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

Relative Risk of Workload Transitions in Positive Train Control

Offices of Safety and
Research & Development
Washington, DC 20590

DOT/FRA/ORD-07/12

March 2007
Final Report

This document is available to the U.S. public through the National Technical Information Service, Springfield, VA.

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.

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.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
March 31, 2007

3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE
Relative Risk of Workload Transitions in Positive Train Control

5. FUNDING NUMBERS
DTFR53-00-D-00030
TOPR 012

6. AUTHOR(S)
John Wreathall, David D. Woods, Alan J. Bing, and Klaus Christoffersen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The WreathWood Group
4157 MacDuff Way
Dublin, 43016

The Ohio State University
Dept. of Systems Engineering
Columbus, OH 43210

ICF Consulting
33 Hayden Road
Lexington, MA 02421

ENSCO, Inc.
5400 Port Royal Road
Springfield, VA 22153

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT/FRA/ORD-XX/XX

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Railroad Administration
Office of Research and Development
1120 Vermont Avenue, NW, Mail Stop 20
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT/FRA/ORD-07/12

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)

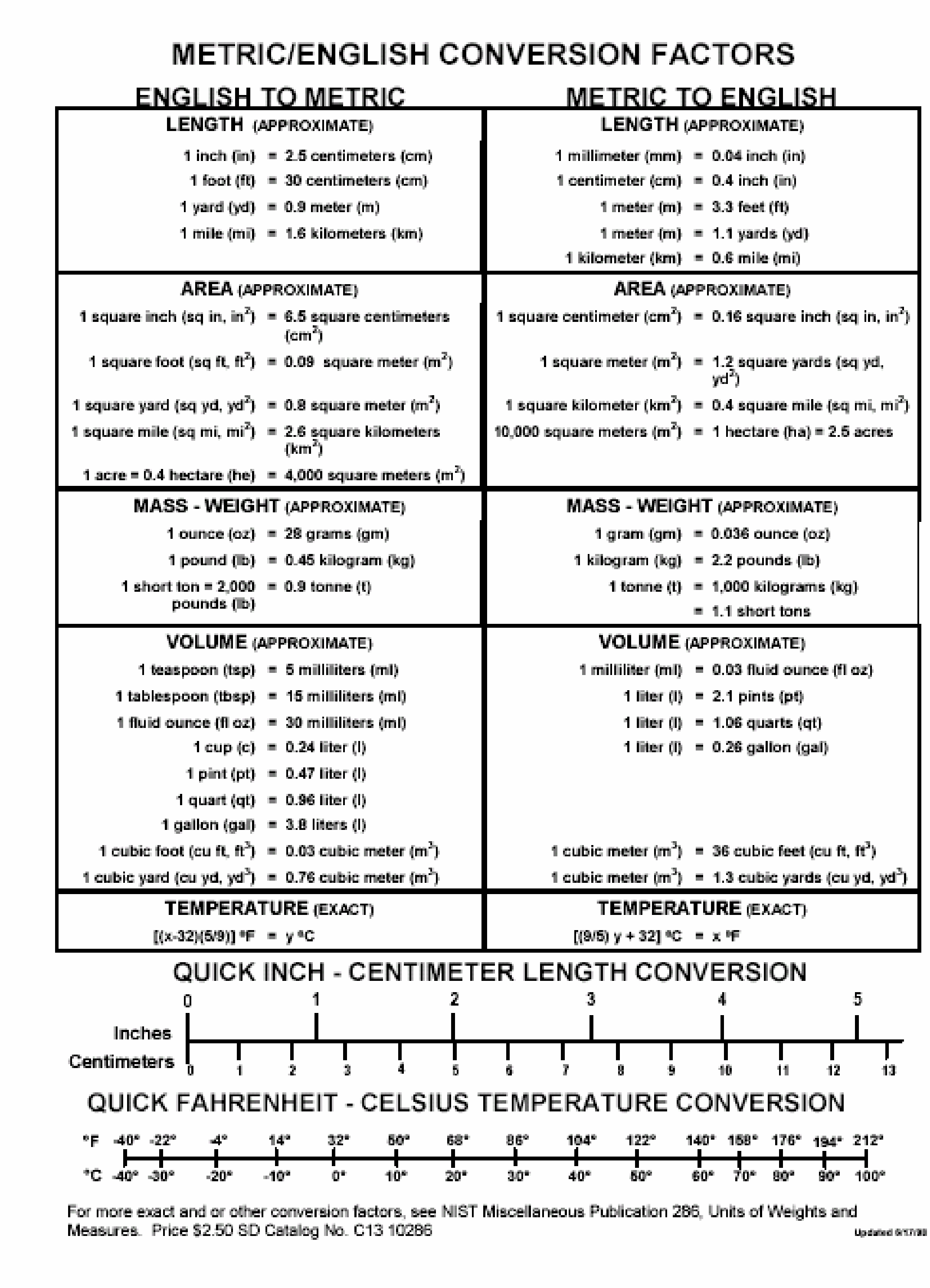
This work proceeded along two parallel paths. First, the research team performed a review and analysis of the fundamental human factors and systems performance issues associated with workload and workmode transitions involving technologies like positive train control (PTC) that can lead to safety and operational problems. These include concerns associated with over-reliance, fixation, skill loss, and shifts in authority between components in the system. Second, the team has examined proposed PTC systems and their intended roles in rail operations to provide an analysis of the risks of the different transitions as they relate to the use of PTC systems in railroading. The opportunities for the high risk failures is greater with PTC systems that provide only an overlay safety function, and are virtually out of sight during normal operations, because the primary risks are associated with the reduction of people's awareness of the system operating state. People tend to rely on protection equipment that is normally functioning and forget when it is inoperative.

14. SUBJECT TERMS
Workload transitions, workmode transitions, positive train control, railroad, train transitions, risk analysis, human reliability

15. NUMBER OF PAGES
62

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited



METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC

LENGTH (APPROXIMATE)

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

AREA (APPROXIMATE)

1 square inch (sq in, in^2)	=	6.5 square centimeters (cm^2)
1 square foot (sq ft, ft^2)	=	0.09 square meter (m^2)
1 square yard (sq yd, yd^2)	=	0.8 square meter (m^2)
1 square mile (sq mi, mi^2)	=	2.6 square kilometers (km^2)
1 acre = 0.4 hectare (he)	=	4,000 square meters (m^2)

MASS - WEIGHT (APPROXIMATE)

1 ounce (oz)	=	28 grams (gm)
1 pound (lb)	=	0.45 kilogram (kg)
1 short ton = 2,000 pounds (lb)	=	0.9 tonne (t)

VOLUME (APPROXIMATE)

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

TEMPERATURE (EXACT)

[(x-32)(5/9)] °F = y °C

METRIC TO ENGLISH

LENGTH (APPROXIMATE)

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

AREA (APPROXIMATE)

1 square centimeter (cm^2)	=	0.16 square inch (sq in, in^2)
1 square meter (m^2)	=	1.2 square yards (sq yd, yd^2)
1 square kilometer (km^2)	=	0.4 square mile (sq mi, mi^2)
10,000 square meters (m^2)	=	1 hectare (ha) = 2.5 acres

MASS - WEIGHT (APPROXIMATE)

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

VOLUME (APPROXIMATE)

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

TEMPERATURE (EXACT)

[(9/5) y + 32] °C = x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION

Inches	0	1	2	3	4	5

Centimeters	0	1	2	3	4	5	6	7	8	9	10	11	12	13

QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSION

°F	-40°	-22°	-4°	14°	32°	50°	68°	86°	104°	122°	140°	158°	176°	194°	212°
°C	-40°	-30°	-20°	-10°	0°	10°	20°	30°	40°	50°	60°	70°	80°	90°	100°

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

Table of Contents

List of Tables

Acknowledgements

The authors express thanks to Dr. Thomas Raslear, Federal Railroad Administration Office of Research and Development, for supporting this work.

Executive Summary

Positive train control (PTC) systems are an area of development in the U.S. railroad industry that is intended to reduce accidents from human errors, such as overspeeding, exceeding limits of authority, and entry to workzones. Such human errors are a frequent contributor to accidents that result in worker fatalities and injuries, significant economic losses to railroads, and, in some cases, harm to the general public.

For the most part, PTC systems work by enforcing penalty brake applications if the engineer fails to comply with the applicable rules listed in the situations above. In many cases the PTC systems function as a backup or overlay system—that is, their interactions with the locomotive crews are minimal when the rules are being complied with, and they only have an effect when one or more rules have been breached, by first warning the engineer and then by applying a penalty brake if compliance with the rule is not achieved within some time limit. Systems differ largely in the technology by which they monitor compliance (from radio- and satellite-communicated data, to onboard databases, to track signals), and a small number play a more active role by providing continuous in-cab displays needed for normal train operations, as in the case of the North American Joint Positive Train Control (NAJPTC) System being developed for application on Amtrak and Union Pacific operations in Illinois.

Previous work in the field of human factors has generally shown that when a new technology is introduced in a workplace, new types of human error can arise because of changes in the ways that work is performed as a result of interacting with the new technology. One new type is known as workload transitions, where the workload of the employee changes significantly at certain times due to the extra demands of interacting with the PTC system. Another new type is known as workmode transitions. In this case, the challenges to the worker come from the need to change the ways of working with the system, rather than simply increasing the amount of work. Both of these types of problems do not occur continuously, but rather they occur at transition points in using the equipment. For example, a workload transition will occur at the start of a journey when the engineer must perform a start-up test of the PTC system. A workmode transition can occur when the engineer must cope with a PTC system that has a more restrictive braking profile, requiring the engineer to initiate braking earlier than would be normal in order to avoid a penalty brake when entering a new speed restriction zone.

In order to explore these and other potential unexpected risks associated with PTC systems, the Federal Railroad Administration (FRA) has supported the project to investigate and evaluate the potential for risks of train accidents from changes to the workload and workmodes of the train crews through use of the PTC systems. This work has proceeded along two parallel paths. First, the research team performed a review and analysis of the fundamental human factors and systems performance issues associated with workload and workmode transitions involving technologies like PTC that can lead to safety and operational problems. These include, for example, concerns associated with over-reliance, fixation, skill loss, and shifts in authority between components in the system. In parallel to this analysis, the team has examined proposed PTC systems and

their intended roles in rail operations, including the features that are salient to workload and workmode issues in operations. Finally, the analysis provides an overview of the kinds of accidents that currently occur from these transitions and how the use of PTC systems may contribute to these kinds of risks.

