address the qualification and training of maintenance personnel as they relate to system maintenance and test requirements.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	that the maintenance personnel have the necessary general electronics background knowledge needed to test and maintain new digital-based systems. This can be achieved through personnel selection or training.	
Need for software version control.	Over the life of a system, new software versions will be released to correct problems identified in earlier versions and/or introduce improvements. Failure to put a process in place for software version control can result in multiple versions of software in the field, at the same time complicating system troubleshooting and maintenance. Inadequate software version control can also result in the wrong version being installed, impacting system reliability.	Safety analyses should address system reliability failures due to installation of inappropriate or incompatible software.
New sources of risk exposure to equipment maintenance personnel.	Unreliable equipment that requires signalmen to spend more time on the track troubleshooting wayside equipment can increase their exposure to risk.	Safety analyses should explicitly consider any added exposure to risk that result from operating or maintaining the systems. In particular, safety analyses should explicitly address issues relating to the reliability of the equipment and impact on risk to the maintenance personnel responsible for testing and fixing the equipment.
System Operation-Related Safety Concerns		
Impact on operations.	Section 4.1 has many examples of actual issues that have affected operations (conservative braking, approach signal update, lost signals, and spurious enforcement). All have the potential to adversely affect operations (traffic and costs). These adverse impacts on operations have the potential to increase the pressure, both on the crews and the railroad management to cut out or otherwise bypass the system, thereby removing the levels of protection provided by the PTC system. FRA must consider the effectiveness of the management processes used by the railroads to	The PRA must consider the potential effects of the PTC system being taken out of service (either because of operational problems or simply from equipment failures). The possible effects of over-reliance may not be possible to model directly (because of a lack of suitable explicit models in HRA), but sensitivity studies can indicate the potential effects of decreased vigilance by the train crews on the overall level of safety.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	ensure that PTC equipment is not removed from operation except for during pre-planned and approved conditions. For example, by what means would management detect tampering with the PTC enforcement functions? Since workers adapt to changes in the levels of protection provided by equipment in subtle (and often unanticipated) ways, railroads must anticipate whether the net effects of removing the PTC system are worse than simply restoring the safety to pre-PTC levels and are lowering the overall level because the system on which they have come to rely is no longer available. Some of these effects are referred to as over-reliance. The PSP should discuss how the appropriate level of safety will be maintained when the system is out of service. These discussions should be beyond statements like “the system will revert to operating practices used during the pre-PTC days.”	
Integration with existing systems.	Section 4.2 identifies several issues (integration of cab displays, operational integration, and varied experience of staff). These are not especially troublesome for crews experienced with these systems but could be difficult for new engineers or those who only use these systems occasionally. FRA’s review of the PSP should identify how the railroad will identify and maintain appropriate levels of competence of staff who are new or occasional users of the PTC system. Aspects of individual systems where specific design features may raise particular challenges may exist (such as the conflicting speed limits in the ACSES display); these may need to be considered on a case-by-case	Safety analyses should address possible impacts of integrating PTC systems with existing systems. This includes examination of potential impact on inexperienced crews under difficult conditions. Options include performing sensitivity studies to identify the possible changes in risk between experienced and inexperienced crews.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
	basis. The PSP must identify any particular design aspects that are unique challenges.	
Interoperability issues.	The movement of experienced crews from equipped to unequipped trains can have the potential for the crews to forget that the PTC system is no longer available to provide protection. This corresponds to the over-reliance issue raised above. In addition, the need for maintaining levels of experience for inexperienced crews who are occasionally called on to operate PTC-equipped trains must be discussed (see above). A third interoperability concern is whether the PTC system clearly and unambiguously indicates whether the system is in operation in the area or whether the train is outside the PTC coverage area. Again the potential exists for crews to over-rely on the PTC system in areas where no coverage exists. FRA should review the extent that coverage is active and is clearly and unambiguously indicated. The final concern is that PTC-equipped trains that travel into other territories may need to comply with different operating rules. FRA should be assured that differences in rules relating to PTC operations from territory to territory will not lead to confusion or unsafe conditions.	Safety analyses should explicitly identify and address potential interoperability issues.

Table 3. Summary of Human Factors Concerns and Their Implications for Safety Analysis and Risk Assessment

Concern	Influence on Human Performance	Implications for Safety Analysis and Risk Assessment
Concerns about the Development and Implementation Process		
User involvement in the design process, person-in-the-loop testing, and gradual implementation process.	Failure to use these methods can and has led to the design of systems that are difficult to use, provide unnecessary opportunities for user error and lead to tweaking in use that create new opportunities for failure. FRA should evaluate the extent to which the design process has incorporated these design methods to minimize operational problems.	

*Wreathall (2003) described and used a structured elicitation approach that can generate estimates of probability (distributions elucidate the uncertainty) based on all the available information, when directly applicable and complete performance data are not available. Results from simulator experiments can be brought into the elicitation process and can enhance the value of such evaluations. Information needs identified in preliminary PRA/HRA analysis can help focus planned experiments.

Appendix A.
Focus Group Questions for Train Crews

INTRODUCTION

Welcome.

Thanks for taking the time to join in this group discussion on impact of the PTC-SYSTEM-NAME on train operations.

I'm … I work as a contractor for the Volpe National Transportation Systems Center and FRA.

This is … who is working with me on this project for the Volpe National Transportation Systems Center and FRA.

The Volpe National Transportation Systems Center and FRA are participating along with representatives of RAILROAD-NAME and other railroads, as well as representatives of labor on an RSAC working group that is looking at the impact of new train technologies such as PTC-SYSTEM-NAME on train operations and safety. The objective is to learn from the experiences of systems such as PTC-SYSTEM-NAME to provide input for the design, operation, and evaluation of future Positive Train Control Systems.

By safety we mean reducing the potential for accidents leading to deaths and injuries to crews, roadway workers, and the public.

As part of this work, we are conducting focus groups to obtain input from locomotive engineers and conductors to get their input on how PTC-SYSTEM-NAME has affected train operations and safety. We'll also be conducting similar group meetings with signal maintenance personnel and mechanical department maintenance personnel to get their input as well.

Our particular concern is on Human Factors Issues. How PTC-SYSTEM-NAME impacts your ability to do your job and to maintain safety. We are interested in finding out what things about PTC-SYSTEM-NAME make it easier for you and how it improves safety. We are also interested in any problems that you have encountered with PTC-SYSTEM-NAME and any concerns you might have on its impact on safety.

Your opinions and suggestions are very important to us and will help shape the kinds of new technologies that are introduced in the future. Both your National and Local labor representatives and RAILROAD-NAME support this effort and hope that you will give your honest opinions and suggestions.

With your permission, we would like to tape record the session because we don't want to miss any of your comments. Your comments will remain strictly confidential.

While we will be writing a report summarizing what we learned, inputs of individuals will remain anonymous.

Also, if at any point you would like us to turn off the tape recorder or erase something said earlier, we will do so. Is it OK to tape record?

Keep in mind that we're just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

We expect that you will have different points of view. Please feel free to share your point of view even if it differs from what others have said.

If you want to follow up on something that someone has said, you want to agree, or disagree, or give an example, feel free to do that. We are here to ask questions, listen, and make sure that everyone has a chance to share. We're interested in hearing from each of you. So if you're talking a lot, I may ask you to give others a chance. And, if you aren't saying much, I may call on you. We just want to make sure we hear from all of you.

OPENING QUESTION

Tell us who you are, a little about your railroad background, and your experience with PTC-SYSTEM-NAME?

- How long have you been running trains equipped with PTC-SYSTEM-NAME?
- Do you run trains that are equipped with PTC-SYSTEM-NAME exclusively or do you sometimes run trains without PTC-SYSTEM-NAME?

QUESTIONS ABOUT HOW PTC-SYSTEM-NAME AFFECTS THEIR WORK

- Can you tell us what PTC-SYSTEM-NAME does?
- Is it easy to understand and use the PTC-SYSTEM-NAME interface? Any problems you have encountered?
- How about entering information? Is there any information you need to enter at the start of a trip? Is it easy to enter this information?
- Can you say a little about how the PTC-SYSTEM-NAME system changes how you operate the train if at all?
    - o How does operating a train equipped with PTC-SYSTEM-NAME differ from running a train not equipped with it?
        - Did it require any change to the operating rules?
        - Does it change how much you look outside the cab versus inside the cab? Does it serve as a source of distraction?
        - Does it change how much you have to rely on things in your head or things on paper (like personal notes or temporary speed restriction lists)?
        - Does it change communication between the locomotive engineer and the conductor?

        - Does it change your communication with dispatchers? Roadway workers? Others?
        - Does it affect your ability to think ahead? Anticipate what is coming next (e.g., next signal, next grade-crossing, next work zone)?
        - Does it affect how you brake? How early you brake?
        - Do you think there is a potential problem with complacency? Where a locomotive engineer might get to rely on the PTC-SYSTEM-NAME system and stop being as alert to potential problems as he or she might be?
        - Any other changes you can think of?
    - How can you tell that the PTC-SYSTEM-NAME system is activated and protecting you? Is it easy to tell when it is activated? Is it easy to tell when it is off? When it is malfunctioning?
    - PTC-SYSTEM-NAME is designed to “seamlessly operate over various territories: non-equipped, CAB signal/ATC only; SES-only; combined PTC-SYSTEM-NAME, AMTRAK ACSES, ‘unknown’, installation area.”
        - Have you experienced transition between these modes/territories?
        - Do you think the display makes it easy to tell that you are transitioning between these modes/territories?
        - Do you envision any problems in operating in any of these modes/territories? Perhaps particularly on the ACSES system?
        - Do you envision any problems in transitioning between these modes/territories (e.g., getting confused which mode/territory you are in; having difficulty transitioning from one operating style to another)?

QUESTIONS ABOUT LEARNING TO OPERATE PTC-SYSTEM-NAME

- What kind of training did you get on PTC-SYSTEM-NAME? Did you feel it was sufficient? Are there ways it could be improved?
- Was there a steep learning curve for you?
- Do you think that operating a train with PTC-SYSTEM-NAME is easier to learn for an old-timer with years of experience running a train or someone who is just learning to operate a train?

- What kind of challenges would a novice engineer experience who was first trained on an PTC-SYSTEM-NAME territory and then moved to a non-PTC-SYSTEM-NAME territory?

- Did you get training on the ways that PTC-SYSTEM-NAME might fail, and what it would mean for how you would need to operate the train?

QUESTIONS ABOUT IMPACT ON SAFETY

PTC-SYSTEM-NAME is intended to improve safety by displaying and enforcing:

- Positive stop-signal
- Fixed (civil) speed limits
- Variable (signal) speed limits
- Temporary speed limits
- Anything else?

We are interested in understanding your perspectives on the factors that contribute to errors and accidents in each of these cases and to what extent you feel that PTC-SYSTEM-NAME is effective in catching errors and preventing accidents.

- Let's start with speed limits (signal speeds, fixed speed limits, and temporary speed limits). What do you think are the main factors that might cause a train to exceed its speed limits (in the non-PTC-SYSTEM-NAME case)?
    - How about miscommunication? Is that a factor? Can you think of any examples where that has occurred?
    - How about organizational pressure to stay on time or make up time? Is that a factor?
    - How about fatigue?
    - How about level of experience? Are there some kinds of errors that a less experienced person might make that a more experienced person is less likely to make and vice versa?
    - Missing a signal? What might cause that?
    - Missing a temporary speed restriction? What might cause that?
    - Of the factors we discussed, which do you think are the most important factors?

  - Do you think that PTC-SYSTEM-NAME is effective in catching speed limit violations?

Following sections may not apply but may touch upon anyway in case it may apply.

- Let’s turn to work area restrictions. What do you think are the main factors that might cause a train to enter a work zone without proper authority (in the non-PTC-SYSTEM-NAME case)?
  - How about communication errors with the dispatcher?
  - How about communication errors with the roadway workers?
  - Of the factors we discussed, which do you think are the most important factors?
  - Do you think that PTC-SYSTEM-NAME is effective in catching unauthorized entry into a work zone?

- Let’s continue with interaction with roadway workers for a minute.
  - How do you keep track of roadway workers in the territories you are traveling through?
  - What things can go wrong, what could cause a roadway worker to be in a place you didn’t expect? What can you do in those cases?

- Are there any other safety issues that concern you that you think that PTC-SYSTEM-NAME is effective in catching and preventing accidents?

- Are there any other safety issues that concern you that you think that a PTC system should address that PTC-SYSTEM-NAME does not address?

QUESTIONS ABOUT SURPRISES/PROBLEMS/NEW SOURCES OF SAFETY PROBLEMS

We’ve talked about the potential benefits of PTC-SYSTEM-NAME, now let’s turn to problems with PTC-SYSTEM-NAME, if any.

Sometimes, when you introduce a new system, it can have some consequences that weren’t anticipated by the designers of the system. For example, it might increase workload or create new kinds of errors. For example with a digital alarm clock you can set the alarm for 6 p.m. instead of 6 a.m. by mistake; this wouldn’t happen with an analog clock.

So, with respect to PTC-SYSTEM-NAME, are there any new problems that have come up? Any surprising behavior of the system that you don’t understand or are concerned about?

Have you ever experienced PTC-SYSTEM-NAME present faulty information (e.g., say signals were there that were not or vice versa)? For example, have you ever experienced a false proceed with PTC-SYSTEM-NAME in place? (A false proceed occurs when the signal system says it is okay to proceed to the next block, but it is in fact not okay to proceed.)

Have you ever experienced a PTC-SYSTEM-NAME full service brake enforcement? If so, what made it happen?

Have you ever experienced or heard about a case where PTC-SYSTEM-NAME initiated a full service brake when it should not have?

Have you ever experienced a case where PTC-SYSTEM-NAME failed to activate when it should have?

Has PTC-SYSTEM-NAME ever malfunctioned (not operating or not operating well)? If so, was it easy to tell that it was not operating or not operating well?

The performance of PTC-SYSTEM-NAME depends on the data that is fed to it. Have you encountered any problems due to incorrect data entry (either by locomotive engineer, block operator, or database manager)?

Are there any other issues you can think of relating to the introduction of PTC-SYSTEM-NAME? Any concerns you might have?

Do you see any potential issues that might arise when

- Expanding beyond this Pascack valley line?

- Expanding to freight trains?

- Expanding so that PTC-SYSTEM-NAME equipped trains operate on Amtrak ACSES territory?

- New engineers begin operations with the protection of PTC-SYSTEM-NAME or ACSES rather than traditional systems (e.g., perhaps they would develop a reliance or dependence on these systems that could affect their performance)?