The risks associated with workload and workmode transitions when using PTC systems can occur in two different conditions: when the PTC system is working normally and when failures in the PTC equipment occur.

When the PTC system is working normally, the dominant risk is the potential for human errors when the locomotive leaves the area covered by the PTC system. The possible failures that can occur include the following:

- *Complacency*, where the train crew has become over-reliant on the protection provided by PTC and simply forget that coverage is no longer being provided.
- *Skill loss*, where the train crew has lost some of the knowledge (speed limits, boundary limits, etc.) that is essential to safe handling of the train as a result of relying on the PTC system.
- *Primary/backup reversal*, where the crew looks to use the PTC system as a normal information system (such as providing current location, indications of speed limits, etc.).
-

When failures in operation of the PTC system are considered, only one scenario creates the possibility of a high risk:

- *Complacency following failures of the onboard equipment*, where the crew, having isolated the system following its failure, now forgets that coverage by the system is no longer available.

Compared with the existing accident rates without PTC operations, these scenarios are likely to be much lower contributions to risks of accidents. Railroads and PTC system designers, however, should be aware that new accident types are possible and that measures in the display designs and the user training can prepare users to avoid the potential for workload- and workmode-related accidents.

1. Introduction

1.1. Background

Organizations in the United States are making considerable efforts to develop PTC systems that are intended to improve the safety of train operations. The primary functions of PTC systems are to enforce railroad operating rules associated with:

- Speed limits (permanent and temporary)
- Enforcement of limits of authorities (signal and dark territories)
- Enforcement of protection of work zones

Some systems provide additional protection against other conditions, such as misaligned switches and broken rails, but the three primary functions are the core functions of PTC systems. These core functions are used in this analysis as the framework of safety that PTC systems are intended to accomplish.

For the most part, PTC systems work by enforcing penalty brake applications if the engineer fails to comply with the types of rules listed above. In many cases, the PTC systems function as a backup or overlay system—that is, their interactions with the locomotive crews are minimal when the rules are being complied with, and they only have an effect when one or more rules have been breached, by first warning the engineer and then by applying a penalty brake if compliance with the rule is not achieved within some time limit. Systems differ largely in the technology by which they monitor compliance (from radio- and satellite-communicated data, to onboard databases, to track signals), and a small number play a more active role by providing continuous in-cab displays needed for normal train operations.

Authors studied the possible human factors and reliability issue associated with one of the PTC systems—the communications-based train management (CBTM) system being developed by CSX—and identified possible issues associated with changes in the way engineers might interact with the PTC systems that are not what the designers intended (Wreathall, Roth, Bley, & Multer, 2003). One example is the issue of over-reliance, where engineers may become reliant on the warning signals generated by the PTC system as a normal basis for acting, thus substituting (rather than adding) the PTC system's judgment about when action is required for the engineers. An independent barrier to the engineer's failure no longer exists (the purpose of the PTC systems), since the engineer is relying on the same system to provide him with a warning, as well as act to stop the train. Failure of the PTC system, in this case, will lead to failure of both the engineer to act and the PTC system to enforce the stop. Others have identified similar issues as a potential concern with PTC systems (see, for example, Sheridan, Gamst, & Harvey, 1999).

1.2. Purpose of This Project

In order to explore this and other potential unexpected risks associated with PTC systems, FRA has supported the project to investigate and evaluate the potential for risks of train accidents from changes to the workload of the train crews through use of the PTC systems. The term workload has been classically applied to the concept of the amount of work (particularly mental work) that a person or team may be called on to perform in a period of time and was the focus of attention in the early 1990s in relation to tasks associated with complex military equipment. The general view associated with human interactions with systems has broadened to that of how new equipment (particularly new human-system technologies like displays and barriers) can change not only the workload but also the ways of working by the users. This is referred to as workmode transitions. The concept of workmode transitions is discussed in more detail.

This work has proceeded along two parallel paths. First, the research team performed a review and analysis of the fundamental human factors and systems performance issues associated with workload and workmode transitions involving technologies like PTC that can lead to safety and operational problems. These include, for example, concerns associated with over-reliance, fixation, skill loss, and shifts in authority between components in the system; Section 2 summarizes this work. In parallel to this analysis, the team examined proposed PTC systems and their intended roles in rail operations; Section 3 provides a perspective on the types of PTC systems being proposed and the features of systems that are salient to workload and workmode issues in railroad operations. Section 4 summarizes accidents that may currently occur from the kinds of transitions being considered. Section 5 provides the analysis concerning the risks of the kinds of transitions as they relate to the use of PTC systems in railroading activities. Section 6 summarizes the analysis.

2. Workload & Workmode Transitions, Automation, and PTC

2.1. Introduction

The concept of workload transitions describes a potential human performance issue of concern in the context of increasing levels of automation in rail operations. Workload transitions refer to the transition from low to high workload experienced by human operators in the wake of unexpected failures or other anomalies. In this work, it has been found necessary to broaden the existing concept of workload transitions to encompass the impacts likely to be seen as a result of introducing PTC into rail operations. This report describes the more inclusive concept of workmode transitions as a more appropriate class of events to examine for rail operations. Workmode transitions result from routine situations (such as movement across different territories) or non-routine situations (such as automation failures) that cause changes in the knowledge, skills, or strategies required to perform effectively. The degree to which a domain is subject to workmode transitions is called its level of heterogeneity. Rail operations are relatively high in their level of heterogeneity.

It is easy to refer to automation as if it were a well-defined and homogenous category of technology. Clearly, however, this is not the case in reality. Automated systems differ on many dimensions that have varying impacts on the nature of performance in the target environment. The one dimension that (unfortunately) seems to dominate many discussions of human interaction with automation is the relative level of autonomy of human and machine agents. The taxonomy of levels of automation first presented by Sheridan (1978) describes variations in the relative degree of autonomy of automated systems and human agents. This taxonomy continues to be in use as a framework for discussions of human interaction with automated systems (for recent examples, see Moray, Inagaki, & Itoh, 2000; Parasuraman, Sheridan, & Wickens, 2000). The authors believe, however, that this is a misleading and counterproductive way to think about the space of possibilities in the design of human-machine systems. The Sheridan-Verplank levels are a prescriptive framework that lead naturally to thinking in terms of how functions should be allocated between humans and automated systems. It reinforces a dichotomous view of the roles of humans and automation dating back to Fitts (1951), whose list describes tasks best performed by men versus those best given over to machines: "Men are better at… Machines are better at…" (aka MABA-MABA).

The problem with this perspective is not that relative autonomy is unimportant, but that it downplays and de-emphasizes the issues of human-machine coordination that appear no matter what the relative autonomy of human and machine agents. Relative autonomy is just one of many dimensions of automated systems (Woods, 1996) that influence the cognitive work and forms of coordination needed to achieve high levels of performance in the joint system of human and machine agents working together (Hollnagel, 1998).

In addition to autonomy, for instance, automation varies in terms of how it influences operators' access to information and the availability of new forms of information about the state of the world (observability). This can change information sampling behavior, search patterns, and the cognitive work involved in integrating data into meaningful information (see Woods, 2003, for an example of this in the case of human-robot coordination). Automation can also change authority relationships between human and machine agents. Forms of high authority automata include envelope protection systems in aviation and auto-braking in rail operations.[1]

The new systems and technologies proposed for train operations vary in terms of the cognitive work functions performed, in terms of levels of observability, autonomy, and authority, and therefore in terms of their impact on joint system performance. For example, a new system could combine in-cab signaling with envelope protection functions on top of the basic train engineer tasks.

PTC is somewhat different from the forms of automation most often studied in the literature on human-machine interaction. Typically, these involve automated systems that take an ongoing, active part in the control of some complex dynamic process, often changing the role of the human operator to one of supervisory control. This shift in roles is a major part of studies in aerospace that examine automation as a team player (e.g., Layton, Smith, & McCoy, 1994; Sarter, Woods, & Billings, 1997). In contrast, PTC is more akin to, for example, envelope protection systems on commercial aircraft or automatic safety systems in nuclear power plants. The distinguishing feature of these (high authority) systems is that under routine operating conditions they remain inactive and outside the control loop, taking over or becoming engaged only when an abnormal or potentially threatening condition is detected.

Issues of coordination in joint systems based on protection envelopes and takeovers of control include factors such as levels of false alarms, control conflicts (see the Nagoya accident (Sogame & Ladkin, 1996) and related incidents in aviation), handling disruptions created by the takeover, re-establishing normal control modes after the initiating event, and authority-responsibility double binds. Alternatives to takeover or protection joint systems also exist in the form of critiquing architectures for joint systems (Guerlain et al., 1999).

The basic unit of analysis for these discussions is the joint system that consists of people, automata, and other cognitive tools (Hollnagel, 1998; Hutchins, 1995; Woods, 2002; Woods & Tinapple, 1999). This places coordination, shifting work strategies, and synchronization at the center of any analysis of cognitive work. The joint systems perspective has replaced the substitution approach that treats people and automata as separate and mostly independent and interchangeable parts. One of the temptations in designing certain kinds of automated systems is to assume independence from humans' activities in the system. This is especially true of automation intended to act in the role of a backup or redundant safety net. It is easy to see how designers might be led to assume that such systems would have little or no impact on how people go about their routine

[1] High authority automata, however, cannot also takeover responsibility as that is unique to human accountability relationships (Woods, 2002). Responsible agents experience consequences associated with outcomes. In general, people with authority tend to be assigned responsibility as well. Dividing responsibility and authority creates double binds and dilemmas, which can degrade performance (Billings, 1996; Woods, Johannesen, Cook, & Sarter, 1994, Chapter 4).

activities. In general, however, human performance is configurable in nature. That is, people react to the totality of their task environments, including the perceived nature of automated systems in the background. Ultimately, the issue is not simply human performance but rather joint system performance, especially as events create the need to move from one form of joint system to another.

2.2. Workload Transitions

The performance issues that this report will examine most closely are those related to the notion of workload transitions. Huey and Wickens (1993) present the only major work on workload transitions. This work was the product of an expert panel assembled by the National Research Council in an effort to understand the impact of crew-size reductions on the performance of U.S. Army M-1 tank crews. Workload transitions are sudden onsets of high cognitive workload after some lengthy period of relative inactivity. The 1993 report noted that, at the time, although workload was an intensely studied topic, workload transitions had received very little direct attention. Unfortunately this continues to be the case. Despite the apparent impetus provided by the 1993 report, relatively little new work has emerged specifically on the topic.

The transitions that are the concern here result from gaps in the performance of PTC functions—when it is not available in sections of track, when failures occur, or when sections support different PTC systems. In fact, similar kinds of transitions are a standard feature of the world of train operations in general—train engineers often need to transition smoothly across the territories of different track owners with different sets of operating rules. Dispatchers must often handle trains, simultaneously or in sequence, with varying characteristics (e.g., freight versus high-speed passenger).

As a result, it is more appropriate for the purposes of this report to take a less narrow view of workload transitions than the one adopted in Huey and Wickens (1993). The research team needed to adopt a broader definition that considered the effects of adding automation to the nature of transitions and their effects in a joint system. The research team refers to workmode transitions as encompassing any functionally significant change in the qualitative or quantitative aspects of the work performed by experienced train operators or dispatchers. A functionally significant change is any change in conditions that entails a shift in the skills, knowledge, or strategies that must be activated in order to perform effectively.

2.3. Workmode Transitions and Heterogeneity

The basic form of work transitions in today's and future rail operations involves the need to switch among modes of work as the characteristics of the situation demand. Workmode transitions introduced by gaps in PTC and other automation overlay systems expand the potential for train engineers and dispatchers to confront more frequent and more varied forms of workmode transitions. The research team refers to this characteristic of rail operations as heterogeneity (i.e., the potential for people in a role to experience various workmode transitions). The question is how various characteristics of such automation could impact the types and consequences of workmode transitions and how this additional heterogeneity due to the introduction of PTC-like automation is likely to influence operations.

Heterogeneity is a systems property that can serve as a useful guide to joint systems analysis. The first question becomes the ability to anticipate and prepare for transition points. Events that initiate workmode transitions include:

- Failures in parts or all of the PTC system
- Changes in PTC support available across territories

Constraints in these events exist, as some initiators can be anticipated and other unplanned-for events are by their nature unpredictable (e.g., PTC system failures).

When PTC systems fail or are unavailable, a shift for the engineer or dispatcher to use a fallback mode of operation occurs. For example, when trains move across territories with different (or no) PTC systems, engineers need to shift to alternative strategies consistent with the support for that section of territory. Strategies that were effective or highly practiced in the previous mode of work may be different or less practiced in the fallback mode of work. Thus, the second question becomes what kinds of joint system performance are required after the transition, and can people be effective in (a) shifting to and (b) continuing to carry out the tasks/strategies associated with the new workmode.

Two general classes of breakdowns are of interest after anticipation or detection of the transition. One is breakdowns in automaticity following transitions, which refers to the highly proficient sets of skills (and the associated basic cognitive processes) built up by experienced train engineers. The other is breakdowns in coordination across distributed human and machine agents, which concerns the synchronization of information and task exchange between various parties in recognizing the transition and after the transition has taken place.

Hence a framework for analyzing joint systems in train operations has begun to emerge—potential gaps in PTC systems are compensated for through the human's ability to move from one mode of operation to another. In order to develop and use the framework in predicting and analyzing new failure modes, this report first needs to provide an overview of potentially relevant themes in human-automation coordination.

2.4. Surprising Effects of New Technology

Studies of the impact of technological change in aviation, health care, air traffic management, or many other areas undergoing change today (e.g., Cook & Woods, 1996a, 1996b; Dekker & Woods, 1999; Obradovich & Woods, 1996; Smith et al., 1998) find that technology change initiates a process that changes the nature of practice:

- New roles emerge.
- What is canonical (routine) and what is exceptional change.

- The kinds of erroneous actions and assessments that can be expected change.
- The paths to failure change.
- People in their various roles adapt by actively altering tools and strategies to achieve goals and avoid failure.

First, the demands may involve new or changed tasks, such as device setup and initialization, configuration control, or operating sequences. Second, cognitive demands change as well, creating new interface management tasks, new attentional demands, the need to track automated device state and performance, new communication or coordination tasks, and new knowledge requirements. Third, the role of people in the system changes as new technology is introduced. Practitioners may function more as supervisory controllers, monitoring and instructing lower order automated systems. New forms of cooperation and coordination emerge when automated systems are capable of independent action. Fourth, new technology links together different parts that were formerly less connected. As more data flows into some parts of a system, the result is often data overload. Coupling a more extensive system more tightly together can produce new patterns of system failure. As technology change occurs, the price of new benefits is often a significant increase in one or another type of operational complexity.

When these reverberations of technology change are not anticipated, surprises occur: surprises in the form of accidents that represent new paths to failure and in the form of negative side effects unanticipated by designers—automation surprises—breakdowns in coordination between people and automata (Billings, 1996; Dekker & Hollnagel, 1999; Sarter & Amalberti, 2000, for the case of cockpit automation).

2.4.1 Clumsy Automation

Clumsy automation represents the situation where, when automation is added to an existing process, the addition can add to the workload of the users, often by making tasks in times of already high workload more difficult, such as by adding layers to the access of needed information or by requiring users to allocate additional resources to managing the automation as well as the basic system. Often such automation systems do ease the workload of users when conditions are already light (and thus appear helpful), and only when presented with challenging situations does the extra burden become apparent.
The source of clumsy automation is often classic flaws in the design of interactive, computer-based devices (Woods et al., 1994). Devices impair rather than support cognitive work when they do the following:

- Make things invisible, especially hiding interesting events, changes, and anomalies.
- Proliferate modes.
- Force serial access to highly related data.
- Proliferate windows and displays.
- Contain complex and arbitrary sequences of operations, modes, and mappings.
- Add new interface management tasks.
- Suppress cues about the activities of other team members, both machine and human.

These characteristics create a number of negative impacts on human cognition and activities:

- Increase demands on user memory.
- Complicate situation assessment.
- Undermine attentional control skills (where to focus when).
- Add workload at high-criticality, high-tempo periods.
- Constrain the users' ability to develop effective workload management strategies.
- Impair the development of accurate mental models of how the device functions and its underlying processes.
- Decrease knowledge calibration (i.e., mislead users into thinking that their models are more accurate than they actually are).
- Undermine coordination across multiple agents.

2.4.2 Mode Errors

Mode errors are a prominent example of the new and often unexpected kinds of failures that can be created when automation is introduced into a given work environment. They have a particular relevance to the current discussion because of the analogies they bear to the structure of workmode transitions. The concept of mode error originated in the context of relatively simple computerized devices, such as word processors, used for self-paced tasks where the device only reacts to user inputs and commands. Mode errors in these contexts occur when an intention is executed in a way appropriate for one mode when, in fact, the system is in a different mode. In this case, mode errors present themselves as errors of commission (that is, where a person takes an action that, for the situation, is inappropriate).

In one sense a mode error involves a breakdown in going from intention to specific actions. In another sense, however, a breakdown in situation assessment has occurred—the practitioner has lost track of the device's mode. One part of this breakdown in situation assessment seems to be that device or system modes tend to change at a different rhythm compared to other user inputs or actions. Mode errors emphasize that the consequences of an action depend on the context in which it is carried out. On the surface, the operator's intention and the executed action(s) appear to be in correspondence; the problem is that the meaning of action is determined by another variable—the system's mode status.

2.4.3 User Adaptation: Task and System Tailoring

Cook, et al. (1991) coined the terms system tailoring and task tailoring to describe the kinds of adaptations that users make in reaction to the introduction of poorly designed new technology. System tailoring adaptations tend to focus on shaping the technology itself to fit the pre-existing strategies of operators and the demands of the field of activity (e.g., adaptation focuses on the setup of the device, device configurations, and how the device is situated in the larger context).

In task tailoring, operators adapt their strategies, especially cognitive processing strategies, for carrying out tasks to accommodate constraints imposed by new technology. For example, information systems that force operators to access related data serially instead of in parallel result in a proliferation of windows and new window management tasks (e.g., searching for related data, decluttering displays as windows accumulate, etc.). Operators may tailor the device itself, for example, by trying to configure windows so that related data is available in parallel, but they may still need to tailor their activities. Task and system tailoring represent examples of operators' adaptive coping strategies for dealing with clumsy aspects of new technology, usually in response to criteria such as workload, cognitive effort, ease of use, and robustness to common errors. The danger associated with these strategies is that adaptation based on operators' locally defined criteria can lead to brittle features in the larger system. In the language of adaptation, local work practices become overspecialized with respect to the prevailing conditions, thus becoming highly sensitive and prone to fail when these conditions change.

2.4.4 Increased System Coupling

Automation and computerization increase the degree of coupling among parts of a system. Some of this coupling is direct; some results from potential failures of the automation; and some is the result of the effects of automation on the cognitive activities of the practitioners responsible for managing the system. For example, higher coupling produces more side effects to failures. A failure is more likely to produce a cascade of disturbances that spreads throughout the monitored process. Symptoms of faults may appear in what seems to be unrelated parts of the process (effects at a distance). These and other effects can make fault management and diagnosis much more complicated. Highly coupled processes create or exacerbate a variety of demands on cognitive functions (Woods, 1988). For example, increased coupling creates:

- New knowledge demands (e.g., knowing how different parts of the system interact physically or functionally)
- New attentional demands (e.g., deciding whether or not to interrupt ongoing activities and lines of reasoning as new signals occur)
- More opportunities for situations with conflicts between different goals
- New strategic tradeoffs (e.g., creating or exacerbating conflicts and dilemmas that produce new forms of system breakdown (see Woods, Tittle, Feil, & Roesler, 2004))

Automation may occur in the service of stretching capacity limits within a system. These efficiency pressures, however, may very well create or exacerbate double binds that practitioners must face and resolve. These pressures may also reduce margins, especially by reducing the system's error tolerance and the practitioners' ability to recover from error and failures. Although not a stated purpose of PTC, the new capabilities may be exploited to achieve increases in traffic density, with smaller margins of safety between trains (at least on high-traffic routes). It will be important to consider how this might affect the recovery interval subsequent to a PTC failure (i.e., the period of time in which actions can be taken to prevent serious consequences). In addition, the presence of PTC may influence the complexity of traffic flows. Dispatchers may take advantage of some of the PTC capabilities to tailor routings more effectively to suit the moment-to-moment traffic situation and the capabilities of individual trains, thereby reducing the level of consistency from day to day. This could make it more difficult to predict the cascade of effects due to delays or accidents in a given sector of track.

In another sense of coupling, technology change often facilitates greater participation by formerly remote individuals. People, who represent different but interacting goals and constraints, can now interact more directly in the decisionmaking process. The connectivity and communication capabilities provided by PTC may well foster this sense of coupling. There is a concern, however, about the effects of failures in the PTC system that will require people to alter their modes of collaboration.