INPUT TO DESIGN

Do you know whether any locomotive engineers had input or involvement during the design of PTC-SYSTEM-NAME?

If you had 5 minutes to talk with key designers, what would you say?

- Are there any minor modifications to PTC-SYSTEM-NAME that you would suggest to increase its impact?
- Any major redesign?

ENDING

All things considered, do you think that PTC-SYSTEM-NAME is a good system?

Do you think it makes train operations safer?

Are there any things you would suggest trying to do better in the next PTC system based on the lessons learned from PTC-SYSTEM-NAME?

Is there anything that we should have asked about but did not? Anything that you came wanting to say that you did not get a chance to say?

Appendix B.
Focus Group Questions for Signalmen

INTRODUCTION

Welcome.

Thanks for taking the time to join in this group discussion on impact of the PTC-SYSTEM-NAME on train operations.

I'm … I work as a contractor for the Volpe National Transportation Systems Center and FRA.

This is … who is working with me on this project for the Volpe National Transportation Systems Center and FRA.

The Volpe National Transportation Systems Center and FRA are participating along with representatives of Amtrak and other railroads, as well as representatives of labor on an RSAC working group that is looking at the impact of new train technologies such as PTC-SYSTEM-NAME on train operations and safety. The objective is to learn from the experiences of systems such as PTC-SYSTEM-NAME to provide input for the design, operation, and evaluation of future Positive Train Control Systems.

By safety we mean reducing the potential for accidents leading to deaths and injuries to crews, roadway workers, and the public.

As part of this work, we are conducting interviews and focus groups to obtain input from locomotive engineers, conductors, signal maintenance personnel, and mechanical department maintenance personnel to understand the impact of PTC-SYSTEM-NAME from their perspective.

Our particular concern is on Human Factors Issues. How PTC-SYSTEM-NAME impacts your ability to do your job and to maintain safety. One topic we are interested in is maintenance issues associated with the introduction of new technologies such as PTC-SYSTEM-NAME. We are interested in how easy new systems such as PTC-SYSTEM-NAME are to maintain, what new maintenance challenges these new technologies pose, and what new training requirements and activities they bring.

We are also interested in your perspective on how PTC-SYSTEM-NAME improves safety. We are interested in any problems that you have encountered with PTC-SYSTEM-NAME and any concerns you might have on its impact on safety.

Your opinions and suggestions are very important to us and will help shape the kinds of new technologies that are introduced in the future. Both your National and Local labor representatives and RAILROAD-NAME support this effort and hope that you will give your honest opinions and suggestions.

With your permission, we would like to tape record the session because we don't want to miss any of your comments. Your comments will remain strictly confidential.

While we will be writing a report summarizing what we learned, inputs of individuals will remain anonymous.

Also, if at any point you would like us to turn off the tape recorder or erase something said earlier, we will do so. Is it OK to tape record?

Keep in mind that we’re just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

We expect that you will have different points of view. Please feel free to share your point of view even if it differs from what others have said.

If you want to follow up on something that someone has said, you want to agree, or disagree, or give an example, feel free to do that. We are here to ask questions, listen, and make sure that everyone has a chance to share. We’re interested in hearing from each of you. So if you’re talking a lot, I may ask you to give others a chance. And, if you aren’t saying much, I may call on you. We just want to make sure we hear from all of you.

OPENING QUESTION

Tell us who you are, and a little about your railroad background.

What territory do you cover? What proportion is PTC-SYSTEM-NAME territory?

MAINTENANCE ACTIVITIES ASSOCIATED WITH PTC-SYSTEM-NAME

Can you tell us some of the major signal maintenance activities associated with PTC-SYSTEM-NAME? Installation activities? Active versus Passive Transponders: are the maintenance activities the same?

What are some of the most common problems that have arisen with PTC-SYSTEM-NAME?

What are some of the most difficult aspects of maintaining PTC-SYSTEM-NAME? Troubleshooting PTC-SYSTEM-NAME problems when things go wrong?

Do you get involved in maintaining PTC-SYSTEM-NAME software? Upgrading software? Is version control an issue?

Were there any issues that arose during the PTC-SYSTEM-NAME installation process?

TRAINING ON PTC-SYSTEM-NAME

Can you tell us what training you received on PTC-SYSTEM-NAME? Do you feel the training was sufficient?

CHALLENGES TO MAINTENANCE

One of the areas we are concerned about are factors that can make maintenance more challenging and contribute to maintenance errors that can impact safety. Experience from other industries such as aviation suggest a number of factors that can contribute to maintenance errors.

I'm going to mention some of the factors that have been identified as challenges to maintenance in other industries and ask if they are an issue for you and particularly if they are an issue with respect to maintenance of PTC-SYSTEM-NAME systems.

- Lack of appropriate tools/equipment: Need to jury-rig equipment
- Problems in the physical environment
- Inadequate documentation
- Unworkable procedures/need for work-arounds
- Need to maintain private brain book
- Time pressure
- Communication problems
    - Within a team
    - During shift turn-over
    - Communication with vendors who supply the equipment and provide hardware and software upgrades
    - Communication with users of the equipment
- Fatigue
- Lack of training/experience
- Organizational problems
    - Inadequate supervision
    - Inadequate policies

ERRORS AND NEAR MISSES

Have there been any recent cases where a maintenance error or near miss occurred? Can you describe the factors that contributed to it?

SECTION ENDING

From the perspective of ease of maintenance and prevention of maintenance errors, if you had 5 minutes to talk with key designers, what would you say?

- Are there any minor modifications to PTC-SYSTEM-NAME that you would suggest to make it easier to maintain and reduce the potential for maintenance errors?
- Any major redesign?

How about recommendations with respect to training, documentation, or policies?

THE ROLE OF PTC-SYSTEM-NAME IN INCREASING WORKER PROTECTION

One of the objectives of the PTC-SYSTEM-NAME system is to provide an additional level of protection to roadway workers by ensuring that a train cannot enter their work limits or exceeds the maximum authorized speed specified in a slow order.

First we'd like to understand what kinds of accidents happen and why when the PTC-SYSTEM-NAME system is not there (in non-PTC-SYSTEM-NAME territory), and then we'd like your input on whether PTC-SYSTEM-NAME helps prevent these types of accidents and how.

Let's start with trains exceeding their maximum authorized speed limits set by a slow order.

In a non-PTC-SYSTEM-NAME territory (or this territory before PTC-SYSTEM-NAME), how are slow orders communicated to train crews?

What indications does a train crew have that they are about to enter a restricted speed zone?

What things might lead to a train to exceed the maximum authorized speed limits set by a slow order?

Have you ever experienced or heard about a case where a train exceeded a slow order speed limit? What factors contributed to it?

How does PTC-SYSTEM-NAME ensure that a train doesn't exceed the maximum authorized speed limit specified by a slow order?

Do you have confidence that the PTC-SYSTEM-NAME will keep trains from exceeding slow order speed limits?

Have you ever experienced or heard of a case where PTC-SYSTEM-NAME failed to prevent a train from exceeding a slow order speed limit?

Do you have any concerns about the reliability or effectiveness of PTC-SYSTEM-NAME?

Are there any other issues you can think of relating to the introduction of PTC-SYSTEM-NAME? Any concerns you might have?

Another role of PTC technology is to prevent trains from entering a work limit without authority.

How are work limits protected?

How does a train get authority to enter a work limit?

What indications does a train crew have that they are approaching a work zone?

What things might lead to a train to enter a work limit without authority?
Have you ever experienced or heard about a case where a train entered a work limit without authority?

How does PTC-SYSTEM-NAME keep trains from entering work limits?

Has PTC-SYSTEM-NAME changed communication between roadway workers and train crews? Has it changed how train crews use horns and whistles to alert roadway workers of their presence?

Do you have confidence that the PTC-SYSTEM-NAME will keep trains from entering work limits?

Do you have any concerns about the reliability or effectiveness of PTC-SYSTEM-NAME?

OTHER CONTRIBUTORS TO ROADWAY WORKER ACCIDENTS – INJURIES AND DEATHS

So far we've talked about accidents that occur because a train is exceeding a speed restriction or is somewhere it isn't supposed to be. These accidents are explicitly addressed by PTC-SYSTEM-NAME.

We'd also like your perspective on other types of accidents where a roadway worker is struck by a train. Our aim is to understand how new PTC or related technologies could be used to reduce those types of accidents as well.

A recent review of roadway worker fatalities found that 34 percent were the result of being struck by a train while working, 17 percent were caused by being struck by a train on an adjacent track, and 16 percent were caused by walking into a train, on the way to or back from a job.

Can we talk about each of these; what are some of the things that contribute to those types of accidents?

Let's start with struck by train while working.

What kinds of situations are there where a train is allowed to travel on track where roadway workers are working? (Working limits versus train approach warning versus individual train detect)

How are roadway workers alerted that a train is approaching?

What factors might cause a roadway worker to fail to clear the track in time?

- Training
- Experience
- Weather
- Visibility/hearing
- Communication errors
- Complacency
- Fatigue
- Other factors

Are the factors the same for working limits versus train approach warning versus individual train detect?

What might cause a roadway worker to be outside their limits of authority? Wrong track? Wrong portion of territory? Wrong time? (authority expired)

What about struck by a train on adjacent track?

Is it common to have situations where a roadway worker would be working on a track and a train could be going by on an adjacent track?

In those cases, how would the roadway worker know that a train might be coming through on the adjacent track?

How are roadway workers alerted that a train is approaching?

Would there be a lookout assigned to look out for a train?

Would the train be informed that there were roadway workers on the track?

What factors might cause a roadway worker to inadvertently foul the adjacent track and be struck?

- Training
- Experience
- Weather
- Visibility/hearing
- Communication errors
- Complacency
- Fatigue
- Other factors

Are the factors the same for working limits versus train approach warning versus individual train detect?

What about walking into train?

What factors might cause a roadway worker to walk on a track where a train might come by, either on the way too or back from work?

- Training
- Experience
- Weather
- Visibility/hearing
- Communication errors
- Complacency
- Fatigue
- Other factors

ADDITIONAL OPPORTUNITIES TO IMPROVE ROADWAY WORKER SAFETY

We've talked about several types of roadway worker accidents that are not explicitly addressed by PTC-SYSTEM-NAME. Do you feel that new PTC technology could help prevent those types of accidents?

Do you have suggestions for how new technologies, such as GPS or new communication technologies, could be used to reduce the potential for roadway worker accidents?

For example, a hand-held device that would include GPS that would help to locate where the roadway workers were and provide alerts to approaching trains?

ENDING

All things considered, do you think that PTC-SYSTEM-NAME is a good system?

Do you think it makes train operations safer?

If you had 5 minutes to talk with key designers, what would you say?

- Are there any minor modifications to PTC-SYSTEM-NAME that you would suggest to increase its impact on safety?
- Any major redesign?

Are there any things you would suggest trying to do better in the next PTC system based on the lessons learned from PTC-SYSTEM-NAME?

Is there anything that we should have asked about but didn't? Anything that you came wanting to say that you didn't get a chance to say?

Appendix C.
Focus Group Questions for Maintenance-of-Way Employees

INTRODUCTION

Welcome.

Thanks for taking the time to join in this group discussion on impact of the on train operations.

I work as a contractor for the Volpe National Transportation Systems Center and FRA.

This is … who is working with me on this project for the Volpe National Transportation Systems Center and FRA.

The Volpe National Transportation Systems Center and FRA are participating along with representatives of RAILROAD-NAME and other railroads, as well as representatives of labor on an RSAC working group that is looking at the impact of new train technologies such as PTC-SYSTEM-NAME on train operations and safety. The objective is to learn from the experiences of systems such as PTC-SYSTEM-NAME to provide input for future Positive Train Control Systems.

By safety we mean reducing the potential for accidents leading to deaths and injuries to crews, roadway workers, and the public.

As part of this work, we are conducting interviews and focus groups to obtain input from locomotive engineers, conductors, trackmen, signalmen, and electrical technicians to understand the impact of PTC-SYSTEM-NAME from their perspective.

Our particular concern is on Human Factors Issues. How PTC-SYSTEM-NAME impacts your ability to do your job and to maintain safety. We are interested in finding out what things about PTC-SYSTEM-NAME make it easier for you and how it improves safety. We are also interested in any problems that you have encountered with PTC-SYSTEM-NAME and any concerns you might have on its impact on safety.

Your opinions and suggestions are very important to us and will help shape the kinds of new technologies that are introduced in the future. Both your National and Local labor representatives and support this effort and hope that you will give your honest opinions and suggestions.

With your permission, we would like to tape record the session because we don’t want to miss any of your comments. Your comments will remain strictly confidential.

While we will be writing a report summarizing what we learned, inputs of individuals will remain anonymous.

Also, if at any point you would like us to turn off the tape recorder or erase something said earlier, we will do so. Is it OK to tape record?

Keep in mind that we’re just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

We expect that you will have different points of view. Please feel free to share your point of view even if it differs from what others have said.

If you want to follow up on something that someone has said, you want to agree, or disagree, or give an example, feel free to do that. We are here to ask questions, listen, and make sure that everyone has a chance to share. We're interested in hearing from each of you. So if you're talking a lot, I may ask you to give others a chance. And, if you aren't saying much, I may call on you. We just want to make sure we hear from all of you.

OPENING QUESTION

Tell us who you are, and a little about your railroad background.

What territory do you cover? What proportion is PTC-SYSTEM-NAME territory?

THE ROLE OF PTC-SYSTEM-NAME IN INCREASING WORKER PROTECTION

One of the objectives of the PTC-SYSTEM-NAME system is to provide an additional level of protection to roadway workers by ensuring that a train cannot enter their work limits or exceed the maximum authorized speed specified by a slow order.

First, we'd like to understand what kinds of accidents happen and why when the PTC-SYSTEM-NAME system is not there (in non-PTC-SYSTEM-NAME territory), and then we'd like your input on whether PTC-SYSTEM-NAME helps prevent these types of accidents and how.

So let's start with trains entering a work limit without authority.

In a non-PTC-SYSTEM-NAME territory (or this territory before PTC-SYSTEM-NAME), how are work limits protected?

How does a train get authority to enter a work limit?

What indications does a train crew have that they are approaching a work zone?

What things might lead to a train to enter a work limit without authority?

Have you ever experienced or heard about a case where a train entered a work limit without authority?

How does PTC-SYSTEM-NAME keep trains from entering work limits?

Has PTC-SYSTEM-NAME changed communication between roadway workers and train crews? Has it changed how train crews use horns and whistles to alert roadway workers of their presence?