2.4.5 Primary/Backup Inversion

Occasionally, systems introduced as backups or as additional layers of redundancy are subject to a phenomenon (Wiener & Curry, 1980) termed primary/backup inversion. Wiener and Curry used this to refer to the tendency of flight crews to come to rely on alerts and warnings as the primary indicators of problems with the aircraft, rather than as secondary to instrument indications. Another example is the use of Global Positioning System (GPS) guidance systems by general aviation pilots. Although GPS is officially supposed to serve only as a redundant or backup mode of navigation, it has become clear that some pilots adopt it as their primary navigation method. The result has been a number of incidents where pilots have flown into trouble as a result of problems with GPS. This is clearly a potential issue for PTC and related systems, particularly with respect to the use of auditory warnings to indicate signal aspects to engineers. One can perhaps imagine high workload situations where engineers fail to perform a visual check of displayed signals, relying instead on the auditory warning to inform them of any potential conflicts. This could be particularly concerning in situations where the high workload task that has engaged the engineers causes them to give less than full attention to the auditory signal.

2.4.6 Shifts in Authority

The introduction of new automation often entails changes in the authority structure of the man-machine system (Woods, 1996). Typically, the automation is given the authority to take certain actions on its own initiative, with or without the approval of human operators. Shifts in authority can create confusion about who is really in charge of operating the system. This type of confusion contributed to at least one rail accident at Shady Grove, a station on the Washington, DC, Metro system (NTSB, 1996). In this case, a train operating under automated control in poor traction conditions overshot a platform and struck a stationary train, killing the driver of the first train. The accident resulted in part from a strict policy of the operating organization to run trains under automated control at all times, in all weather conditions, except for emergency situations. This policy effectively blocked the humans in the system from applying their knowledge, skills, and judgment to make operating decisions. In the Shady Grove case, controllers at the operations center had become aware of several instances of trains overshooting platforms, but their requests to allow trains to switch to manual control in order to compensate for the track conditions were denied based on the policy.

The Shady Grove accident is a very instructive one for issues related to automated control of trains. It illustrates the need to facilitate the ability of human operators to assess the need to override the automation and to give them the means to do so if necessary (e.g., if conditions outside the design scope of the automation are encountered). Apart from organizational factors such as those in the Shady Grove incident, supporting these needs demands that automated systems be designed as team players (Christoffersen & Woods, 2002; Malin et al., 1991). Team play involves two fundamental criteria. People need to be able to assess the automation's perception of the current conditions and compare this with independent indications (the observability criterion). If people judge that the automation may take inappropriate actions, they must be given ways to override or re-direct the automation (the directability criterion). These characteristics preserve and support people's ability to make intelligent decisions about control.

When automated systems with high authority hide their activities (i.e., low observability), the result can be bumpy transfers of control, such as in the China Airlines case described in Billings (1991). In this incident, a Boeing 747 aircraft flying at cruise altitude lost power in one engine. Unbeknownst to the pilots, the automation attempted to compensate for the loss of power by making progressively more severe control inputs to the flight surfaces. When the captain disengaged the autopilot, the airplane immediately rolled, yawed, and entered a steep descent. The pilots were able to recover control but not without extensive damage to the airplane.

A question raised with respect to PTC has been whether engineers might try to trick the automation (e.g., by deliberately entering incorrect consist information) in order to change its performance characteristics (e.g., to achieve less conservative braking profiles). The prevailing opinion seems to be that this is unlikely given the probability that such activities would be recorded and detected. Nonetheless, it exemplifies the problems that can arise when authority is taken away from human operators. Another question with respect to PTC is whether operators will be given the means to repair any inconsistencies in the automation's model of the context (e.g., an unusual condition not accounted for in the signaling loop). Can users repair gaps between the automation's model and the actual operating context?

2.5. Human Performance Concerns

The authors now begin to sharpen the discussion to more closely match the human performance issues raised by the introduction of PTC. In one sense, workmode transitions present an analogy to mode transitions. Recall from the discussion of mode errors above that mode transitions involve a change in the environment that alters the mapping between intentions and the appropriate actions. Mode errors have a dual nature because they can be thought of as errors in situation assessment (i.e., failure to detect a mode transition) or as slips of action (i.e., breakdowns in performance under a new mode (Norman, 1981)). The following touches on a number of issues that can be identified with one or another of these aspects of mode errors.

2.5.1 Monitoring and Complacency

As emphasized above, the introduction of automated systems often creates new or altered monitoring requirements for human operators. A number of studies have shown decrements in failure detection performance relative to manual control when humans act as supervisors of automated controllers (e.g., Ephrath & Young, 1981; Wickens & Kessel, 1979, 1981). These types of failures are largely attributed to humans being removed from direct interaction with the process, thus losing some of the feedback associated with directly observing the effects of control activities.

Effective monitoring is most likely to occur when operators are active observers, engaged in seeking and generating information (e.g., Mumaw, Roth, Vicente, & Burns, 2000). In contrast, passive involvement by human operators can lead to degraded situation awareness (Endsley & Kiris, 1995). Degraded situation awareness means that at any given moment, human operators may have an incomplete or stale model of the state of the world and the factors driving how the state is changing. The penalties for degraded awareness tend to appear if the automation fails or encounters an unfamiliar circumstance, requiring the human operator to suddenly take a more active role in control. When operators have been out of the loop, a cost is associated with orienting to the detailed features of the situation. Operators must come up to speed before they can participate effectively in control activities. In addition to monitoring the controlled process, a key function of human operators in automated systems is to monitor for failures in the automation itself.

One of the concerns often raised about human monitoring of automated systems is that, because the systems are generally quite reliable, operators may become complacent, meaning that they will fail to monitor the automation as closely as they should to ensure that it is performing properly (e.g., Parasuraman, Molloy, & Singh, 1993). Instances will almost surely occur where problems in the automation go unnoticed for a period of time. The most common design response to this is to generate alarms to notify the operator of any faults or suspicious conditions. This strategy, however, carries its own risks. The problem of false alarms is well known in supervisory control. Because the potential consequences of missing a fault condition can be high, a tendency exists to set a low threshold for triggering alarms to alert operators to potential problems. The result of course is a tendency for operators to discount the alarms—the cry wolf syndrome. False alarms can be especially problematic when the base rate of actual failures is low. When base rates are low, even a highly sensitive warning system with an objectively low false alarm rate tends to produce a large proportion of warnings that are not indicative of actual problems (Parasuraman, Bahri, Deaton, Morrison, & Barnes, 1997).

2.5.2 Fixation

False alarms can lead to one of the forms of fixation identified by DeKeyser and Woods (1990). Cognitive fixation is a pattern of performance normally associated with diagnostic reasoning tasks where people fail to revise their situation assessment appropriately as new evidence comes in over time. DeKeyser and Woods described three forms of fixation: *everything but that*, where people entertain many hypotheses but never the right one; *nothing but this*, the opposite of the first form, where people doggedly persist in one strategy or goal, seemingly unable to shift or consider other possibilities; and *everything is OK*, where people do not respond to cues in their environment, even if multiple indications exist that something is going wrong. The third form is the one likely to be provoked by high false alarm rates. In the third instance, they seem to discount or rationalize away indications that contradict their current, nominal model of the situation.

2.5.3 Skill Loss

One of the frequently mentioned issues in the use of automated systems is the possibility of loss of skill on the part of human operators. If the automation is reliable and competent, the human supervisor may only rarely get the opportunity to exercise his control skills. Over the long term, this can lead to a loss of proficiency on the original control task (e.g., Wiener, 1988; Wiener & Curry, 1980). This phenomenon can influence both manual and cognitive skills. One of the major cognitive skills that might suffer from automated control is anticipatory ability. For example, there are proposals for air traffic control systems that will perform predictive functions, including envisioning potential future conflicts. Such systems may lead to decay in the ability of air traffic controllers to extrapolate future trajectories (Wickens, 1998).

Another possibility is that people will develop heuristics and methods of doing their job that depend on the information normally available from the automation. When the automation fails, the question is whether they are able to fall back to using more complex models and methods. Organizational responses to this vulnerability include periodic training or designated days on which the system is to be operated in manual mode (e.g., Parasuraman, Mouloua, & Molloy, 1996; Rose, 1989).

2.5.4 Inert Knowledge

A variety of research results have revealed dissociation effects where knowledge accessed in one context remains inert in another (Gentner & Stevens, 1983; Perkins & Martin, 1986). In evaluating performance, the critical questions about knowledge are not whether the problem-solver possesses relevant domain knowledge, but whether he/she can access and utilize situation-relevant knowledge under the conditions in which the task is actually performed. Inert knowledge may be related to cases that are difficult to handle or novel in some way, not because people do not have the individual pieces of knowledge necessary to build a solution, but because they are not normally used together in the same context. Sarter and Woods (1994) found that some pilots possessed knowledge in the sense of being able to recite the relevant facts in debriefing, but they were unable to apply the same knowledge successfully in an actual flight context—that is, their knowledge was inert.

Results from accident investigations often show that the people involved did not call to mind all the relevant knowledge during the incident, although they knew and recognized the significance of the knowledge afterwards. The triggering of a knowledge item X may depend on subtle pattern recognition factors that are not present in every case where X is relevant. Alternatively, that triggering may depend critically on having sufficient time to process all the available stimuli in order to extract the pattern. This may explain the difficulty that practitioners have in seeing the relevant details in a certain case where the pace activity is high and where multiple demands on the practitioner exist.

2.5.5 Slips and Lapses

Reason (1990) refers to inert knowledge as a contributing factor to certain kinds of slips and lapses. Specifically, these errors result from failures to access knowledge relating to changes in the circumstances under which a given routine is normally executed. Reason describes the example of going to the kitchen to make a cup of instant coffee for yourself (your normal routine) and a cup of tea for a friend, but returning to your friend with two cups of coffee. Reason explains this error as a result of failing to make an attentional check at the branch point of the procedure (i.e., after boiling water and simply proceeding along the coffee-making route). The need to make slight variations to highly practiced routines, particularly when the new circumstance is relatively rare, is likely to produce these kinds of errors. Such phenomena may be particularly relevant in the case where train operators must sustain a seldom used fallback mode of performance after a PTC-induced workmode transition. In general, one might expect that highly automatized behaviors (such as information sampling patterns) will tend to be a source of potential errors in a context characterized by workmode transitions.

2.6. Summary

Based on the foregoing discussions, the research team selected the following aspects for analysis in PTC operations for the potential for risks from workload and workmode transitions to occur:

1. Complacency
2. Fixation
3. Skill loss and inert knowledge
4. Primary/backup inversion
5. Mode errors
6. Shifts in authority
7. Loss of situational awareness

Section 5 discusses the results of this analysis by considering the likelihood of transitional situations where these types of problems may occur.

3. Types of PTC Systems

3.1. Introduction

Present day freight railroad train control practice embodies significant automation and automated supervision of the dispatcher’s activities but relatively little automation of the train operator’s function. Passenger railroads, with high density operations and large numbers of people at risk in an accident, have been much more active in using automated systems on the train. The following summarizes present practices.

3.1.1 Dispatching and Train Control

There is a long history of automation in dispatching and train control. Nineteenth century mechanical interlockings physically prevented conflicting signal and turnout settings over a given area. More modern relay and microprocessor interlockings do the same thing, by refusing to respond to attempts by the dispatcher to set unsafe routes. Automatic block systems, with signals controlled by track circuits, can manage the movements of a sequence of trains along a railroad line, with the dispatcher only intervening if a need to stop or change the routing of a selected train exists or if a problem occurs.

Another layer of automation in train control is the automatic routing of trains. In this case, a central computer tracks the movements of individual trains, and it selects and sets up routes to follow either pre-set routings or routings optimized to minimize delays. The route-setting function is independent of the safety-critical block and interlocking systems. A fault in route setting should not lead to an unsafe route being set in the field. These systems exist more commonly in Europe, where dispatching centers have used train describers, which identify and track individual trains by number on big wall displays and on screens at dispatcher desks, with a link to schedules and pre-planned routings. In the United States, computer-aided dispatching (CAD) systems are beginning to add software to optimize and implement train movements. The dispatcher is thus shifting from a hands-on operator to a supervisor of the automated system, with all that this implies for situational awareness and workload and workmode transitions.

PTC systems do not directly automate any of the dispatcher’s duties. PTC, however, can change the information available to a dispatcher and change the means of communication between dispatcher and the train. Examples of these changes include:

- More precise information about train location and speed is available and can be used in automated routing systems.
- Dispatchers may enter information on a new work zone or a temporary speed limit into the system for transmission to the train, rather than it being transmitted by voice radio.

3.1.2 The Train Crew

In contrast, much less automation of the train crew's functions has occurred. The safe operation of most main line trains relies on compliance with visual signals, dispatcher instructions (usually received by voice radio in the United States), and a large number of written operating rules and instructions. The automatic safety systems for engineers that do exist are all of the envelope protection kind, which will intervene to apply brakes only when the engineer fails to respond correctly to selected signals or instructions. Simple systems of this type, which will apply the brakes if an engineer fails to acknowledge an in-cab warning of a more-restrictive signal, have been in use since about 1900. These are intermittent Automatic Train Stop (ATS) systems in the United States. Such systems, with a number of variations and enhancements, are widely in use on European main lines and in a few locations in the United States. More complex Automatic Train Control (ATC) or Automatic Train Protection (ATP) systems, which provide continuous supervision of train speed, relative to signal indications and (sometimes) permanent and temporary speed limits, are in use on the Northeast Corridor in the United States and on European and Japanese high-speed passenger lines. The safety performance of such systems is extremely good—as far as this team is aware at the time of this report, a train occupant fatality has never occurred for any reason on any purpose-built high-speed rail line in nearly 40 years, since the Tokaido Shinkansen opened in Japan.

Train control and safety systems on purpose-built high-speed lines have a much simpler task than those on a mixed-traffic main line rail network. The whole system—trains, infrastructure, and train control—is designed and built at the same time as an integrated system, only one or two types of train are operated (having uniform braking characteristics), the track layout is simple with few junctions, and the pattern of train operations is very simple and consistent. Retrofitting a train control system with comparable functions to existing rail lines is a much more difficult proposition. Both train operations and track layouts are much more complex, and new equipment usually has to work with a variety of existing trackside and train-borne equipment. In fact, the Northeast Corridor between Boston and New Haven is one of the few places in the world where retrofitting of a train control system comes close to meeting FRA's desired functionality for PTC systems on an existing line.

The primary function of PTC is to provide supervisory control (that is, acting like a supervisor looking over the shoulder of the primary responsible party—the engineer), which will intervene if the operator fails to operate the train in accordance with signal indications and applicable operating directives. The following section describes PTC functions and systems.

3.2. Overview of PTC Systems

The intention of PTC systems is to provide protection against some of the most significant causes of railroad accidents:

- Trains exceeding the limits of authority, such as passing red signals or going past the limits of their authority as issued by dispatchers in dark territory operations
- Trains exceeding speed limits (either permanent or temporary)
- Trains entering work zones without approval

PTC systems generally provide protection from these types of events by comparing the locomotive’s position (as detected by GPS on the locomotive) with knowledge of the train’s limits of authority, locations of work zones, and locations of speed limits. This knowledge can be obtained in a variety of ways, depending on the specific PTC system. For example, the CBTM system under development by CSX Corporation provides data to an onboard computer via a radio data link from the dispatchers’ CAD system that has the current data stored within it. This data link provides the CBTM computer with information about what boundaries of authority the dispatcher has authorized, for example.

Should the PTC computer detect that the train is exceeding the limits of authority or is in breach of any of the other protection modes, it provides a warning to the locomotive crew; if no appropriate action is taken by them, it stops the train. Thus, PTC systems in this sense provide backup (overlay) protection rather than act as a primary control system—it is still the train crew’s responsibility to comply manually with rules related to authorities, speed restrictions, and work zones as if the PTC system did not exist.

The CBTM system provides a display to the locomotive engineer, showing the system’s operational status, and, in the event of an approaching restriction or need for a penalty brake application (e.g., in the event of overspeeding), it provides both aural and visual warnings. The CBTM interface design is under development and is planned to appear as a colored cathode-ray tube display in the area of the main displays at the engineer’s control stand, replacing the earlier small monochromatic displays that were located out of the engineer’s normal view.

In addition to the CSX CBTM system, several PTC systems are under development or in trial application. These include the Advanced Speed Enforcement System (ASES) used by New Jersey Transit, the Incremental Train Control System (ITCS) used by Amtrak and Norfolk Southern in Michigan, and the NAJPTC System under development for application on Amtrak and Union Pacific operations in Illinois.

All PTC systems provide protection in conceptually similar ways to the CBTM system. Each system, however, has variations in its details, especially in terms of the display type and location. For example, the NAJPTC System is intended to allow higher speed passenger operations between St. Louis and Chicago. In order to do so, the in-cab system's display provides information about signal aspects and other information (such as upcoming speed limits and work zones) further down the track than the engineer would be able to see at the high-speed operations, which is a component needed for normal operations as well as for enforcing safety. Consequently it is located prominently in the train engineer's normal field of view. ITCS and ASES provide indications of the train's speed, and current and upcoming speed limits to the engineer; these are located prominently in the engineer's normal field of view. The location of these displays, for instance, can play an important role in the possible concerns with transitions, as discussed in the next section.

The emphasis in this analysis is on the effects on train crews (principally locomotive engineers) because, with the current designs of PTC systems, they are the people affected. PTC system uses do not directly affect others involved in train controls (primarily dispatchers) other than in very marginal ways. For instance, the CAD system captures dispatchers' control actions and relays them to the onboard train system in ways that are invisible to the dispatcher. Failures in the CAD system could result in possibly erroneous instructions being sent to the train crews and the PTC system for action; nothing is unique in the failure opportunities because of the presence of the PTC system. The only likely interaction between dispatchers and the PTC system with the current generation of designs is that, when PTC system failures occur, the train crew must get authorization from the dispatcher to shut down the PTC system. The effect of PTC system failures on the train crews is considered explicitly in this analysis, but there is no further consideration of the effect on dispatchers—the anticipated effect would be only a slight increase in workload to record the failure.

3.3. Characteristics Relevant to Workload and Workmode Transitions

For any of the PTC systems to have the potential to be susceptible to many of the kinds of concerns associated with transitions discussed in Section 2.5, it must be capable of types of interactions with the users. The following discusses issues of concern and the relevant characteristics of the systems.

- *Complacency*: This requires that the PTC system provides some level of operational action on which the engineer can become over-reliant. The most obvious example would be to rely on the system to stop the train at the end of its authorities or to enforce speed restrictions. Concerning the speed restrictions, however, the enforcement would be through bringing the train to a halt by a penalty brake application, which is very undesirable for an engineer.
- *Fixation*: For fixation to be an issue, something must exist on which the engineer can be fixated. Most typically this would be through the displays, or some aspect thereof, which would include speed indications, upcoming changes or restrictions, or any information about location (such as with the NAJPTC System).
- *Skill loss and inert knowledge*: Skill loss could occur with PTC systems in cases where people have become overly reliant on the system to provide protection—similar to the complacency issue above—and then are unable to act swiftly or accurately enough when the system fails. Inert knowledge problems could occur

when engineers are required to use formal knowledge or training that has not normally been put into practice, as might occur when having to perform diagnostic or problem-solving actions with the system during operations.

- *Primary/backup inversion*: As with complacency, the potential of a PTC system to become the normal control system can occur if it is used to accomplish the functions for which it is expected to provide a backup.
- *Mode errors*: Mode errors are unlikely with the current designs of PTC systems that have only one mode. However, the growing complexity, as seen with the new interface designs for the CBTM system, and the extended use of the NAJPTC System as an operational aid, as well as a protective device, may raise the potential of this class of concern in the future.
- *Shifts in authority*: Shifts in authority can come about in two ways: shifts in authority between the automation system and people, and changing the roles between people involved with the system, such as the engineer and the dispatcher. Within the use of PTC systems as an overlay system, limited opportunities to create shifts in authority seem to exist; although as the systems extend their capabilities and uses, the potential exists for these shifts to occur.
- *Loss of situational awareness*: Loss of situational awareness can come about through the PTC system acting as a distraction to the locomotive crew from continuing to observe outside the cab as the train is moving, such as reading error messages after the system has failed.

3.4. Opportunities for Transitions While Using PTC Systems

Two kinds of workload and workmode transitions can occur while using PTC systems: transitions in service made by the equipped locomotive and failures in operation by the PTC system. The following summarizes specific instances of these transitions. Section 5.2 analyzes the potential for the issues identified in Section 2.5 occurring during these transitions.