Do you have confidence that the PTC-SYSTEM-NAME will keep trains from entering work limits?

Have you ever experienced or heard of a case where PTC-SYSTEM-NAME failed to prevent a train from entering a work limit without authority?

Do you have any concerns about the reliability or effectiveness of PTC-SYSTEM-NAME?

Let’s turn to trains exceeding their maximum authorized speed limits set by a slow order.

In a non-PTC-SYSTEM-NAME territory (or this territory before PTC-SYSTEM-NAME), how are slow orders communicated to train crews?

What indications does a train crew have that they are about to enter a restricted speed zone?

What things might lead to a train to exceed the maximum authorized speed limits set by a slow-order?

Have you ever experienced or heard about a case where a train exceeded a slow order speed limit? What factors contributed to it?

How does PTC-SYSTEM-NAME ensure that a train doesn’t exceed the maximum authorized speed limit specified by a slow order?

Do you have confidence that the PTC-SYSTEM-NAME will keep trains from exceeding slow order speed limits?

Have you ever experienced or heard of a case where PTC-SYSTEM-NAME failed to prevent a train from exceeding a slow order speed limit?

Do you have any concerns about the reliability or effectiveness of PTC-SYSTEM-NAME?

Are there any other issues you can think of relating to the introduction of PTC-SYSTEM-NAME? Any concerns you might have?

IMPACT OF INCREASED TRAIN SPEED WITH PTC-SYSTEM-NAME

One of the things about PTC-SYSTEM-NAME is that it allows trains to travel at a higher speed.

Has the change in train speed impacted how you do your job?

Does the increase in train speed impact the potential for accidents?

OTHER CONTRIBUTORS TO ROADWAY WORKER ACCIDENTS – INJURIES AND DEATHS (ASK OF SIGNALMEN AND TRACKMEN)

So far we’ve talked about accidents that occur because a train is exceeding a speed restriction or is somewhere it isn’t supposed to be. These accidents are explicitly addressed by PTC-SYSTEM-NAME.

We’d also like your perspective on other types of accidents where a roadway worker is struck by a train. Our aim is to understand how new PTC or related technologies could be used to reduce those types of accidents as well.

A recent review of roadway worker fatalities found that 34 percent were the result of being struck by a train while working, 17 percent were caused by being struck by a train on an adjacent track, and 16 percent were caused by walking into a train, on the way to or back from a job.

Can we talk about each of these; what are some of the things that contribute to those types of accidents?

Let’s start with struck by train while working.

What kinds of situations are there where a train is allowed to travel on track where roadway workers are working? (Working limits versus train approach warning versus individual train detect)

How are roadway workers alerted that a train is approaching?

What factors might cause a roadway worker to fail to clear the track in time?

- Training
- Experience
- Weather
- Visibility/hearing
- Communication errors
- Complacency
- Fatigue
- Other factors

Are the factors the same for working limits versus train approach warning versus individual train detect?

What might cause a roadway worker to be outside their limits of authority? Wrong track? Wrong portion of territory? Wrong time? (authority expired)

What about struck by a train on adjacent track?

Is it common to have situations where a roadway worker would be working on a track and a train could be going by on an adjacent track?

In those cases, how would the roadway worker know that a train might be coming through on the adjacent track?

How are roadway workers alerted that a train is approaching?

Would there by a lookout assigned to look out for a train?

Would the train be informed that there were roadway workers on the track?

What factors might cause a roadway worker to inadvertently foul the adjacent track and be struck?

- Training
- Experience
- Weather
- Visibility/hearing
- Communication errors
- Complacency
- Fatigue
- Other factors

Are the factors the same for working limits versus train approach warning versus individual train detect?

What about walking into train?

What factors might cause a roadway worker to walk on a track where a train might come by, either on the way too or back from work?

- Training
- Experience
- Weather
- Visibility/hearing
- Communication errors
- Complacency
- Fatigue
- Other factors

ADDITIONAL OPPORTUNITIES TO IMPROVE ROADWAY WORKER SAFETY

We've talked about several types of roadway worker accidents that are not explicitly addressed by PTC-SYSTEM-NAME. Do you feel that technologies such as PTC-SYSTEM-NAME could help prevent those types of accidents?

Do you have suggestions for how new technologies, such as GPS or new communication technologies, could be used to reduce the potential for roadway worker accidents?

For example, a hand-held device that would include GPS that would help to locate where the roadway workers were and provide alerts to approaching trains?

ENDING

All things considered, do you think that PTC-SYSTEM-NAME is a good system?

Do you think it makes train operations safer?

If you had 5 minutes to talk with key designers, what would you say?

- Are there any minor modifications to PTC-SYSTEM-NAME that you would suggest to increase its impact?
- Any major redesign?

Are there any things you would suggest trying to do better in the next PTC system based on the lessons learned from PTC-SYSTEM-NAME?

Is there anything that we should have asked about but did not? Anything that you came wanting to say that you did not get a chance to say?

Appendix D.
Focus Group Questions for Mechanical Department Employees

INTRODUCTION

Welcome.

Thanks for taking the time to join in this group discussion on impact of the PTC-SYSTEM-NAME on train operations.

I'm …, I work as a contractor for the Volpe National Transportation Systems Center and FRA.

This is … who is working with me on this project for the Volpe National Transportation Systems Center and FRA.

The Volpe National Transportation Systems Center and FRA are participating along with representatives of Amtrak and other railroads, as well as representatives of labor on an RSAC working group that is looking at the impact of new train technologies such as PTC-SYSTEM-NAME on train operations and safety. The objective is to learn from the experiences of systems such as PTC-SYSTEM-NAME to provide input for the design, operation, and evaluation of future Positive Train Control Systems.

By safety we mean reducing the potential for accidents leading to deaths and injuries to crews, roadway workers, and the public.

As part of this work, we are conducting interviews and focus groups to obtain input from locomotive engineers, conductors, signal maintenance personnel, and mechanical department maintenance personnel to understand the impact of PTC-SYSTEM-NAME from their perspective.

Our particular concern is on Human Factors Issues. How PTC-SYSTEM-NAME impacts your ability to do your job and to maintain safety. One topic we are interested in is maintenance issues associated with the introduction of new technologies such as PTC-SYSTEM-NAME. We are interested in how easy new systems such as PTC-SYSTEM-NAME are to maintain, what new maintenance challenges these new technologies pose, and what new training requirements and activities they bring.

Your opinions and suggestions are very important to us and will help shape the kinds of new technologies that are introduced in the future. Both your National and Local labor representatives and RAILROAD-NAME support this effort and hope that you will give your honest opinions and suggestions.

With your permission, we would like to tape record the session because we don't want to miss any of your comments. Your comments will remain strictly confidential.

While we will be writing a report summarizing what we learned, inputs of individuals will remain anonymous.

Also, if at any point you would like us to turn off the tape recorder or erase something said earlier, we will do so. Is it OK to tape record?

Keep in mind that we're just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

We expect that you will have different points of view. Please feel free to share your point of view even if it differs from what others have said.

If you want to follow up on something that someone has said, you want to agree, or disagree, or give an example, feel free to do that. We are here to ask questions, listen, and make sure that everyone has a chance to share. We're interested in hearing from each of you. So if you're talking a lot, I may ask you to give others a chance. And, if you aren't saying much, I may call on you. We just want to make sure we hear from all of you.

OPENING QUESTION

Tell us who you are, your job title, and your background.

MAINTENANCE ACTIVITIES ASSOCIATED WITH PTC-SYSTEM-NAME

Can you tell us some of the major maintenance activities associated with PTC-SYSTEM-NAME?

What are some of the most common problems that have arisen with PTC-SYSTEM-NAME?

What are some of the most difficult aspects of maintaining PTC-SYSTEM-NAME? Troubleshooting PTC-SYSTEM-NAME problems when things go wrong?

Do you get involved in maintaining PTC-SYSTEM-NAME software? Upgrading software? Is version control an issue?

Were there any issues that arose during the PTC-SYSTEM-NAME installation process?

TRAINING ON PTC-SYSTEM-NAME

Can you tell us what training you received on PTC-SYSTEM-NAME? Do you feel the training was sufficient?

CHALLENGES TO MAINTENANCE

One of the areas we are concerned about are factors that can make maintenance more challenging and contribute to maintenance errors that can impact safety. Experience from other industries such as aviation suggest a number of factors that can contribute to maintenance errors.

I'm going to mention some of the factors that have been identified as challenges to maintenance in other industries, ask if they are an issue for you, and particularly if they are an issue with respect to maintenance of PTC-SYSTEM-NAME systems.

- Lack of appropriate tools/equipment: Need to jury-rig equipment
- Problems in the physical environment
- Inadequate documentation
- Unworkable procedures/need for work-arounds
- Need to maintain private brain book
- Time pressure
- Communication problems
    - Within a team
    - During shift turnover

  - Communication with vendors who supply the equipment and provide hardware and software upgrades
  - Communication with users of the equipment
- Fatigue
- Lack of training/experience
- Organizational problems
  - Inadequate supervision
  - Inadequate policies

ERRORS AND NEAR MISSES

Have there been any recent cases where a maintenance error or near-miss occurred? Can you describe the factors that contributed to it?

ENDING

From the perspective of ease of maintenance and prevention of maintenance errors, if you had 5 minutes to talk with key designers, what would you say?

- Are there any minor modifications to PTC-SYSTEM-NAME that you would suggest to make it easier to maintain and reduce the potential for maintenance errors?
- Any major redesign?

How about recommendations with respect to training, documentation, or policies?

Are there any things you would suggest trying to do better in the next PTC system based on the lessons learned from PTC-SYSTEM-NAME?

Is there anything that we should have asked about but did not? Anything that you came wanting to say that you did not get a chance to say?

Appendix E.
Event Analysis Case Studies

The following five case studies apply a structured methodology for analyzing human errors issues in railroad accidents. The methodology *A Technique for Human Event Analysis* (ATHEANA) was developed for human reliability analysis in the nuclear power industry.

The purpose of this methodology was to accommodate and represent human performance in probabilistic risk assessments to resolve safety questions (Forester et al., 2000). The methodology assumes that significant human errors occur as a result of a combination of influences. These influences include operating conditions, as well as human-centered factors. The ATHEANA methodology provides a framework to represent the interrelationships among error mechanisms, operating conditions, and performance-shaping factors that set them up, and the consequences of the error mechanisms in terms of how the overall system can be rendered less safe.

The five case studies illustrate this methodology through its application to a variety of train collisions and derailments previously reported by the National Transportation Safety Board or the Federal Railroad Administration.

Event Analysis: Derailment and Collision at Back Bay Station, Boston, Massachusetts.

Type of Accident: Derailment and Collision

Date and time: December 12, 1990, 8:23am EST

Location: Back Bay Station, Boston.

Railroad: AMTRAK & MBTA

Fatalities/injuries: 0/453

Other losses: $12,675,000

Data sources: (FRA, NTSB, railroad, press): NTSB/RAR-92/01; Boston Globe Article: *280 Hurt in Back Bay Crash Riders Flee Smoke-Filled Tunnel; Area Damaged,* Dec 13, 1990

Data entry by: John Wreathall

Event Summary

Event description: At 8:23am, Amtrak train 66 (The Night Owl) derailed and struck MBTA commuter train 906 as both entered Back Bay Station, Boston, MA. The Amtrak train was traveling at 76 mph within a 30 mph speed restriction, on a 9 degree curve in a tunnel. It derailed and struck the MBTA train on the adjacent track. A fire ignited after the collision. The Amtrak train was being operated by an apprentice engineer under supervision of the locomotive engineer. The engineer reported that the train braking did not perform as expected, but subsequent testing did not find any faults, and the speed history on the train event recorder showed that braking was started late (~26 sec) and was not consistent with "normal" train handling, as taught or as described by other engineers. There was no speed sign indicating the speed limit.

Event surprises: That the event happened at all: the apprentice engineer had operated 2 Amtrak trains into Boston in the days before the accident (including Amtrak train 66 on the previous day), and had been on territory familiarity runs into Boston from New Haven in the period August 13 – September 13. The locomotive engineer was well experienced, with about 21 years operating generally in the New Haven – Boston territory, and had operated Amtrak 66 as a regular assignment (5 days /week) since the end of October 1990. (Note: He had two infractions for passing stop signals while distracted, in 1979 and March 1990. He was also involved in a head-on collision accident in New York in July 1984, where 1 fatality and 115 injuries occurred; he was found not at fault.)

FRA/Railroad responses: Amtrak: Installed advanced warning speed limit sign on approach to speed-limited area; installed signal circuitry so the approach signal shows "approach medium" aspect (i.e., speed not to exceed 30 mph)—automatic speed control system (cab signaling system? ACSES?) will enforce this if the engineer does not respond.

NTSB recommendations: Extend inputs to training program evaluation and approval process (FRA); conduct evaluations of engineer training program and improve as necessary (Amtrak, BLE, UTU); develop qualification procedure for apprentice engineers (Amtrak)

Event Characterization

Deviations from expected conditions: None

Any key mismatches between rules/instructions and performance: Failure to comply with generally accepted braking procedure and approach speed profile when approaching Back Bay Station tunnel.

Most negative influences: Lack of experience by apprentice engineer. In training program, he had weak scores for train handling in classroom and simulator settings.

Lack of supervision by engineer (assumed). Supervising engineer identified in previous events as someone who can become distracted.

Most positive influences: None identified (?)

Key Work Mode Transition Issues

Mode changes: Apprentice engineer operating train, end of journey

Transfer of control: Apprentice engineer operating train

Shifts in authority: Apprentice engineer operating train under supervision

Skill loss: Engineer in supervisor mode

Coming up to speed: Apprentice engineer operating train

Primary/backup reversion: None

Fixation: End of journey?

Significance of Event:

Extreme or unusual conditions: Apprentice engineer operating train.

Contributing pre-existing conditions: None known

Misleading or wrong information: Engineers reported that locomotive braking performance was not as expected, though NTSB testing indicated that nothing was wrong and the data recorder showed no early braking as reported by engineer. (There was an “air blowing sound” from the brake air valve reported by the apprentice to the supervising engineer, who explained it was “just a bit of dirt” in the valve—“usually no big deal.”)

Information rejected or ignored: The 30 mph speed limit was indicated only by timetable; there was no posted sign for the speed limit.

Multiple hardware failures: None reported

Transitions in progress: End of journey (5 minutes from arriving at last stop)

Similar to other events: Possibly similar to Southall (UK), where train passed signal at danger on the approach to Paddington terminus—driver was occupied with putting stuff in bag.

KEY PARAMETER STATUS

Initial Conditions	Accident Conditions
Train performing normally and was ahead of schedule after earlier delays due to unscheduled stops (baggage car door found open, unscheduled passenger pickup). Some overspeeding eliminated prior delays.	Considerable overspeeding on entering tunnel and approach to Back Bay Station.

TRAIN/PROCESS STATUS

Initial Plant Conditions & Configurations	Accident Conditions & Consequences
Configuration: The train was a mixed Amtrak consist (two different types of passenger cars) of two locomotives, two material handing cars, two baggage cars, 5 passenger cars and a dining car. **Noteworthy Pre-existing Conditions**: There was a buildup of oil on the service brake valves that led to irregular air pressure in the locomotive independent brakes. NTSB concluded this did not contribute to any problems in brake performance. **Initiator**: Overspeeding into the 9° curve at Back Bay Station. (Calculated speed of derail on this bend for the locomotive was approximately 59mph).	**Automatic Responses**: None. (No automated warning or control system was in use at this speed limit.) **Failures**: Failure of the engineers to slow train to speed limit.

Action Summary

Event Timeline:

Key: U = unsafe actions

E = equipment failures (significant to the event)

H = non-error (non-recovery) actions

R = recovery actions

V = event of interest

Pre-Initiator

V1: 10:30pm (12/11). Amtrak 66 departs Washington Union Station

H1: 4:30am (12/12). Locomotive engineer and apprentice engineer (with rest of train crew) report for duty at New Haven. They receive written list of speed limits for the journey to Boston South Station.

H2: 4:36am. Engineer and apprentice board diesel electric locomotive pair in New Haven yard, review defect log and perform locomotive brake tests.

H3: 5:25am. Amtrak 66 departs New Haven on time. Apprentice engineer is operating train under supervision. Locomotive crew performs moving brake test (all OK).

V2: 6:40am. Train stops for 6 minutes for conductor to close open baggage car door—train 6 minutes late as a result.

H4: 6:48am. Supervising engineer cautions apprentice engineer for slowing too early for the stop at Westerly.

U1: 7:06am – 7:46am. Train travels at speeds up to 110mph between Kingston and Providence (train speed limit is 100mph). Supervising engineer cautions apprentice for accelerating to quickly after the stop at Kingston.

V3: 7:56am. Train makes an unscheduled stop for 4 minutes to pick up passengers at S. Attleboro (another train was delayed).

U2: 7:56am – 8:16am. Train travels at speeds up to 110mph between S, Attleboro and Rt. 128 (train speed limit is 100mph).

H4: 8:16+am. Apprentice reports "air blowing sound" near automatic airbrake valve. Engineer tells the apprentice that it is probably "a bit of grit in the valve" and that application and release of the automatic air will stop the problem. The apprentice reportedly follows these directions, both now and at a later time when the same thing happens. [Note: these brake applications are not recorded on the locomotive event recorder. However this may be a result of the actions being shorter in duration than the sampling interval (5.75 sec) on the recorder.]

Initiator

U3: 8:21am. Train passes "Pickle Factory" (MP 225.7) at ~107mph. (This is where other engineers say braking should begin to comply with the 30 mph limit at MP227.)

U4: 8:22am. Apprentice engineer applies full service brake at about MP 226.7, and then reduces throttle power (sequence contrary to training and Amtrak procedure).

V4: 8:23am. Train enters tunnel and passes MP 227 (start of 30 mph speed limit) at ~100 mph (NTSB estimate - data recorder indicates ~103mph).

R1: 8:23am. Emergency braking implemented (evidence of sand on track) 480 feet (or 4 seconds) before derail.

V5: 8:23am. Train derails at MP 227.45 and collides with MTBA Train 906. Final speed recorded before impact is 76mph.

UNSAFE ACTIONS AND OTHER EVENTS

ID	Description
U1	Apprentice engineer over-speeds (~110 mph, train limit is 100mph). Train had been ahead of schedule prior to delay to close baggage car door but is now 6 minutes late.
U2	Apprentice engineer over-speeds (~110 mph). Train had been on schedule prior to unscheduled stop to pick up passengers but is now 4 minutes late.

U3	Supervising engineer tells apprentice to start applying automatic air brakes when approaching Gurgles Street Station (MP 226.2), which is about 0.5 mile after the point that other engineers say they would begin braking.
U4	About 0.5 mile after the point when supervising engineer directed braking to start, apprentice engineer places train in a full service brake with locomotive throttle still in position 8 (full power) and then reduces power setting after a few seconds. Even though the engineer has applied braking, train passes the speed limit at more than 100 mph. The speed reduction rate shown by the event recorder (NTSB report) does not indicate maximum braking at this point.
H1	Crew provided with written speed limits at start of duty. (No visual limit sign is provided at MP 227.)
H2	Change of locomotives takes place at New Haven, from overhead electric to diesel electric, so crew checks locomotives (2) in yard before coupling to train.
H3	Apprentice was scheduled to work this train as part of the Amtrak training program.
H4	Oil contamination was found during the post-crash NTSB testing of the valve, but was determined not to have caused any braking problems.
R1	Supervising engineer places train in emergency braking.

HUMAN DEPENDENCIES

IDs	Dependency Mechanism	Description
None identified		

EVENT DIAGNOSIS LOG

Time	Accident Progression & Symptoms	Response
8:21 am	Train passes “Pickle Factory” (MP 225.7), considered to be the point to start barking bay other engineers.	No action taken. Supervising engineer tells apprentice to start braking action when approaching Ruggles Street Station (MP 226.2). The time to travel from MP 225.7 to 226.2 is estimated to be 16 sec.
8:22 am	Train passes Ruggles Street Station approach signal at about 108 mph.	Apprentice engineer begins braking action about 9 sec after passing signal.
8:23 am	Train reaches MP 227 (start of 30 mph speed restriction) about 9 seconds after start of braking	No extra action taken.
8:23 am	Train approaches curve in tunnel	Supervising engineer initiates emergency braking, 480 feet (4 sec) before derailment.

EVENT ANALYSIS: COLLISION NEAR BRYAN, OHIO

Type of Accident: Collision involving three trains

Date and time: January 17, 1999, 1:58am EST

Location: Near Bryan, OH.

Railroad: Conrail

Fatalities/injuries: 2/0

Other losses: $5,294,000

Data sources: (FRA, NTSB, railroad, press): NTSB/RAR-01/01

Data entry by: John Wreathall

Event Summary

Event description: About 1:58 a.m. on January 17, 1999, three Consolidated Rail Corporation (Conrail) freight trains operating in dense fog on a multiple main track were involved in an accident near Bryan, Ohio. Mail-9, an intermodal train (or "van train" in the parlance of Conrail) traveling westbound on track No. 1, struck the rear of a slower moving westbound van train, TV-7, at milepost (MP) 337.22. The collision caused the derailment of the 3 locomotive units and the first 13 cars of Mail-9 and the last 3 cars of TV-7. The derailed equipment fouled the adjacent No. 2 track area and struck the 12th car of train MGL-16, which was operating eastbound on that track. The impact caused 18 cars in the MGL-16 consist to derail. The derailed equipment from the 3 trains totaled 3 locomotives and 34 cars. The engineer and conductor of Mail-9 were killed in the accident. The crewmembers of TV-7 and MGL-16 were not injured. Figure 1 attached shows the sequence of events (taken from NTSB report).

Event surprises: Mail-9 was operating at or near its authorized speed of 60 mph in spite of the dense fog, whereas TV-7 was operating at below 40 mph because of the fog—the visibility was estimated to between 10 to 15 feet at the crash site. (Conrail operational rules did not require engineers or dispatchers to provide warnings of visibility or other weather problems, though some did by radio. Fog is reported to occur at the accident location about 18 days /year [i.e., 5 percent of the year] on average.)

FRA/Railroad responses:

NTSB recommendations: Develop and facilitate PTC systems for high-risk areas (to FRA); ensure that operational efficiency checks include uniform operating procedures in reduced visibility (to railroads); Advise members of lessons learned from this event (to BLE, UTU, AAR).

Event Characterization

Deviations from expected conditions: Visibility down to less than 10 to 20 feet.

Any key mismatches between rules/instructions and performance: Signals became visible for exceptionally short durations—even less than 1.5 seconds in visibility >200 feet.

All train operations in the area were speeding in excess of the visibility limits, possibly because of commercial (and personal pride) pressures, but some were speeding much in excess of visibility. This inconsistency was a factor that caused trains to ‘bunch up.’

Most negative influences: Visibility

Most positive influences: -

Key Work Mode Transition Issues

Mode changes: Weather-related changes to trains speeds—priority of time pressure vs. visibility requirements.

Transfer of control: The informal use of the road radio by individual train crews to keep other trains informed of their progress could lead to the expectation that an absence of information means an absence of other trains. However the process of announcing progress was not required and its use was intermittent.

Shifts in authority: -

Skill loss: -

Coming up to speed: Crew members of the Mail-9 locomotive had been off duty for about 40 hours (engineer) and 8.5 days (conductor) prior to accident trip.

Primary/backup reversion: -

Fixation: Meeting the schedule

Significance of Event:

Extreme or unusual conditions: Weather (dense fog)

Contributing pre-existing conditions: -

Misleading or wrong information: The informal use of the road radio by individual train crews to keep other trains informed of their progress could lead to the expectation that an absence of information means an absence of other trains. However the process of announcing progress was not required and its use was intermittent. Thus the silence of the slowed train could be thought of as “misleading.”

Information rejected or ignored: -

Multiple hardware failures: -

Transitions in progress: -

Similar to other events: ?

KEY PARAMETER STATUS

Initial Conditions	Accident Conditions
The three intermodal (van) and one mixed freight trains were initially dispatched to run about 10 to 17 minutes apart, with authorized speeds of 60mph (van) or 50mph (mixed).	Trains had closed up because of the delay in getting the first (mixed freight) train onto a siding, and had led to the intermediate trains to slow for signals. Because of the reduced visibility, the crew of the last train (Mail-9) missed an *approach* signal (requiring slowing to no more than 30 mph and be prepared to stop at the next signal) and then missed the next signal displaying *stop-and proceed* (requiring the train to stop, then proceed at no more than 20 mph and be able to stop within half the distance of vision). Mail-9, traveling at 56 mph, caught up to the previous train (TV-7) that was accelerating from a signal and traveling at 8mph.

TRAIN/PROCESS STATUS

Initial Conditions & Configurations	Accident Conditions & Consequences
Configuration: Normal dispatching operations Noteworthy Pre-existing Conditions: Late at night; dense fog Initiator: Train Mail-9 passed two signals traveling at about maximum authorized speed and collided with a slower moving train.	Automatic Responses: None Failures: None

Action Summary

Event Timeline:

Key: U = unsafe actions

E = equipment failures (significant to the event)

H = non-error (non-recovery) actions

R = recovery actions

V = event of interest

Pre-Initiator

V1: 12:15 am, 1/17/1999, High-tonnage mixed freight train PIEL-6A departs Toledo on track 1 of Conrail’s Chicago double track main line.

V2: 12:41am, Van train TV-99 departs Toledo on track 2 for Chicago.

V3: 12:51am, Van train TV-7 departs Toledo on track 1.

V4: 1:08 am, Van train Mail-9 departs Toledo on track 1.

V5: 1:10am, TV-99 crosses over to track 1, behind PIEL-6A.

V6: 1:37am, PIEL-6A passes control point (signal) CP342. Following train TV-99, traveling at 55mph, reaches automatic block signal 3341W (about 8 miles to the rear of PIEL-6A). See Figure 1 for visual representation of this and subsequent events.

V7: 1:46am, TV-99 reaches CP340 indicating an *approach* aspect, and slows in anticipation of a *stop* indication at CP342. TV-7 reaches ABS 3351W indicating *approach* at about 39mph.

V8: 1:50am, TV-99 having stopped at CP342 (because PIEL-6A occupied the next block) now receives an approach aspect and starts to move. TV-7, having been notified that TV-99 was stopped, slows to 5mph in anticipation of a stop-and-proceed aspect at ABS 3381W. MAIL-9 passes CP329 (9 miles to the rear of TV-7) at 60mph.

V9: 1:55am, TV-7, now having an approach aspect at 3381W, begins to accelerate slowly.

U1: 1:55am, MAIL-9, now about 5 miles to the rear of TV-7 and traveling at 56mph, passes 3341W that shows an *approach* aspect.

U2: 1:58am, MAIL-9 passes a *stop-and-proceed* aspect at 3351W at 56mph and collides with TV-7 moving at 8mph.

Initiator: Event U2.

HUMAN DEPENDENCIES

IDs	Dependency Mechanism	Description
U1 & U2 (plus other train operations)	Overspeeding in fog	A combination of personal/professional “pride” plus some evidence of corporate pressure to stick to timetable even in bad weather.

EVENT ANALYSIS: COLLISION NEAR CHASE, MARYLAND

Type of Accident: Rear-End Collision

Date and time: January 4, 1987, December 12, 1990, 1:30 PM EST

Location: Gunpaw Interlocking near Chase, Maryland in the North East Corridor

Railroad: AMTRAK & Consolidated Rail Corporation

Fatalities/injuries: 16/174

Other losses: $16,561,000

Data sources: NTSB/RAR-88/01

Data entry by: Emilie Roth

Acronyms: ACS – Automatic Cab Signal; ATS – Automatic Train Stop; ATC – automatic train control

Event summary

Event description: At about 1:16 PM EST a northbound Contrail train ENS-121 departed Bay View yard at Baltimore, Maryland, on track 1. The train consisted of three diesel-electric freight locomotive units. At around the same time a northbound Amtrak passenger train 94 left Pennsylvania Station in Baltimore on track 2. The passenger train included a “vintage” car.

Track 1 and Track 2 converge at the Gunpow interlocking to a single track (Track 2)

The block station operator requested that switch 12 at Gunpow, a remote-controlled interlocking, be lined for straight through movement on track 2, so that the Amtrak train could go through first. The wayside signal aspects displayed for Amtrak train 94 approaching Gunpow on track 2 were “clear” at both the distant (816-2) and home (2N) signal locations. The wayside signal aspects for Conrail ENS-121 on track 1 were “approach” at the distant signal (816-1) and “stop” at the home signal (1N).