3.4.1 Transitions in Service

1. Enter PTC coverage (including initialization with train data, etc.)
2. Leave PTC coverage
3. Enter workzone
4. Leave workzone
5. Enter permanent speed restriction
6. Leave permanent speed restriction
7. Enter temporary speed restriction
8. Leave temporary speed restriction
9. Enter authorized territory/block
10. Leave authorized territory/block
11. Enter siding
12. Leave siding
13. Enter restricted speed rule
14. Leave restricted speed rule

15. Receive directive from dispatcher
16. Report position
17. Reach failed signal showing false stop
18. Reach failed signal showing false proceed
19. Suffer failed CTC system
20. Recover from failed CTC system
21. Suffer failed cab signaling system
22. Recover from failed cab signal system
23. Receive detector warning
24. Start shift
25. End shift

3.4.2 Failures in Operation of the PTC System

1. Failure of the onboard communications subsystem
2. Other onboard system failures
3. Loss of communications with wayside devices
4. Failure of zone controller

4. Accident Review

4.1. Introduction

This project is concerned with the extent to which workload and workmode transitions can affect the safety of railroad operations where PTC systems are used. In particular, concern exists that operations with PTC may introduce new transition events, leading to new opportunities for train crew and dispatchers to make errors that could cause an accident. The purpose of the analysis described in this chapter is to provide background for the detailed analysis of PTC-related workload/mode transitions in Section 5 in two areas:

- To provide a sense of the scale of train accident risks associated with PTC-related workload/mode transitions, by summarizing the numbers and types of PTC-preventable accidents. This includes both the extent to which the overall risk of train accidents can be reduced by implementing PTC and where a risk exists that PTC benefits will be less than anticipated due to workload/mode transition problems.
- To review detailed descriptions of a sample of past human factors train accidents to develop a sense of the significance of workload transitions in causing these accidents. With a few exceptions, these accidents occurred on lines operated with conventional train control methods. Minimal operating experience with PTC exists and only limited experience with traditional ATC, other than on high-density passenger lines.

4.2. Railroad Accident Risks

This section provides a brief discussion of overall railroad accident risks and the subset of those accidents that are PTC-preventable.

Under current FRA regulations, railroad accidents in the United States must be reported to FRA in the prescribed format if damage to railroad property exceeds a set amount.

Approximately 3000 reportable accidents occur per year. Table 1 lists actual accident numbers and accident rates (accidents/million train miles). These numbers are reported in the FRA Railroad Accident/Incident Reporting System (RAIRS). The numbers are for all types of train and railroad, including passenger and freight trains, light locomotives, work trains, and cuts of cars for Class I, regional, and local freight railroads and passenger systems.

Table 1. FRA-Reportable Accidents 1997–2004

Year	Accidents	Rate: Accidents/ Million Train Miles
1997	2397	3.54
1998	2595	3.77
1999	2768	3.89
2000	2983	4.13
2001	3023	4.25
2002	2738	3.76
2003	2992	4.02
2004	3104	3.98

Both the number of accidents and the accident rate have increased over this period. Railroad traffic increased rapidly over the period 1997 to 2001, straining both the railroad workforce and railroad plant and equipment. This, and some operational problems in individual railroads, led to a small decline in safety performance. The situation stabilized and has shown improvement after 2001, with a slowing of traffic growth and efforts by the railroad to resolve its operating difficulties.

The majority of these accidents occur on yard and industry tracks during switching activities, where PTC would not be applicable. The numbers of accidents on main and siding tracks, where PTC could be installed, are as shown in Table 2. FRA defines sidings as "auxiliary tracks used for meeting and passing trains;" as such these are regularly used by line-haul trains, and most would be equipped with PTC.

Table 2. FRA-Reportable Main and Siding Track Accidents 1997–2004

Year	Main Track Accidents	Siding Track Accidents	Total
1997	867	106	973
1998	934	101	1035
1999	858	106	964
2000	976	120	1096
2001	1025	111	1136
2002	886	79	965
2003	967	95	1062
2004	992	106	1098

The majority of these accidents result from mechanical failures of track or equipment components and collisions at grade crossings. Except for a few conditions that can be detected by automated systems (for example, broken rails that interrupt track circuits or a rock fall detected by slide fence), PTC systems cannot prevent mechanical, track, or grade crossing accidents. Advances in hazard detection technology, however, should increase the number and types of hazard that can be detected reliably in real time. Detector alarms could warn train crews or stop a train via the PTC system.

Human factors accidents—accidents in which the event that triggers an accident is an error by train crew or other railroad operations employees—comprise about 20 percent of these mainline accidents, as shown in Table 3.

Approximately 20 percent of these human factors accidents are preventable by a full-function PTC system. Part of FRA's analysis of PTC costs and benefits included an extensive review of potentially PTC-preventable accidents. A team of reviewers representing railroad management and labor reviewed each accident description and determined whether PTC would or might prevent the accident, and which of four levels of PTC capabilities would be needed. This effort identified 752 accidents that would or might prevent an accident over the 14 years from 1988 to 2001, an average of 54 per year. Of these, about four accidents involved passenger trains, and four were non-human factors accidents caused by track or equipment faults detected by hazard detection systems.

Table 3. FRA-Reportable Human Factors Accidents 1997–2004

Year	Main Track Accidents	Siding Track Accidents	Total
1997	169	35	204
1998	195	42	237
1999	168	27	195
2000	215	44	259
2001	194	37	231
2002	195	34	229
2003	209	36	245
2004	209	38	248

The review team's interpretation of the preventability of accidents in this most recent effort was quite conservative. An earlier similar effort for the period 1988-1997 identified a total of 944 over 10 years for an average of 94 per year. This number, however, included a substantial number of rail and other track defects that might be detected by track circuits and other defect warning systems that were not included in the later review. Other areas where interpretation of accident preventability depends on the specific capabilities of individual PTC systems are accidents involving on-track work and inspection equipment that does not normally activate track circuits and the ability to detect wrongly aligned switches. The latter requires that the switch have a position sensor that communicates with the train control system.

The following are the principal causes of PTC-preventable human factors accidents (with corresponding FRA accident cause code):

- H215: Block signal–failure to comply (approximately 8 per year)
- H702: Switch improperly aligned (approximately 5 per year)
- H605: Failure to comply with restricted speed (approximately 4 per year)
- H216: Interlocking signal–failure to comply (approximately 3 per year)
- H204: Fixed signal–failure to comply (approximately 3 per year)

- H401: Failure to stop train in clear (approximately 3 per year)
- H404: Mandatory authority (track warrant, etc.)–failure to comply (approximately 3 per year)

Together these causes comprise more than half of all PTC-preventable accidents.

Based on these data, approximately 50-60 human factors accidents (as defined in the FRA reporting guide) are potentially preventable by universal application of PTC. Experience with traditional ATC suggests that well-designed train control systems do in fact prevent the majority of accidents they are designed to prevent. Very few examples of preventable accidents on ATC-equipped lines exist, and those that can be found usually have happened when part of the system was out of service. Existing systems are also vulnerable to many of the same kinds of workload/mode transitions as new technology PTC, and no obvious smoking gun exists to suggest that these transitions significantly reduce the effectiveness of ATC. Extensive service experience with traditional ATC exists, however, and the systems and procedures in place today are the result of long evolution. It is very possible that early experiences of workload/mode transition problems were later resolved.

In conclusion, the annual number of accidents where PTC-related workload/mode transitions could be a factor, and which could be mitigated by proper understanding of transition issues and application of countermeasures, is probably fewer than 10.

4.3. Railroad Accident Review

4.3.1 Summary of Review

The purposes of this review were to gain an understanding of the extent to which workload/mode transitions are a factor in past train accidents and to use this information to throw some light on how safety might be affected by PTC-related transitions.

By reviewing a total of 47 freight and 13 passenger PTC-preventable accidents, the research team has determined what causal factors contributed to the occurrences. The period covered by the accidents is 1996-2003 for the freight accidents and 1986-2003 for passenger accidents. Where the accident involved a collision between freight and passenger trains, the type of at-fault train was used in this analysis.

The primary sources for accident descriptions were National Transportation Safety Board reports and briefs on individual accidents, as well as material contained in FRA's accident files. Thus the sample only contains more serious accidents, usually involving one or more fatalities or serious injuries and substantial property damage.

4.3.2 Causal Factors

The approach to accident analysis involved identifying whether one or more causal factors contributed to the accident. This analysis was an attempt to go beyond the immediate event that triggered the accident (for example, passing a signal at danger) to look at situations that explained why that specific error was made by a particular individual at that place and time.

Table 4 shows the causal factors used to characterize accidents.

Table 4. Causal Factors for Accident Analysis

Descriptor	Abbreviation
Communication problems–failure to follow correct procedures, lack of effective procedures, defective equipment (e.g., radios)	Communications
Workload or workmode transition, or just high workload	WL/MT
Inexperience or lack of aptitude for job	Inexperience
Engineer or dispatcher lack of fitness for duty because of excessive fatigue, drug or alcohol abuse, or medical condition	Fitness
Inattentiveness with no other explanatory factors	Inattention
Loss of situational awareness or mistaken expectations	Expectations
Equipment failure or poor equipment design, either signal and train control or rolling stock	Equipment
Weather conditions, usually poor visibility	Weather
Distractions, usually of engineer	Distraction

The communications category was further subdivided by the apparent source of the problem—dispatcher errors and omissions, engineer errors and omissions, and equipment problems. In many cases, however, it was not possible from available information to determine where the communications problem lay or that multiple missteps in communications contributed to the accident.

4.3.3 Freight Train Accidents

Table 5 gives the occurrence of causal factors in order of the number of occurrences in the 47 freight train accidents reviewed. The figure in the percent column is the percentage of accidents in which the causal factor was present.

Table 5. Causal Factors in Freight Train Accidents

Causal Factor	Number	Percent of Total
Inexperience	22	47%
Communications (all)	18	38%
Dispatcher	4	9%
Engineer	4	9%
Equipment	1	2%
Other/unknown	9	19%
Fitness for duty	16	34%
Expectations, situation awareness	13	28%
Distraction	13	28%
Inattentiveness (no other explanation)	11	23%
Workload/mode transition	10	21%
Equipment design, condition	10	21%
Weather	10	21%

The review of the 47 accidents identified a total of 123 causal factors, showing that an average of 2.6 factors contributed to each accident. The following gives comments on each causal factor, starting with the most common.