The Conrail ENS-121 train crew (Locomotive Engineer and Brakeman) appeared to have missed both signals (or at least were delayed in observing the second signal) and at 1:30 PM went through switch 12 at Gunpow (in spite of the fact that it was not aligned for this movement). When this happened, the aspect of signal 2N for track 2 changed from “clear” to “stop”. The engineer of train 94 saw the change in signal and put the train into Emergency braking. However, the train was traveling between 120 and 125 mph and could not be stopped before colliding into train ENS-121. The engineer and 15 passengers on train 94 died.

Event surprises: There were several surprising aspects of this event.

- Most importantly was that the train crew on Conrail ENS-121 missed one and possibly two signals.
- In addition both trains were traveling at speeds greater than they were supposed to be. Had the trains been traveling at the required speed, the collision might have been avoided or at least might have been less severe.

- In addition, the accident occurred very close in time and space to when Conrail ENS-121 first entered the interlocking without authority. Specifically Train ENS-121 came to a stop 349 feet beyond the home signal for the Gunpow interlocking.
- There was evidence that the Automatic Cab Signal alerter whistle on Conrail ENS-121 that was designed to sound if a train violated a signaled condition, had been disabled at some earlier point in time (the sound was muted) so that it failed to alert the Conrail train crew that they had missed the signals.
- There was evidence of problems in organizational culture at Amtrak:
    - That placed pressure for on-time service resulting in perceived pressure to exceed speed limits (or at least interpret them liberally).
    - There were problems in rules and procedures that created ambiguity in what the applicable speed restrictions were and who was responsible for informing whom about what.
- Finally, there was evidence that the Conrail ENS-121 train crew's performance may have been impaired from marijuana. The evidence was circumstantial but this was the conclusion drawn by the NTSB.

<u>NTSB recommendations</u>:

NTSB identified a number of issues including:

- Adequacy of the signal and safety backup systems
- Amtrak's dispatching and management concern with on-time performance
- Compatibility of freight trains with high-speed passenger trains in a high-density train environment

NTSB concluded that FRA and AMTRAK should have required Conrail to use automatic safety backup devices on all trains in the Northeast Corridor (i.e., PTC systems). They recommended that all locomotives operating on the high-speed passenger train trackage of the NEC should be equipped with Automatic Train control. They also recommended that pending installation of the ATC devices that all locomotives and trains not equipped with such devices be required to stop before entry onto the high speed tracks regardless of signal aspect, and to request and receive permission before proceeding.

<u>FRA/Railroad responses</u>: Amtrak agreed for a need for Automatic Train Control (ATC) on all locomotives operating on the Northeast Corridor, however they indicated that it is up to FRA to require freight and commuter trains using the NEC to be equipped with ATC. With respect to the NTSB suggestion that all trains not equipped with ATC stop before entry onto the high-speed tracks, Amtrak indicated that it would be neither effective nor practical. Amtrak did put in place limits on all freight traffic to 30 mph between 6 am and 10 pm (when there is high speed passenger train traffic). The safety board indicated that they did not feel these measures would provide the requisite protection "since engineers who would disregard restrictive signals would be likely to disregard speed limitations as well. " Conrail indicated that they were considering retrofitting its locomotive units with some form of ATS or ATC. They also indicated that they

were considering replacing the air-operated ACS alerter whistle with an electronic ‘warbling” device that was less irritating and could not be nullified.

As of Dec. 1987 Conrail had installed ATS and electronic alerters on 841 of the 1,583 locomotive units in service.

In May 1987 the DOT proposed that all trains operating on the NEC between Washington and Boston be fitted with ATC. The proposal was adopted under FRA Order Docket 87-2 on Nov. 19, 1987. Installation was to be completed by January 1990.

Event characterization

Deviations from expected conditions: There were several deviations from expected conditions:

- Amtrak 94 included a Heritage-class passenger car, which meant that it should have been traveling at a restricted speed of 105, instead of the maximum authorized speed of 125 mph. The dispatcher was not aware that Amtrak 94 had a Heritage-class car.
- Conrail train ENS-121 consisted of three diesel-electric freight locomotives, resulting in ambiguity as to whether it qualified as a ‘freight train’ that needed to obey freight train speed restrictions of 50 mph.
- Normally every effort is made to operate Conrail’s freight trains over the corridor during the ‘window’ when there are no passenger trains (11:56 pm to 6:43 AM) so that freight trains and passenger trains would generally not operate at the same time. This was an unscheduled freight run.
- Because of the New Year holiday, Amtrak was operating on an expanded Sunday schedule on the day of the accident.
- The cab signal alerter whistle was not operational. There was also a missing light bulb in the ACS
- The Conrail Engineer had a history of speeding and DUI (in a car) and may have been a regular marijuana smoker. The brakeman may have been a regular marijuana smoker as well and this may have contributed to their performance problems.

Any key mismatches between rules/instructions and performance:

- Both trains were going faster than the applicable speed limit.
- Conrail train ENS-121 left the train yard without the proper safety equipment functioning. In particular, the deadman pedal inoperative, no functioning console radio, muted ACS alerter whistle, and missing ACS light bulb.

Most negative influences:

- The performance of locomotive engineer and brakeman on Conrail Train ENS-121 may have been degraded due to marijuana.

Most positive influences: None identified (?)

Key Work Mode Transition Issues

Mode changes: The Conrail locomotive engineer was used to traveling this route at night when Amtrak trains were not running. Consequently he may not have expected an Amtrak train, and have expected that the dispatcher would have set the switch to allow him to switch from track 1 to track 2 without stopping.

Also, since Conrail scheduled its freight trains in and out of Baltimore at night and this was not a scheduled event, it is probable that the engineer and brakeman did not expect to be called to work on the day of the accident. [Both men had been drinking alcoholic beverages the night before.]

Transfer of control:

Shifts in authority:

Skill loss:

Coming up to speed:

Primary/backup reversion:

Fixation:

Significance of Event:

Extreme or unusual conditions:

- Amtrak 94 included a Heritage-class passenger car, which meant that it should have been traveling at a restricted speed of 105, instead of the maximum authorized speed of 125 mph. The dispatcher was not aware that Amtrak 94 had a Heritage-class car.
- Conrail train ENS-121 consisted of three diesel-electric freight locomotives, resulting in ambiguity as to whether it qualified as a 'freight train' that needed to obey freight train speed restrictions of 50 mph.

Contributing pre-existing conditions:

- Multiple, complex rules that created ambiguity with respect to which rule or procedure applied:
    - Applicable speed limit for train ENS-121. [Amtrak's general manager interpreted the rules to say that the 50 mph maximum freight train speed applied; Conversely Amtrak general superintended considered that this was superseded by rule 1157 G1 that provided a maximum of 60 mph. If these top-level managers could not agree on the applicable speed limit, how would the Conrail ENS-121 be expected to know the appropriate rule that applied?]
    - Whether and how dispatcher should have been informed that train 94 contained a Heritage class car, and thus that its speed was restricted to 105 mph.
- A culture at Amtrak that stressed on-time schedule and de-emphasized safety. NTSB wrote, "safety has not had sufficient management support" and "corridor speed and schedules were paramount, perhaps even above safety."

- Amtrak train 94 was 5 ½ minutes behind schedule and was being followed by Amtrak train 112 (4 minutes later) on track 2, which was also behind schedule.
- There was an organizational climate that placed pressure on train crews to meet schedules.
    - In the aftermath of a head-on collision of two Amtrak passenger trains at Hell Gate, New York, on July 23, 1984, the president of the Brotherhood of Locomotive Engineers asserted that Amtrak supervisors were encouraging and even 'pressuring' corridor engineers to violate speed restrictions in order to maintain scheduled running times.
    - Before beginning an assessment in August 1984, FRA noted that Amtrak trains tended to be operated at speeds in excess of allowable limits.
- The dispatcher was not made aware that Amtrak train 94 included a Heritage-class passenger car, which required it to run at a reduced speed of 105 mph. As a result he allowed Amtrak train 94 to go ahead of Amtrak train 112, which could go at 125 mph, and was 47 minutes behind schedule already. There was no procedure in effect to make the Dispatcher aware of the inclusion of a Heritage class passenger car. The general superintendent in charge of the Philadelphia Division stated that it was the conductors' responsibility to notify the Dispatcher of any restricted speed cars in their trains.

<u>Misleading or wrong information</u>:

- In Cab signal unit of Conrail train ENS-121 may have not displayed 'approach' signal aspect because of a missing bulb.
- Cab signal alerter whistle on train Conrail ENS-121 failed to sound when the cab signal changed to a more restrictive aspect.

<u>Information rejected or ignored</u>:

- Locomotive Engineer missed the wayside signal aspects for the distant signal (approach signal aspect) and possibly also the home signal 'stop'.

<u>Multiple hardware failures</u>:

- There was a missing bulb in the four-aspect cab signal unit for the Conrail ENS-121 train (the Cab signals are: clear, approach medium, approach and restricting) so that the 'approach' aspect may not have lit up when the train reached the distant signal.
- If an engineer fails to acknowledge a more restrictive cab signal aspect, a loud shrill air-operated whistle is supposed to be activated in the cab when the wayside signal is passed. However, in Conrail train ENS-121 this whistle appeared to have been disabled. Specifically, investigators found that the port of the whistle was wrapped tightly with duct tape severely dampening the sound of the whistle so that it could not be heard over the sound of an idling engine.
- The console radio on Conrail train ENS-121 was not working. The crewmembers attempted to fix it prior to departure but were not able to. Instead they checked out a portable radio with a relatively short transmitting range. This violated rules requiring a functioning console radio.

Transitions in progress: Going from two tracks (Track 1 and Track 2) to one track (Track 2). More specifically at the Gunpow interlocking, the four-tracked NEC converged to two tracks on the bridge spanning the Gunpowder River.

Complacency issues: There is some (small) possibility that the Conrail ENS 121 crew were relying on the alerter whistle, which did not sound because it had been muted with duct tape. The NTSB noted that when the ACS system was fully functional, it made the wayside signal system appear to be redundant. The SB believes that the engineers may have become dependent on the ACS aspects. However, they note that the operating rules still require engineers to observe and respond to wayside signals and ACS. Quote "The ACS system is merely a backup to the wayside signal system and an aid to the locomotive crew when visibility is poor."

Similar to other events:

- In 1979 the Safety board investigated a rear-end collision that killed two crewmembers on the Union Pacific Railroad. In that accident, a brakeman muted the ACS alerter whistle with a rag; a relieving crew later went past a 'stop and proceed' wayside signal with a 'restricting' aspect on the ACS and struck another train. As a result of its investigation, the Safety Board recommended that UP modify its ACS apparatus to provide to automatic penalty brake application when the engineer fails to acknowledge a more restrictive signal.
- Possibly similar to Southall (UK), where train passed signal at danger on the approach to Paddington terminus—driver was occupied with putting stuff in bag. In this case the failure of the brakeman off ENS-121 to observe the two wayside signals may have been partly due to the fact that he was not observing the signals at the time they were passed.

KEY PARAMETER STATUS

Initial Conditions	Accident Conditions
Conrail train ENS-121 left Bay View yard at Baltimore, MA at about 1:16 PM on its way to Harrisburg, PA. Almost simultaneously Amtrak train 94 left the Pennsylvania Station in Baltimore, 3.8 miles south of Bay View. Train 94 left Baltimore 5 and ½ minutes behind schedule. Further, Amtrak passenger Train 112 left Baltimore on track 2 about 4 minutes behind train 94 and about 47 minutes behind schedule.	

TRAIN/PROCESS STATUS

Initial Plant Conditions & Configurations	Accident Conditions & Consequences
Configuration: Conrail train ENS-121 consisted of three diesel-electric freight locomotive units	**Automatic Responses**: None. (The automated alerter whistle that was supposed to sound when the cab signal changed to a more

manned by an engineer and a brakeman.

Amtrak train 94 consisted of two electric locomotives, nine coaches, and three food service cars. Most significantly it included a Heritage class passenger car which meant that meant that its speed was restricted 105 mph according to the NEC timetable rule

In addition to an engineer, conductor and three assistant conductors, there were 7 Amtrak service employees and about 660 passengers on the train.

Noteworthy Pre-existing Conditions: See text -- lots

Initiator: The Engineer on Conrail Train ENS-121 failed to stop his train in compliance with home signal 1N before it fouled track 2 at Gunpow.

restrictive aspect was suppressed.)

Failures: Failure of the Engineer and Brakeman on Train ENS-121 to observe the two restrictive signal aspects. As a result, the train entered the Gunpow interlocking fowling track 2.

Action Summary

Event Timeline:

Key: U = unsafe actions

E = equipment failures (significant to the event)

H = non-error (non-recovery) actions

R = recovery actions

V = event of interest

Pre-Initiator:

V1: Approx. 12:16 pm EST the ENS-121 crew arrived for duty one hour before train departure time.

U1: Crew of ENS-121 was responsible for pre-departure testing. The console radio on the lead Engine was not functioning. They tried to fix it but failed. Instead they checked out a portable radio with a relatively short transmitting range. This violates rules requiring a working console radio. Also it is not clear that they tested ACS equipment as required. After the accident it was determined that the ACS alerter whistle had been muted by wrapping duct tape. In addition, there was a bulb missing for the ‘approach’ aspect of the ACS. In addition, the deadman pedal was inoperative. All this points to inadequate pre-departure testing.

V2: 1:16 pm EST Northbound Conrail freight train ENS-121 left Conrail’s Bay View Yard and entered the Northeast Corridor (NEC) onto Amtrak’s main track 1.

U2: Conrail train ENS-121 was traveling at approximately 64 mph, whereas the speed restriction in effect for freight trains on track 1 was 50 mph (and 60 mph for passenger trains).

U3: The dispatcher decided to allow Amtrak Train 94 to go ahead of Amtrak train 112, even though Amtrak Train 94 was supposed to operate at a lower speed (105 mph) than Amtrak train 112 (125 mph).

V3: Approx. 1:16 pm EST Amtrak's northbound passenger train 94, left the Pennsylvania station in Baltimore, 3.8 miles south of Bay view on Track 2.

V4: 1:20 pm EST Amtrak train 112 leaves Pennsylvania station behind Amtrak train 94 on track 2. It was 47 minutes behind schedule

U4: Amtrak train 94 traveled at between 120 and 125 mph even though it contained a Heritage car that meant its speed was restricted to 105 mph. The conductor said that he had informed the Locomotive Engineer of the speed restriction.

V5: At 1:29 pm Block station operator controlled the remote control switch at the Gunpow interlocking (Switch 12) so that it was lined up for through movement on track 2. This resulted in the wayside signals displayed for train 94 to be 'clear" permitting the train to proceed at maximum authorized speed. The northbound home signal for track one displayed 'stop' and the distant signal for track 1 (located 10, 318 feet south of the home signal) displayed 'approach".

U5: The Locomotive Engineer and the Brakeman on Conrail train ENS-121 failed to observe the "approach" signal aspect at the distant signal on track 1.

V6: Automatic cab signals (ACS) in the lead locomotive cabs of both trains should had had corresponding signals.

E1: There was a light bulb missing in the ACS for train ENS-121, as a result the 'approach' aspect did not come on.

E2: If an engineer fails to acknowledge a more restrictive cab signal aspect, a loud shrill air-operated whistle is supposed to be activated in the cab when the wayside signal is passed. However, in Conrail train ENS-121 this whistle appeared to have been disabled. As a result it likely did not come on loud enough to alert the Engineer that he passed a signal at danger.

U6: The locomotive Engineer and the Brakeman on Conrail train ENS-121 failed to observe (or were delayed in observing) the 'stop' signal aspect on the home signal on track 1.

Initiator:

U7: 1:29.24 PM, EST Conrail train ENS-121 entered switch 12 at Gunpow and moved onto track 2. The train was going at 64 mph.

V7: 1:29:26 Home signal on track 2 switched to display 'stop' aspect for Amtrak train 94.

V8: 1:29: ?? PM EST (a few seconds later), train ENS 121 was struck in the rear by Amtrak train 94. The engineer of train 94 apparently recognized that the aspect of signal 2N was 'stop' and put his train into emergency braking, but the train was traveling between 120 and 125 mph, and could not be stopped before colliding with train ENS-121.

UNSAFE ACTIONS AND OTHER EVENTS

ID	Description
U2	Conrail train ENS-121 was traveling at approximately 64 mph, whereas the speed restriction in effect for freight trains on track 1 was 50 mph (and 60 mph for passenger trains). There was difference of opinion with respect to whether the rule restricting travel to 50mph applied to Conrail train ENS-121 because it was made up of locomotive engines – it was argued that perhaps the rule applying to ‘freight trains’ did not apply to train ENS-121. The Amtrak general manager-transportation indicated that train ENS-121 was not a freight train and was subject to passenger train track speeds of up to 60 mph.
U3	The dispatcher decided to allow Amtrak Train 94 to go ahead of Amtrak train 112, even though Amtrak Train 94 was supposed to operate at a lower speed (105 mph) than Amtrak train 112 (125 mph). Apparently no one informed the dispatcher that Amtrak train 94 contained a Heritage car and was therefore supposed to travel at only 105 mph. There was ambiguity as to whether the Conductor on train 94 was responsible to tell the Dispatcher.
U4	Amtrak train 94 traveled at between 120 and 125 mph even though it contained a Heritage car that meant its speed was restricted to 105 mph. The conductor said that he had informed the Locomotive Engineer of the speed restriction. It is possible that the Engineer assumed the dispatcher wanted him to go at 125 mph since he had train 94 go in front of train. Had train 94 been going at 105 mph the train would have been able to stop more than 1,000 feet short of a collision.
U5	The Locomotive Engineer and the Brakeman on Conrail train ENS-121 failed to observe the “approach” signal aspect at the distant signal on track 1. The locomotive engineer claimed that the wayside signal displayed an ‘approach limited’ aspect [this would imply that the switch was aligned from track 1 to track 2 which was not the case.] The brakeman said that he was standing up and was preparing his lunch. As a result, he said he did not observe any of the wayside signals approaching Gunpow. He said that he observed an ‘approach medium’ aspect on the ACS. [This would mean that the switch was aligned from track 1 to track 2, which was not the case.] The fact that the Conrail crew testified that they saw signals that in fact they could not have seen (The TSB verified that the signals were functioning properly), suggests that their expectations were that the switch would be aligned to allow them to switch to track 2 might have influenced them. The fact that the ‘approach’ light bulb was missing on the ACS and that the cab

UNSAFE ACTIONS AND OTHER EVENTS

ID	Description
	signal alerter whistle was suppressed, meant that these redundant ‘safety net’ cues were not available.
U6	The locomotive Engineer and the Brakeman on Conrail train ENS-121 failed to observe (or were delayed in observing) the ‘stop’ signal aspect on the home signal on track 1.
	Subsequent tests indicated that the crew should have been able to see the ‘stop’ aspect for wayside signal 1N when they were still more than 5,000 feet south of it. This was sufficient distance to stop even without using emergency braking. The safety board concluded that the crewmembers were not looking ahead to see signal 1N.
E1, E2	The ACA aspect should have changed to ‘restricting’, and should have caused the alerter whistle to sound. However, the whistle had been suppressed.
	A restricting ACS aspect required the crew to reduce speed to at least 20 mph.
U7	1:29.24 PM, EST Conrail train ENS-121 entered switch 12 at Gunpow and moved onto track 2. The train was going at 64 mph. The safety board believed the engineer applied the emergency brakes when it was less than 2,000 ft from signal 1 N. Had the train been traveling at 55 mph or less, it would have stopped short of the turnout.

HUMAN DEPENDENCIES

IDs	Dependency Mechanism	Description
U2, U4	Organizational pressures to maintain schedule	Both Conrail ENS-121 and Amtrak 94 were exceeding their applicable speed limits;
U2, U4	Multiple, conflicting rules leading to ambiguity in interpretation	There were disagreements as to whether Conrail ENS-121 was going above its applicable speed limit; and disagreement as to whether the Dispatcher should have been informed that Amtrak 94 had a heritage car that required it to go at a slower speed.
U5, U6	Mutual distraction	Neither the Locomotive Engineer nor the brakeman on Conrail ENS-121 observed the restricted signal aspects, possibly because they were distracted (it was reported that they were conversing at the time, and that the brakeman was preparing lunch.
U5, U6	Distraction/inattention	The brakeman reported that he was not monitoring either the wayside signals nor the In cab signals because he was standing up preparing his lunch.

EVENT DIAGNOSIS LOG

Time	Accident Progression & Symptoms	Response
	Train ENS-121 passes distant wayside signal. Signal aspect was “approach”	No action taken. Locomotive engineer failed to recognize the “approach” signal. Under sworn testimony stated that the aspect was “approach limited’, but the TSB established that this could not have been the case.
	Train ENS-121 passes	No action taken. Locomotive engineer failed to recognize the signal
	Train ENS-121 passes home signal. Signal aspect was “stop”	Locomotive engineer indicated that he observed the “stop” aspect, although he was unable to estimate how far he was from the signal when he observed it. He immediately placed the train in emergency brake. The train was traveling at about 64 mph. It did not stoop short of the home signal but ran through switch 12, which was 349 feet beyond the home signal.
	Train 94 passes home signal. Signal aspect switched to ‘stop’ when ENS-121 entered switch 12.	Train 94 locomotive engineer puts train into emergency braking

Event Analysis: Collision at Shady Grove Station, Gaithersburg, MD.

Type of Accident: Collision

Date and time: January 6, 1996, 10:40 pm EST

Location: Shady Grove passenger station, Gaithersburg, Maryland.

Railroad: Washington Metropolitan Area Transit Authority (WMATA)

Fatalities/injuries: 1/0

Other losses: $2.1-2.6 million

Data sources: NTSB/RAR-96/04 railroad accident report

Data entry by: Jordan Multer

Event Summary

Event description: About 10:40 p.m. on January 6, 1996, Washington Metropolitan Area Transit Authority (WMATA) Metrorail subway train No. T-111, operating on the “Red Line” segment of the Metrorail system, failed to stop as it entered the aboveground Shady Grove passenger station near Gaithersburg, Maryland, the final station on the Red Line. The four-car train ran by the station platform and continued about 470 feet into the Metrorail yard north of the station, where it struck a standing, unoccupied subway train (a 6-car “gap” train1) that was awaiting assignment. The train operator was fatally injured; the two passengers on the train were uninjured.

Event surprises: Snow on the tracks causes several train to slip and overshoot the Rockville station stop. Because the train was partially off the platform, its doors would not automatically open. The controller instructed the train operator to “drop [open] the left and right breakers” (to keep the doors from opening on the first car) and to service the station off the second, third, and fourth cars.

When train T-111 entered the Rockville station (the station just before Shady Grove), the main train control system electronically transmitted to it the performance level 3 that was in effect for that station and that would have limited train T-111’s top speed over the 2.68-mile route segment between the Rockville and Shady Grove stations to 59 mph, with a normal rate of acceleration. This performance level transmission was suspended while the train serviced the station. When the train finished servicing the station, the performance level was reestablished. But because the lead car of the train was outside the station limits, performance level 3 was lost and the train’s speed control system defaulted to performance level 1 as the train departed the station. Performance level 1 was the highest (fastest) performance level. The lead car had to be within the station limits for the performance level to be reestablished at the level set by the controller.

FRA/Railroad responses: WMATA: Instituted policy that gap trains be stored on the track opposite the one normally used for trains arriving on mainline and as deep as possible in the tail track. Instituted new policy making passenger safety the responsibility of every WMATA employee. Train Operator is authorized to stop the train if instructed to take any action that would adversely affect passenger safety. This policy also put in place a maximum speed of 49 mph during inclement weather. WMATA began new training procedures for the controller.

WMATA discontinued the use of oral instructions to operations control staff. Written instructions were to be used when rule changes were made.

NTSB recommendations: Analyze braking performance under low adhesion conditions; Take measures necessary to ensure compatibility between cars braking performance and automatic train control system design; Discontinue the use of non-vital and non-fail-safe automatic train supervision subsystem to perform safety critical functions; Make it impossible to default to higher speed conditions when a lower speed condition is required for safety; Establish management controls to ensure changes to railroad operations are properly evaluated; Establish, document and enforce a maximum authorized speed for every segment on operating system; Develop a rule government placement of standby (gap) trains; Implement procedures for active monitoring of both automated control system and train operation; permit manual intervention when potential automated system failures are recognized; Include unambiguous guidelines for recognizing emergency situations that require the train to stop; Discontinue the practice of oral instructions to convey standard operating procedures; Implement procedures to ensure that operating personnel receive all bulletins, special orders or notices about their responsibilities.

Event Characterization

Deviations from expected conditions: Margin of safety for track ATC block design (based upon availability of 75 percent of full service braking) was inadequate to assure safe operation. Train 111 overshot Rockville station stop preventing it from properly picking up information from automated train control subsystem. System defaulted to least restrictive level instead of most restrictive condition.

Any key mismatches between rules/instructions and performance: Standby (gap) train was positioned on same track as incoming trains in violation of verbal instructions to place them on opposite track.

Instructions to place standby trains on track opposite incoming trains was routinely violated.

Most negative influences: A non-vital and non-fail-safe subsystem was called upon to provide a safety-critical function.

WMATA management failed to comply with its own established formal rules for making changes to operating procedures. They used oral instructions and notices instead “special orders” or other document appropriate to rule changes. Normal checks and balances were absent.

Most, important Metrorail policies and operating procedures were derived from rigid, top-down, highly centralized management processes. Metrorail engineering personnel had access to information regarding the incompatibility between the ATC block design and the stopping profile of trains in inclement weather, but this information was not sought out or considered during the decision making process.

Most positive influences: None identified (?)

Key Work Mode Transition Issues

Mode changes:

Transfer of control: Rule change removes discretion from train operator to change from automatic to manual train operation, except in emergency.

Shifts in authority:

Skill loss:

Coming up to speed:

Primary/backup reversion: None

Fixation: End of journey?

Significance of Event:

Extreme or unusual conditions: Snow on track contributed to low adhesion.

Contributing pre-existing conditions: Margin of safety for Track ATC block design (based upon availability of 75 percent of full service braking) was inadequate to assure safe operation.

Incompatibility between braking requirements of ATC block design and braking capabilities of rail cars was masked by WMATA of operating trains manually in inclement weather (latent condition).

Opening the car doors caused the train to temporarily lose the assigned performance level (speed limit). With the train outside the station limits, the train could receive the signal for reduced speed due its location in the station.

Misleading or wrong information: Management perception that wheel flats were caused by manual operation resulted in rule change preventing manual operation, except in emergency situations. The perception resulted in rule change preventing manual train operation except in emergencies.

Information rejected or ignored: In the half hour preceding the accident, controllers had asked for and been denied permission to permit train operators to change to manual mode. These requests came after trains had reported overrunning stations because of slippery rails. But the controllers did not make this request specifically with respect to train T-111, even though that train presented them with a safety hazard that was far more serious and more immediate than any they had faced since their shift began. The controllers apparently were not able to diagnose the problem as one that required more than adherence to standard operating procedures.

Multiple hardware failures: None reported

Transitions in progress: none:

Similar to other events:

KEY PARAMETER STATUS

Initial Conditions	Accident Conditions
Snow began falling at 9:10 pm. Train operations were normal until controllers began receiving reports of trains overrunning station platforms because of slippery tracks. Train T-111 had no problem servicing the first 21 of 23 stations.	The controller received a report from train operator of T-110 of a station overrun at the Twinbrook station. The controller entered the most restrictive performance level in the automation for outbound trains heading toward Rockville. Train T-111 reports overrunning Twinbrook station.

TRAIN/PROCESS STATUS

Initial Plant Conditions & Configurations	Accident Conditions & Consequences
Configuration: The train consisted of four cars operating under mode 1 (automatic train operation). **Noteworthy Pre-existing Conditions**: Incompatibility between braking requirements of ATC block design and braking capabilities of rail cars was masked by WMATA of operating trains manually in inclement weather (latent condition). **Initiator**: The operator of train T-111 overran the Rockville station platform by one car.	**Automatic Responses**: Automation was braking at the time of the accident. Speed was set at default (highest speed setting) at time of accident. **Failures**: Automation was unable to stop the train in time to avoid collision. Automation was never able to brake to a safe stop under the low adhesion conditions and the high speed at which the train was moving.

Action Summary

Event Timeline:

Key: U = unsafe actions
E = equipment failures (significant to the event)
H = non-error (non-recovery) actions
R = recovery actions
V = event of interest

Pre-Initiator

V1: 10:18 pm: The operator of the train (T-110) preceding the accident train (T-111) reported overrunning the station platform at Twinbrook to the controller due to slippery tracks.

H1: 10:22 pm: The button controller entered the most restrictive performance level (maximum speed of 49 mph) servicing trains from Twinbrook to Shady Grove.

V2: 10:27 pm. Train T-111 reports to radio controller that train overran station platform at Twinbrook by all 4 cars. He was instructed by the radio controller not to service the Twinbrook station and continue to the Rockville station.

Initiator

H2: 10:31:55 p.m. The operator of train T-111 called the Red Line controller to report that he had overrun the Rockville station platform by 1 car.