Inexperience—22 occurrences. These typically involve engineers or dispatchers with limited experience, typically less than 2 years. This category also includes experienced operators or dispatchers who were unfamiliar with the territory, local operating practices, or the locomotive type. A few instances involve experienced individuals, but evidence shows a lack of aptitude (e.g., a previous history of accidents or rules violations) or a direct statement that the job demands made a particular individual nervous or stressed.

Communications—18 occurrences. These typically involve communications mixups between train crews, dispatchers, and operating employees in the field. Unreliable radio communications are sometimes a factor. In at least one case, the problem was a lack of proper communication among crewmembers in the cab—an experienced engineer failed to properly assist and instruct a student engineer when approaching a difficult-to-see signal. In about half the cases, it was not possible to determine where the error occurred; where it was possible, dispatchers and engineers appeared to be equally responsible.

Fitness for duty—16 occurrences. These events usually involve train crew who are sleep deprived or under the influence of alcohol or drugs. Fatigue seems to be the dominant factor, sometimes associated with a sharp change in personal routine (for example, a person just returned to work after illness or a vacation). A few instances of engineers' poor health or prescription medications affecting their on-the-job performance also exist.

Expectations/situation awareness—13 occurrences. These are somewhat similar to workmode transitions because an operator, almost always train crew, lost situational awareness and continued to operate a train on incorrect assumptions. The assumptions usually reflected the usual routine rather than a changed and unusual situation that prevailed on the day of the accident.

Distraction—13 occurrences. Mostly occasions where the operators, usually train crew, were distracted and missed a crucial signal. Some distraction events were workload-related (for example, missing a signal while attending to radio communications or a locomotive problem), as well as by non-essential activities, such as a personal cellphone call or just chatting with other cab occupants.

Inattentiveness—11 occurrences. These are accidents where the only explanation for the accident is inattention, with little or no evidence that other causal factors were involved.

Workload/mode transition—10 occurrences. These events all contain some elements of the transitions of interest, in that the individual responsible had to cope with either a change in workload or a change to a different and sometimes less familiar operating environment. The transitions are rarely the only causal factor but may have been the last straw that caused the accident. An example would be operating under direct traffic control or its equivalent after failure of line side signals, or a spike in workload (e.g., frequent radio communications), when approaching a terminal at the end of the shift. Expectation/situational awareness and distraction accidents are somewhat similar because both involve a change from normal routine or workload. In addition, experienced operators are much less likely to be adversely affected by such events.

Plant and equipment design or condition—10 occurrences. These are occasions where a technical problem with plant and equipment was a key factor in causing the accident, or where poor design or installation is involved. Problems with brakes (for example, failing to make proper brake tests) or poorly located signals that were difficult to see were notable factors.

Weather—10 occurrences. Common factors are poor visibility due to fog or falling snow and sun glare, both making it difficult to see signals and maintain proper awareness of train location.

To summarize, this analysis showed that workload/mode transitions were clearly a factor in about 20 percent of the accidents reviewed. If the definition of a transition is broadened to include loss of situational awareness and some of the distraction-related accidents, then transitions could be a factor in up to half of all accidents. In addition, it is clear from the analysis that the combination of a transition event and an inexperienced operator is especially hazardous. This latter situation arose in anecdote by David Nelson (of KKO and Associates) who, while working as a temporary dispatcher on a commuter rail line, had to cope with a disabled train in the morning rush. This situation produced a heavy workload, as well as a high risk, as trains were routed manually around the obstruction, running the wrong way on a line equipped with only automatic block signals.

4.3.4 Passenger Train Accidents

Table 6 gives the occurrence of causal factors in the 13 passenger train accidents included in the review.

Table 6. Causal Factors in Passenger Train Accidents

Causal Factor	Number	Percent of Total
Workload/mode transition	7	54%
Expectations/situation awareness	5	38%
Equipment	5	38%
Distraction	5	38%
Inexperience	4	31%
Fitness for duty	4	31%
Inattentiveness	4	31%
Communications	3	23%
Dispatcher	0	0%
Engineer	1	8%
Equipment	1	8%
Other/unknown	1	8%
Weather	0	0%

The mix of causal factors in passenger train accidents differs somewhat from those of freight train accidents, although the nature of the causal factor within each category is similar. Most of the differences can be related to the nature of passenger rail operations and the passenger rail work force. Inexperience is much less of an issue, perhaps reflecting a more senior workforce. Passenger operations are usually scheduled, highly predictable, and take place online equipped with central traffic control cab signals or ATC, greatly reducing the opportunities for communications errors. Workload and workmode transition problems, however, are more prominent, perhaps reflecting the difficulties of a workforce used to highly predictable operations might have in coping with non-routine events and the high level of disruption that would result from a disruption of high density operations.

In conclusion, the analysis suggests that workload/mode transitions are a factor in up to half of PTC-preventable accidents, and the combination of a transition event and an inexperienced operator is particularly hazardous.

5. Analysis of Potential Risks from Workload and Workmode Transitions

This section provides the analysis of the potential for risks from workload and workmode transitions associated with transitions in service in Section 5.2 and with transitions associated with failures in operation of the PTC system in Section 5.3.

5.1. Rating Scales Used in Analysis

Both analyses use qualitative ratings to assess the potential for the frequency of the conditions and the relative likelihood of the issue arising. The research team took this approach since (1) no established human reliability analysis (HRA) techniques exist for this particular type of application and (2) the use of these scales provides an adequate identification of where the greatest risks occur such that, if FRA wishes to consider specific situations and associated risks, they are suitably narrowly defined.

The following scales are used for the analysis.

Frequency of Type of Transition
F–Frequent: Typically once per shift or more
O–Occasional: Typically once per few shifts to once per month
R–Rarely occurs: Typically once per month or less

Risk
H–High: Clear opportunity for unsafe conditions to occur during the transition with a sufficiently high frequency to be of potential concern
M–Moderate: Opportunity for unsafe conditions exists under certain limited contexts within the transition, or the frequency of the occurrence is considered low despite the opportunity for unsafe conditions to occur
L–Low: Little or no opportunity for unsafe conditions to result

5.2. Risks from Transitions in Service

5.2.1 Evaluation

Table 7 presents the evaluation of risks from the transitions in service. For each type of transition, the authors identify the type (e.g., enter coverage), the frequency with which that transition is typically expected to occur using the scale above (Freq), and, for each issue of concern, the potential for risks (H, M, L) with a short rationale for the assignment. For those issues identified as being greater than low, an expanded discussion follows the table. Column headings for the issues are generally the same as the issues identified earlier: ‘Primary/BU’ identifies the primary/backup inversion issue.

Table 7. Risks from Transitions in Service

Transition	Freq	Complacency	Fixation	Skill Loss*	Primary/BU	Mode Error	Shift in Authority	Loss of Situational Awareness
Enter coverage	F	L–System will enforce safety	L–Possible spurious stop from not observing location	L–System will enforce safety	L–System will enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will enforce safety
Leave coverage	F	H–No enforcement when possibly expected	M–May not observe exit from coverage and over-rely on protection (mitigated by possible focus on the PTC display)	H–May not observe exit from coverage and over-rely on protection	H–May not observe exit from coverage and over-rely on protection	None for a single-mode (overlay) system	None for a single-mode (overlay) system	H–May not observe exit from coverage and over-rely on protection
Enter work zone	F	L–System will enforce safety	L–May get enforcement	L–System will enforce safety	L–System will enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–May get enforcement
Leave work zone	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety

Enter permanent speed restriction	F	L–System will enforce safety	L–System will enforce safety	L–System will enforce safety	L–System will enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will enforce safety
Leave permanent speed restriction	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Enter temporary speed restriction	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Leave temporary speed restriction	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Enter authorized territory/ track	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Leave authorized territory/ track	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety

Enter siding	F	M–No enforcement of siding speed rules (unmonitored switches)	M–May enter at excessive speed or against a wrongly set switch	M–May enter at excessive speed or against a wrongly set switch	M–May enter at excessive speed or against a wrongly set switch	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–May enter at excessive speed or against a wrongly set switch
Leave siding	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Enter restricted speed rule	F	M–Does not enforce all restricted speed rules (e.g., stop within half sight distance)	M–Does not enforce all restricted speed rules	M–Does not enforce all restricted speed rules	M–Does not enforce all restricted speed rules	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–Does not enforce all restricted speed rules
Leave restricted speed rule	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Receive directive from dispatcher	F	L–System will continue to enforce safety	M–May miss directive	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Report position	F	L–System will continue to enforce safety	M–May fail to report	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–May fail to report

Reach failed signal showing false stop	R	L–May get enforcement of stop, depending on cause of fault	L–May get enforcement of stop, depending on cause of fault	L–May get enforcement of stop, depending on cause of fault	L–May get enforcement of stop, depending on cause of fault	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–May get enforcement of stop, depending on cause of fault
Reach failed signal showing false proceed	R	M–May get enforcement of stop, depending on cause of fault	M–May get enforcement of stop, depending on cause of fault	M–May get enforcement of stop, depending on cause of fault	M–May get enforcement of stop, depending on cause of fault	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–May get enforcement of stop, depending on cause of fault
Suffer failed CTC system	R	L–System will continue to enforce safety	M–May fail to notice failure, but PTC system should enforce safety	L–May fail to operate within rules, but PTC system should enforce safety	L–May fail to operate within rules, but PTC system should enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–May fail to notice failure, but PTC system should enforce safety
Recover from failed CTC system	R	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
Suffer failed cab signaling system	R	L–System will continue to enforce safety	M–May fail to notice failure, but PTC system should enforce safety	L–May fail to operate within rules, but PTC system should enforce safety	L–May fail to operate within rules, but PTC system should enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–May fail to notice failure, but PTC system should enforce safety
Recover from failed cab signal system	R	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety

Receive detector warning	O	L–Unless engineer expects PTC to act on detector alarm	M–May miss warning	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–May miss warning
Start shift	F	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	L–System will continue to enforce safety	None for a single-mode (overlay) system	None for a single-mode (overlay) system	L–System will continue to enforce safety
End of shift	F	M–Fatigue may lead to over-reliance on PTC in above situations	M–Fatigue may lead to over-reliance on PTC in above situations	M–Fatigue may lead to over-reliance on PTC in above situations	M–Fatigue may lead to over-reliance on PTC in above situations	None for a single-mode (overlay) system	None for a single-mode (overlay) system	M–Fatigue may lead to over-reliance on PTC in above situations

* The potential exists for the engineer to apply braking in such a way that a risk of derailment exists from the concerns that the PTC penalty braking needs to be avoided, either because of its own conservative nature or the view that a PTC penalty brake application is a matter for disciplinary action.