V3: When train T-111 entered the Rockville station, the automatic train control system electronically transmitted a signal that was in effect for that station (the most restrictive) that would limit the train's top speed between Rockville and Shady Grove.

This signal was suspended while the train serviced Rockville station. Because the train had overrun the platform, the train doors would not open automatically. The controller instructed the train operator to override this protective system and open the doors only for the second, third, and fourth cars.

Because the train's lead car was beyond the station platform, the signal establishing the most restrictive performance level was not reestablished after the signal was lost. The performance level defaulted to the highest, least restrictive state.

H3: 10:35 pm: The train operator reported to the radio controller the console speed readouts of 75 limiting and 75 regulated. (Actual speed was later calculated as 45 mph).

H4: 10:36 pm: The train operator called the radio controller again and reported that his actual speed had reached 75 mph.

H5: 10:37 pm: The radio controller called the train operator to see if train speed had dropped. The train operator answered that it's down to 35 limited and 35 regulated. Actual speed was later determined to be in excess of 50 mph.

H6: 10:40 pm: The Shady Grove terminal supervisor reported to the controller that a collision had occurred between train T-111 and a gap train.

UNSAFE ACTIONS AND OTHER EVENTS

ID	Description
U1	Management institutes policy preventing use of manual operation except in emergency
U2	The train operator reported to the radio controller the console speed readouts of 75 limiting and 75 regulated. (Actual speed was later calculated as 45 mph). Train operator fails to recognize the hazardous situation and request change to manual operation.
U3	Controller fails to recognize level of hazard as train approaches Shady Grove and recommend manual operation by train operator

HUMAN DEPENDENCIES

IDs	Dependency Mechanism	Description
1	Mode change	Change from automatic to manual operation required permission from controller. Train operator unaware that of instructions to controller that manual operation could only be enabled in emergency situation.
2	Experience	Train operator has 2 months experience as train operator.
3	Communications	Although experienced controllers were aware that when trains overrun station platform they often lose the correct performance level, they did discuss this issue after learning that the train received a speed of 75 mph.

EVENT DIAGNOSIS LOG

Time	Accident Progression & Symptoms	Response
10:27 pm	Train operator reports completely overrunning Twinbrook station platform to radio controller.	Controller requests train operator continue to next station (Rockville)
10:31 pm	Train overruns Rockville station platform by 1 car	Controller requests train operator service station by disabling automatic door operation and opening doors of cars in station.
10:35 pm	Train operator reports to controller that console speed displays show 75 mph	No action taken.
10:36 pm	Train operator reports to controller again that console speed displays show 75 mph	No action taken.
10:37 pm	Controller asks train operator speed has dropped	Train operator reports that speed console displays 35 mph.
10:40 pm	Shady Grove terminal supervisor reports collision to controller	Superintendent and general manager depart for accident scene.

Event Analysis: DERAILMENT AT CAJON, CALIFORNIA

Type of Accident: Derailment

Date: 2/1/96

Location: Cajon, CA, MP 60.5, FRA Region 7

Railroad: The Atchison, Topeka Santa Fe Railway Co. (ATSF)

Train:

Kind of Train	Train ID	Time-table Direction	Number Locos	Number Cars	Number Loads	Number Empties	Train Length Feet	Train Tonnage	Speed Nearing Accident	Speed at Accident
Freight	HBALT1-131	West	4	49	45	4	2,975	5,025	58	60

Crew:

Crew	Hours on Duty	7.1.1.1.1 Years Experience
Engineer	4h 20m	1-2 years: hired 1991, promoted to engineer 1994; 300+ runs down Cajon
Conductor	4h 20m	0-2 years: hired 1992, promoted to engineer 1994
Brakeman	4h 20m	0-1 years: hired as switchman 1993, promoted to conductor 1995

Method of Operations: time table, double track (south track), special instruction, traffic control system speed passenger 30/freight 20 mph

Fatalities/injuries/Other losses:

Number Casualties			Number Derailed		Locos Damaged			Cars Damaged		
Fatal	Serious	Minor	Locos	Cars	Destroyed	Substantial	Minor	Destroyed	Substantial	Minor
2	1		4	45	3	1		45		

Other consequences:

- Evacuation of 50 people; I-15 closed for several days
- Explosion and fire, escape of HAZMAT (4 of 5 HAZMAT cars breached – 3 with petroleum distillates, denatured alcohol, and trimethyl phosphate respectively burned completely, one with pressurized butylacrylate exploded releasing 1700 gal. to soil, with remained of contained product trucked out
- Property damage about $4 million

Consequence Summary:

Consequence Category	I	II	III	IV	V
PD –property damage CI – community impact	PD<$20,000	PD>$20,000 OR injuries OR CI	PD2 AND [injuries OR CI]	Death	Death AND [PD2 OR CI]

This event (check box)					*7.1.1.2 X*

Data sources (FRA, NTSB, railroad): FRA Accident Investigation file:

- Factual Railroad Accident Report – Accident Investigation No. B1-96
- Railroad Report No. ATSF 11-0296-100
- Transcript of Lester Foster (engineer during accident) interviewed by LA District Attorney 2/1/96 4:55 pm at hospital, whose focus was on whether vandals could have disabled brakes; Mr. Foster provides significant information about the state of the ETD and his assumptions
- Transcript of Lester Foster (engineer during accident) interviewed by Mr. Seipler 2/3/96
- Meeting notes from meeting with California Lt-Gov 2/6/96
    - FRA Proposal: Cojon Pass Accident Response Plan (For Internal FRA Use Only) – Attachment A to above meeting notes
- FRA Emergency Order No. 18 [4910-06]
    - Also published in Fed Reg V 61 No. 28 2/9/96
- FRA Emergency Order No. 28 [4910-06] [not sure it's related to accident, but is in file]
- The Atchison, Topeka and Sante Fe Railway Co. System Timetable No. 5 in effect at 12:01 A.M. Sunday, April 16,1995
- The Atchison, Topeka and Sante Fe Railway System General Orders 1995 – describes operation and testing of ETD
- Additional transcripts: maintenance worker for car added, conversations between crew and dispatcher
- Photographs of accident
- Newspaper accounts of accident
- Many additional documents were available, but were not informative for our purposes
- Floppy disk "REG. 3 ACCIDENT H.Q.0301"

Data entry/interpretation by: Dennis C. Bley

Event summary

Event description**:**

Train HBALT1-31 was westbound out of Barstow. The brakes were "successfully" tested (see description of events H_1, H_2, H_3, U_1, and U_2 on the timeline below) in Barstow. A carman near the 16th car observed the brakes set and release on that car during the full service brake and heard the emergency brake application. It was 47°F, dark and clear.

After a delay of 4 hours because of a mudslide in the Cajon Subdivision, the crew returned at 11:45 p.m. on January 31, 1996. Their van driver observed the conductor push a button on the ETD and manipulate the angle cock on the rear car, before taking him to the loco. The engineer released brakes and ATSF 157 West departed Barstow Yard at 1:17 a.m. The train stopped at Hodge (MP36.7) using auto air brakes (event recorder). Next stopped at Victorville (MP 36.7) using air brakes and engineer considered that he had complied with the timetable instructions that required him to make a "running" air brake test and felt the brakes had operated properly. Next the train stopped at Summit (MP 55.9) at about 3:34 a.m. using at least a 10-psi brake pipe reduction, waiting for a signal.

At 3:30 a.m. the engineer released the brakes and allowed the brake pipe to charge with air for 6.5 minutes to 86 psi and departed Summit. From Summit to Cajon, the track descends westbound, with grades ranging from 3.4 to 2.2 percent and a succession of 13 L/R curves, of 2-8 degrees, up to 1/2 mile each. As the train crested the mountain and began to descend, the engineer applied the dynamic brakes "bunching" his train toward the locos. He also made the first service application of the air brakes, a set of 5-8 psi, observing the DTD pressure reduce to 81 psi. As he noticed the train picking up speed, he made additional application of the brakes, *but the ETD did not show any reduction*. As the train reached 15-18 mph, he made a full service brake application and the ETD showed no reduction. The conductor, who was a promoted engineer, told the engineer to wait a minute "they're going to set up." The engineer waited until 25 mph and made an emergency application of the train air brakes, but the ETD still indicated 81 psi.

As the train reached 45 mph, the engineer told the dispatcher that ATSF 157 West was in emergency, but was not stopping, and to warn all traffic ahead of the situation. At this point the engineer noted that the conductor and brakeman stood to the left of him, looking at him as if to say are you coming. The conductor and brakeman then proceeded down the steps to the door leading to the front platform of the loco. As they exited the cab, the engineer felt the wind coming through the front door.

At 4:09 am the engineer released the air brakes and at 4:09.27 am he reapplied them, at 4:09.34 a.m. he tried reversing the loco wheel rotation. The loco began to tile and at about 4:10 A.M the train derailed of a left hand curve at MP 60.5, falling to a dry creek bed. The lead loc, ATSF 157 came to rest on its right side, 13 minutes, 20 seconds after leaving Summit. The engineer crawled out of the fireman's window. The grade was 3 percent at the point of derailment.

Insufficient braking forces allowed the speed of the train to increase. A blockage in the train line (air brake system) occurred which prevented proper application of the air brakes from the point of the blockage rearward. Due to the massive destruction, the exact point of blockage could not be determined. Simulation analysis indicated that, with three or more working loco dynamic brakes and 16 cars breaking, the train would have either stopped or negotiated the fatal curve. The blockage most likely occurred between the 4th and 8th cars (not accounting for possible brake fade in the analysis).

The 16th car ATSF 90033 was the only car added at Barstow; it had been "bad ordered" and repaired at the Barstow Car Facility for a *crimped air brake pipe*. The investigation focused on the possibility that the car may have developed a kinked air brake hose or a crimped air brake pipe when the train was bunched. On the 5th day of the investigation, about 60 percent of the car was dug out and examined. The cushioning unit (to protect the air hose from train movement) was burned but still inside the sill.

Crew Experience:

Engineer: hired 1991, promoted to engineer 1994; guesses he made 300 trips down Cajon in testimony; he's had other brake problems in the past with "brake valves that have a failure on them but what was unusual about this one I couldn't get a reset on it." It gets a little garbled here, as if the details on brake function are not well ingrained. Also some confusion about indications of a closed angle cock and the need for an armed ETD. Sounds like DA is looking for a trespasser shutting an angle valve – a problem they seem to have in LA.

Conductor: hired 1992, promoted to engineer 1994

Brakeman: hired as switchman 1993, promoted to conductor 1995

Additional notes:

Second interview with engineer on 2/3/96 added some info:

A. …[ETD] wouldn't arm. Com test failure is all I kept getting out of it. It wouldn't arm…

Q. Did you talk to the carman at the end of the train about arming the –

A. I told him…He says okay, you know…Most generally, 90 percent of the time when you get a com test failure, they won't arm.

This transcript provides a good layout of the run. It must be the source of much of the report. Some real heroics on part of engineer to try everything he could to slow the train – some based on stories from previous runaway.

FRA Memorandum July 16, 1996 describes another Cajon runaway – reached 51 mph. This one stopped 5 miles after application of emergency brakes. Conductor said dynamic brakes on three trailing locos did not work; however, analog readout of 2nd loco indicated it was working. Other readouts indicated crew was micro sleeping as speed increased (disagreed with crew statements). Significant discipline accepted.

Event surprises:

- Despite potential consequences of brake failure and single failure nature of air brake common-cause failure:
  - Engineer willing to trust his life and others to a single point of application (typical bias based on insufficient experience?)
  - Carman willing to "assume" on issue affecting others' lives
  - Given LA DA's concern with vandalism, valving out brake pipe must be fairly common; threat not understood by crew?
- Railroad had no rules on testing/operating with/without ETD; i.e., they de facto approve of run with no ETD; FRA too (see below) [although railroads, FRA and unions may have "assumed" self-preservation would be strong enough influence to avoid such operation
  - FRA/Railroad responses: The Sacramento Bee 2/7/96 (from FRA file) reports: The Federal Railroad Administration …issued an emergency order requiring trains like the one that derailed near here Thursday to be equipped with extra braking devices…in working order…that permit an engineer at the front of a train to apply the brakes at the rear of the train, even if there is a blockage in the air brake line…

Event characterization

Deviations from expected conditions: Failed safety hardware not tested or reset before steep descent with many switchbacks

Any key mismatches between rules/instructions and performance: mental model of making run without ETD based on “small” number of descents and discounting of other brake failure events in experience

Most negative influences: Reliance on rules that did not require operable ETD

Most positive influences: Attention during descent; caught problem early on and attempted to slow train

Key Work Mode Transition Issues

Mode changes: N/A

Transfer of control: N/A

Shifts in authority: Both engineer and carman appeared to have relied on other’s judgment

Skill loss: N/A

Coming up to speed: N/A

Primary/backup reversion: N/A

Fixation: Rules. Not required to test or restore ETD

Significance of Event:

Extreme or unusual conditions: None

Contributing pre-existing conditions: ETD tripped

Misleading or wrong information: None

Information rejected or ignored: ETD tripped leaving a single point for application of air brakes

Multiple hardware failures: None

Transitions in progress: Long steep descent

Similar to other events: From report there have been many occasions with air pipe blockage and mountain runaways; we have not reviewed these.

KEY PARAMETER STATUS

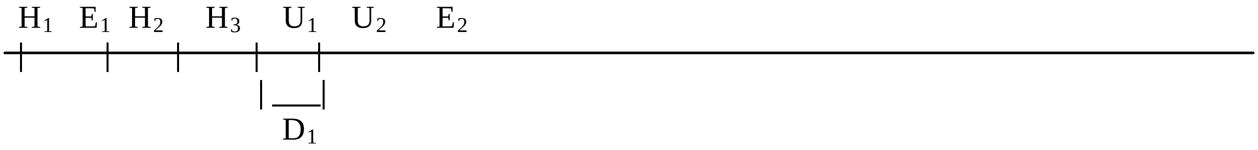
INITIAL CONDITIONS	ACCIDENT CONDITIONS
ETD tripped	Dynamic braking successful, air brakes partial failure.

TRAIN/PROCESS STATUS

Initial Plant Conditions & Configurations	Accident Conditions & Consequences
Configuration: About to begin descent from Cajon Pass **Noteworthy Pre-existing Conditions**: ETD device tripped; known to engineer	**Automatic Responses**: **Failures**: When air pipe blockage occurred, inability to dump air pressure from end of train due to tripped ETD permitted runaway and eventual crash
Initiator: Blockage in air pipe allowed brake application in only the first 4-7 cars	

Action Summary

Event Timeline:



<u>Unsafe Actions and Other Events</u>:

Key: U = unsafe actions

E = equipment failures (significant to the event)

H = non-error (non-recovery) actions

R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS

ID	Description
H_1	After crew coupled locomotive consist to west-most car on track, a carman applied a "blue flag" on the control console of the lead locomotive and informed the crew that the car department needed to inspect and test airbrakes on ATST-90033 (crew waited for this car to be added as 16th car to train. Test done in conjunction with initial terminal air brake test.
H_2	Engineer performed initial terminal air brake test with assistance of carman at east end of train. After train line fully charged with 86 psi air, engineer applied full service brake by reducing train line air pressure by 20 psi – engineer observed head-end-device (HED) indicated reading on end of train device (ETD) had decreased accordingly. Engineer waited about 1 minute and performed leakage test (1.5-2 psi/minute). Engineer then released train air brakes and reading at rear of train by ETD-86 psi. When carman arrived at rear of train, the brakes on last car were already applied. He radioed for engineer to release brakes and when released, he radioed "hi ball" (test ok).
H_3	Engineer informed carman at rear of train that he intended to apply emergency brake (required by ATST operating rules). Initiated application from auto brake valve on locomotive and the brakes applied. He released brakes and pressure returned to 86 psi on ETD. When engineer requested emergency brake test, carman stayed. He did not observe ETD to see if air pressure showed on device. He did look at brake cylinder piston on last car to determine when brakes set and released.
U_1	End of Train Device (ETD) not tested when air brakes tested by carman: The brakes were already applied for the full service test when he arrived at the end of the train and, because ETD tests are normally done before the brakes tests are started, he assumed that the ETD test had been completed. The carman said that the engineer did not request a test of the 2-way feature on the ETD.
U_2	Engineer did not request test of ETD, although he knew it was tripped: From engineer's testimony, he tested his ETD at Barstow: "Com-test tells me that it was not on." He only reported it to the carman. (Note: the transcript is full of jargon.) It says that the carman asked if he was going to arm the ETD and the engineer said "no, because it's a high com-test and fire and it will arm." The gist of it seems to be that he didn't and wouldn't usually report the com-test failure to dispatch or anyone else; he said that the carman "never asked me at the rear of the train to try and rearm …it; and that it is *normal procedure to take the train down Cajon with the ETD not armed* and that the rail company knows that. He can "take it as a marker" i.e., "that's a flasher on the rear of the train where the train flashes. As long as I've got a reading, an ETD reading of the air pressure at the rear of the train the ETD is working at the rear and giving me a reading up here of what the real air pressure of the train is. So that part is working. So we did an air emergency brake test. The whole train went into emergency at the Barstow yard before I left."

HUMAN DEPENDENCIES

ID	Dependency Mechanism	Description
D_1	Both individuals ***assumed*** that the other would cover the situation	

ACCIDENT DIAGNOSIS LOG

Time	Accident Progression & Symptoms	Response
	Engineer recognized that ETD was tripped	
1:17 am	Engineer tested air brakes, but did not test ETD	Carman assumed that engineer had already tested ETD
3:30 am	Began run down west side of Cahon Pass	
	Train failed to respond properly	Engineer made multiple attempts to slow train
4:09 am	Recognized runaway conditions	Reported to dispatcher; conductor and brakeman exited engine; probably jumped to deaths

REFERENCES

Askey, Shumei. (1995). "Design and Evaluation of Decision Aids for Control of High-Speed Trains: Experiments and Model." Ph.D. thesis, MIT. Cambridge, MA.

Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. (2003). *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823, prepared by Sandia National Laboratories. U.S. Nuclear Regulatory Commission, Washington, DC.

Barriere, M.; Bley, D.; Cooper, S.; Forester, J.; Kolaczkowski, A.; Luckas, W.; Parry, G.; Ramey-Smith, A.; Thompson, C.; Whitehead, D.; and Wreathall, J. (2000). "Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)." NUREG-1624, Revision 1, U.S. Nuclear Regulatory Commission.

Billings, C.E. (1996). Aviation Automation: The Search for a Human-Centered Approach. Erlbaum, Hillsdale, NJ.

Bley, D.C.; Kaplan, S.; and Johnson, D.H. (1992). "The Strengths and Limitations of PSA: Where We Stand." *Reliability Engineering and Systems Safety*, Volume 38.

Bley, D.C.; Droppo, Jr., J.G.; and Eremenko, V.A.; eds. (2002). *Risk Methodologies for Technological Legacies*. NATO Science Series, Kluwer Publishers.

Boyack, B.E.; Catton, I.; Duffey, R.B.; Griffith, P.; Katsma, K.R.; Lellouche, G.S.; Levy, S.; Rohatgi, U.S.; Wilson G.E.; Wulff, W.; Zuber, N. "An Overview of the Code Scaling, Applicability, and Uncertainty Evaluation Methodology." Nuclear Engineering and Design, Volume 119, pp. 1-16, 1990.

Budnitz, R.J.; Apostolakis, G.; Boore, D.M.; Cluff, L.S.; Coppersmith, K.J.; Cornell, C.A.; and Morris, P.A. (1997). "Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts." NUREG/CR-6372, U.S. Nuclear Regulatory Commission, Washington, DC.

Center for Chemical Process Safety (CCPS). *(*2001). *Layer of Protection Analysis: Simplified Process Risk Assessment*. Wiley, New York, NY.

Christoffsen, K., and Woods, D.D. (in press). "How to Make Automated Systems Team Players." Advances in Human Performance and Cognitive Engineering Research. E. Salas, ed. Volume 2. JAI Press/Elsevier.

Cullen, W.D. (2000). The Ladbroke Grove Rail Inquiry. HSE Books, Norwich, UK.

Dekker, S. (2002). *The Field Guide to Human Error Investigations*. Ashgate, Burlington, VT.

Department of Transportation (2001). *49 CFR Part 209 Standards for Development and Use of Processor-Based Signal and Train Control Systems*. Proposed Rule (Federal Railroad Administration). Federal Register 66 (155), Friday, August 10, 2001.

Einhorn, J.; Sheridan, T.B.; and Multer, J. (2005). *Preview Information in Cab Displays for High-Speed Locomotives.* Report No. DOT/FRA/ORD-04/12. U.S. Department of Transportation, Federal Railroad Administration, Washington, DC.

Forester, J. A.; Bley, D.C.; Cooper, S.; Kolaczkowski, A.M.; Thompson, C.; Ramey-Smith, A.; and Wreathall, J. (2000). *A Description of the Revised ATHEANA (A Technique for Human Event Analysis)*. PSAM 5, International Conference on Probabilistic Safety Assessment and Management, Osaka (JP), 11/27/2000–12/01/2000. www.osti.gov/dublincore/ecd/servlets/purl/761062-ox05wq/webviewable.

Health & Safety Executive (HSE). (2000). *The Train Collision at Ladbroke Grove 5 October 1999*. HSE Books, Norwich (UK).

Hobbs, A. (1999). *Maintenance Mistakes and System Solutions*. Asia-Pacific Air Safety, 2-7.

Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method*: CREAM. Elsevier, New York.

Kletz, T. (1995). *Computer Control and Human Error*. Gulf Publishing Company, Houston, TX.

Kuehn, G. (1992). *Advanced Train Control System Evaluation: Final Report.* Report No. FRA/ORD-92/32. U.S. Department of Transportation, Federal Railroad Administration, Washington, DC.

Moray, N. (2000). Are Observers Ever Really Complacent When Monitoring Automated Systems? *Proceedings of the IAE 2000/HFES 2000 Congress*.

Multer, J.; Rudich, R.; and Yearwood, K. (1998). Human Factors Guidelines for Locomotive Cabs. Report No. DOT/FRA/ORD-98/03. U.S. Department of Transportation, Federal Railroad Administration, Washington, DC.

Nielsen, J. (1994). *Usability Engineering*. Morgan Kaufmann, San Francisco, CA.

National Transportation Safety Board. (2001). *Most Wanted Transportation Safety Improvements Safety Recommendation.* R-01-6 Implement Positive Train Control Systems. Federal Railroad Adminstration, Washington, DC. http://www.ntsb.gov/Recs/mostwanted/positive_train.htm.

National Transportation Safety Board. (2002). “Positive Train Control Preventable Collisions.” Document No. WG-May-73. NTSB Office of Railroad, Pipeline, and Hazardous Materials Investigations, Railroad Division, Washington, DC.

National Transportation Safety Board. (1996). “Collision of Washington Metropolitan Area Transit Authority Train T-1 11 with Standing Train at Shady Grove Passenger Station, Gaithersburg, Maryland.” Railroad Accident Report No. NTSB/RAR-96/04. Washington, DC.

Norman, D.A. (1990). The ‘Problem’ of Automation: Inappropriate Feedback and Interaction, Not ‘Over-Automation.’ Philosophical Transactions of the Royal Society of London, B 327:585-593.

Parasuraman, R. and Riley, V.A. (1997). Humans and Automation: Use, Misuse, Disuse and Abuse. *Human Factors*, 39, 230-253.

Patterson, E.; Cook, R.; and Render, M. (2002). Improving Patient Safety by Identifying Side Effects from Introducing Bar Coding in Medication Administration. *Journal of the American Medical Informatics Association*, 9, 540-553.

Reason, J. (1990). *Human Error*. Cambridge University Press, Cambridge, England.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate, Burlington, VT.

Reason, J. and Hobbs, A. (2003). *Managing Maintenance Error: A Practical Guide*. Ashgate, Burlington, VT.

Roth, E.M.; Malin, J.T.; and Schreckenghost, D.L. (1997). Paradigms for Intelligent Interface Design in *Handbook of Human-Computer Interaction* (2nd edition). M. Helander, T. Landauer & P. Prabhu (eds.). North-Holland, Amsterdam, pp. 1177-1201.

Roth, E.M.; Patterson, E.S.; and Mumaw, R.J. (2002). Cognitive Engineering: Issues in User-Centered System Design in *Encyclopedia of Software Engineering*, 2nd Edition. J. J. Marciniak (ed.). Wiley-Interscience, John Wiley & Sons New York, pp. 163-179.

Roth, E.M. and Patterson, E.S. (in press). Using Observational Study as a Tool for Discovery: Uncovering Cognitive and Collaborative Demands and Adaptive Strategies in *How Professionals Make Decisions*. H. Montgomery, R. Lipshits, and B. Brehmer (eds.). Lawrence Erlbaum Associates, Mahwah, NJ.

Sarter, N.B. and Woods, D.D. (1995). How in the World Did We Ever Get into that Mode? Mode Errors and Awareness in Supervisory Control. *Human Factors*, 37, 5-19.

Sheridan, T.B. (2002). *Humans and Automation: System Design and Research Issues*. John Wiley & Sons, Inc., in cooperation with the Human Factors and Ergonomics Society, Santa Monica, CA.

Sheridan, T.B.; Gamst, F.C.; and Harvey, R.A. (1999). Reliance and Distraction Effects in PTC Automation. White Paper STD-PTC-DEC-02-99. John A. Volpe National Transportation Systems Center, Cambridge, MA.

Sklar, A.E. and Sarter, N.B. (1999). Good Vibrations: The Use of Tactile Feedback in Support of Mode Awareness on Advanced Technology Aircraft. *Human Factors*, 41 (4), 543-552.

Strauch, B. (2002). *Investigating Human Error: Incidents, Accidents, and Complex Systems.* Ashgate Publishing Company, Burlington, VT.

Switching Operations Fatality Analysis Working Group. (1999). *Switching Operations Fatality Analysis: Findings and Recommendations of the SOFA Working Group*.

Uff, J. (2000). The Southall Railroad Accident Inquiry Report. HSE Books, Norwich, UK.

Uff, J., and Cullen, W.D. (2001). *The Joint Inquiry into Train Protections Systems*. HSE Books, Norwich, UK.

U.S. Nuclear Regulatory Commission, Division of Research. (2002). *Probabilistic Risk Assessment Branch Research Colloquium*. Annapolis, MD.

Weick, K.E., and Sutcliffe, K.M. (2001). *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. Jossey-Bass, San Francisco, CA.

Woods, D.D., and Christoffersen, K. (2003). *Implications of Positive Train Control for Workload Transitions and Human Performance*. OSU, Columbus, OH.

Woods, D.D.; and Dekker, S.W.A. (2000). Anticipating the Effects of Technological Change: A New Era of Dynamics for Human Factors. *Theoretical Issues in Ergonomic Science*.

Woods, D.D.; Johanssen, L.J.; Cook, R.I.; and Sarter, N.B. (1994). Behind Human Error: Cognitive Systems, Computers and Hindsight. CSERIAC, Dayton, OH.

Woods, D.D., and Sarter, N.B. (2000). Learning from Automation Surprises and Going Sour Accidents. In *Cognitive Engineering in the Aviation Domain*. N. Sarter and R. Amalberti, eds. Erlbaum, Hillsdale, NJ.

Woods, D.D.; Sarter, N.B.; and Billings, C.E. (1997). Automation Surprises. In *Handbook of Human Factors/Ergonomics* (2nd ed.). G. Salvendy, ed. Wiley, New York, NY.

Wreathall, J.; Roth, E.; Bley, D.; and Multer, J. (2003). *Human Reliability Analysis in Support of Risk Assessment for Positive Train Control.* Report No. DOT/FRA/ORD-03/15. U.S. Department of Transportation, Federal Railroad Administration, Washington, DC.

ACRONYMS

ABS	automatic block system
ACS	automatic cab signal
ACSES	advanced speed enforcement system
ART	accident review team
ASES	advanced civil speed enforcement system
ATP	automatic train protection
AWS	automatic warning system
CBTM	communications-based train management
DTC	direct traffic control
EIC	employee in charge
FRA	Federal Railroad Administration
HMI	human-machine interface
HRA	human reliability analysis
HST	high-speed passenger train
IDOT	Illinois Department of Transportation
ITCS	incremental train control system
LDS	location determination system
NAJPTC	North American Joint Positive Train Control
NEC	Northeast Corridor
NJT	New Jersey Transit
NORAC	Northeast Operating Rules Advisory Committee
NTSB	National Transit Safety Board
PPA	positive train control-preventable accident
PRA	probabilistic risk assessment
PRT	personal remote terminal
PSP	product safety plan
PTC	positive train control
RSAC	Railroad Safety Advisory Committee
SES	speed-enforcement system
SPAD	signals passed at danger
TPS	train protection system
WMATA	Washington Metropolitan Area Transit Authority