Enforced or penalty braking is a major area of concern with PTC systems. In most PTC systems, penalty braking (usually full-service braking) initiates if, for example, the actual speed exceeds the speed defined by a built-in braking characteristic when approaching the limit of the train's authority. The characteristic is a function of train consist (number of locomotives and cars) and, with some systems, route characteristics like the gradient. Because train brake performance is quite variable, built-in braking characteristics tend to be conservative, forcing braking to be initiated earlier than would be normal practice without PTC. As well as possible disciplinary penalties for the train crew, initiating a penalty brake could cause a train handling accident, particularly under adverse curvature and grade conditions. A delay will also occur while the PTC system is re-set and brakes are released.

5.2.2 Analysis

The following scenarios exist as far as potentially significant contributors to risk of accidents.

5.2.2.1 High Risk

All the high-risk scenarios are associated with trains leaving PTC-covered territories (a transition that may occur one to several times in a single shift until widespread coverage of PTC systems is provided), without the crew understanding or accepting that protection is no longer provided.

- *Complacency* can simply lead to over-reliance on the PTC system to provide protection (or at least warnings to the crew) of upcoming potential hazards, such as interlockings, other trains, or workzones.
- *Skill loss* in this case refers to be equivalent of loss of situation assessment—that is, knowledge of the train's location in relation to the area of coverage of the PTC system with regards to the locomotive's location. Thus, traveling outside the area of coverage of the PTC system without realizing the absence of protection has the potential for train crews to be less vigilant—in a sense, this could be seen as a cause of the complacency problem (above). In principle, skill loss can result in poor train braking that could lead to derailment, and the poor train handling could be a result of trying to avoid a penalty brake when suddenly realizing that the PTC system is alarming.
- *Primary/Backup Reversal* refers to the possibility that train crews may come to regard the PTC system as an operational guide, acting almost as a cab signaling system rather than as an overlay protection system. Once the system is outside the area of coverage, the potential for guidance is lost.
- *Loss of Situation Assessment* is already covered in skill loss (above).

5.2.2.2 Moderate Risk

The table highlights three levels of moderate risk. These differ by the likely frequencies with which the types of transitions are likely to occur. The frequent transitions are sources of a higher risk than those where the frequency is occasional, which, in turn, are considered of greater risk than those that are rare.

<u>Frequent Transitions</u>

- *Leave coverage (fixation)* is only a moderate risk (unlike the other transitions when leaving coverage) because the fixation is on the PTC display; therefore, it is comparatively likely that the crew will observe that PTC is no longer providing coverage.
- *Enter siding (all transition issues)* is a moderate risk because PTC systems provide limited coverage for sidings. Any type of expectation or reliance due to complacency or skill loss of a protection function for the transition through the siding switches (such as speed reduction) would allow the likelihood of an

overspeed event with the possibility of derailment. In addition, should the switch have been wrongly set, no protection is provided for most of the siding switches that are not typically monitored by PTC systems.

- *Enter restricted speed rule (all transition issues)* is a moderate risk because PTC systems only provide partial coverage of the restricted speed rule—typically, PTC will enforce the maximum speed limit (15 mph) but cannot enforce the second component of the restricted speed rule, of being able to stop within half the distance visible from the cab. Therefore, over-reliance, or any other means by which train crews become distracted from handing the train, could lead to overspeeding (within terms of the stopping distance requirement), with the potential for collision.
- *Receive directive from dispatcher (fixation)* relates to directives from the dispatcher that may be missed by the train crew if they are fixated on the PTC system displays. While many of the directives may be enforced by the PTC system (such as taking away block authorizations under direct traffic control), some may not (for example, directing a train to take a siding).
- *Report position (fixation and loss of situation awareness)* relates to crews failing to report their positions, either because they have become fixated with the PTC system (especially if it is displaying error messages, for example) or if they have lost awareness of where they are (loss of situational awareness from preoccupation with the system). Failing to report positions (often over the road channel on the radio, for example) may lead others, such as roadway workers, not to be aware of the approaching train.
- *End of shift (all transitions)* may lead to an increased over-reliance on the PTC system as fatigue builds up at the end of the shift that, in turn, may lead to each of the failure types (fixation, skill loss scenarios, etc.).

<u>Transitions that Are Occasional</u>

- *Receive detector warning (fixation and loss of situation awareness)* represents the times when a train passes a hot-box detector and receives a warning of a fault. When the train crew is fixated on the PTC or has lost their situation awareness, it is possible they will miss the warning, and therefore the cause of the warning is not corrected. Depending on the particular cause, this failure may be a potential contributor to a derailment or damage to the track.

<u>Transitions that Are Rare</u>

- *Reach failed signal showing false proceed (all transition issues)* may result in the PTC preventing the train passing the signal, or it may not, depending on the cause of the failure. For most PTC systems, the train authority information comes through a radio signal from a link with the computer-aided dispatch system (CADS) or its equivalent. If, for some reason, a fault can occur upstream of the radio link that results in a false proceed signal, the PTC system will most likely receive the same false proceed information and not enforce a stop. Almost all the transition issues could lead to the train continuing past the faulty signal in this case. (It is recognized that a false stop is a more likely failure of signaling because of the fail-safe design of the vital components.)

- *Suffer failed CTC system or suffer failed cab signaling system (fixation and loss of situation awareness)* describes how a loss of coverage by non-PTC systems can lead to the possibility of the train crew attempting to continue as if the systems were operational, particularly if they are preoccupied with the PTC system (fixation) or loose track of where they are along the route (loss of situation awareness). While the PTC system should enforce the correct authorities at this point, the possibility exists that a PTC failure would then reduce the likelihood that the crew would stop and realize that the non-PTC system was not operational.

5.3. Risks from Failures in Operation of the PTC System

5.3.1 Evaluation

Table 8 provides the analysis of the risks from failures in operation of the PTC system. The format is generally the same as in Table 7, with the difference being that some equipment failures are deemed to be very rare—that is, the mean time between failures is in the order of greater than 6 months or so; these are identified as VR in Table 8. (The exact values for these failure rates are not known. These estimates are based on general knowledge of industrial electronic failure data, such as those published by the Institute of Electrical and Electronics Engineers (IEEE, 1977).)

The analysis in this section recognizes that the range of PTC systems can have a significant influence on the potential for human failures to occur. Most important is the extent to which the system is a primary system, necessary for normal control operations of the train (as with the NAJPTC System) versus the extent to which the system is an overlay system that only interacts with the train crew when it warns, and then may enforce, a penalty brake application. When the system is used in normal operations, the crew is much more likely to be aware of its condition (e.g., whether it is operational or failed, and whether the data are up-to-date). If the crew is aware of the failure, it is assumed that they will intend to follow the appropriate railroad rules concerning authority and speed limits, and entry into work zones. This analysis, however, recognizes that failures on the part of the crews can occur. The discussion in the next section for specific systems elaborates on this for specific combinations of failures and human issues (e.g., complacency) where appropriate.

In almost all cases, the authors' assumption is that the equipment failure will be a failure to function or a false stop, rather than a wrong side failure. That is, because of the design of the systems, almost all equipment failures will lead to a spurious enforcement or false alarm by the PTC system. Thus the concern is how the absence of the protection provided by the system will affect PTC users once it has been isolated after failure. This report is not primarily concerned with wrong side failures, where the crew expects the protection to work, but it is, in fact, failed. Such failures will be very rare (by design) and should not contribute to any increase in risk.

An additional type of failure beyond the equipment faults considered here is the possibility of incorrect data being entered in the PTC system. For example, some systems require the train crew to enter consist data (for example, in the CBTM system, the consist data affects the braking algorithms) or obtain consist data from other databases that may be in error. While such failures can occur, they do not contribute to the kinds of workload and workmode issues raised in this analysis.

5.3.2 Analysis

5.3.2.1 High Risk

Other onboard failure (complacency)—This failure represents the possibility that, following the initial failure (other than a communications system failure, see Table 8), the crew will isolate the PTC system and then forget that its protection is no longer provided. The likelihood of this failure is very dependent on the location and salience of the display for the crew. For example, in the current design of the CBTM system, the display is located well away from the normal view of the engineer or the conductor. The proposed new display would be located directly in the engineer's view and possibly less likely to be forgotten. Other systems typically have displays more in line with the engineer's vision, though they often depend on a single light to indicate if the system is in service. The more reliable the system, the more likely it will be that people forget it is not working following a failure.

5.3.2.2 Medium Risk

<u>Rare Failures</u>

- *Other onboard failure (fixation)*—This condition represents the case where a failure occurs and is detected by the train crew, who then become preoccupied with trying to diagnose and recover operation of the system. For those PTC systems that use prominent computer displays (principally NAJPTC and the proposed new CBTM systems), the possibility of extensive error messages have the potential for creating a significant distraction. Those systems that use simple light displays or a few characters (e.g., ASES and ITCS) indicating the status of the system will likely be less prone to this problem.
- *Other onboard failure (loss of situation awareness)*—This condition could result from when the train crew has been relying on the PTC system as a position identifier or speed limit reminder, and, after the system has failed and been isolated, they lose the continued awareness of their location or speed. Again, this is more likely with the systems that provide more extensive information, though it is likely that associated displays (for example, with the NAJPTC System) would present salient information about the system being failed.

Table 8. Risks from Failures in Operation of PTC Systems

Subsystem/ Component Failure	**Est Freq**	**Complacency**	**Fixation**	**Skill Loss***	**Primary/BU**	**Mode Error**	**Shift in Authority**	**Loss of Situation Awareness**
Onboard communic-ations receiver	VR	M–System will enforce last received authority until isolated by crew. Possibility exists for crew to forget that coverage no longer provided	M–Possibility exists that crews will become distracted in trying to recover functionality	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory

Other onboard failure	R	H–Loss of coverage, possibly with spurious penalty brake on device failure (depends on design). Possibility exists for crew to forget that coverage no longer provided following system isolation	M–Possibility exists that crews will become distracted in trying to recover functionality	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	M–If the system fails simply by showing no information, the possibility exists that the engineer, after having relied on the system to warn him (e.g., of boundaries) in bad weather, is now provided with no information
Loss of communications with wayside device	R	L–Loss of coverage for failed device. May get enforcement or alarms on approach to failed device	L–Possibility exists that crews will become distracted in trying to recover functionality	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory

Zone controller	VR	M–System will enforce last received authority until isolated by crew. Possibility exists for crew to forget that coverage no longer provided	L–Possibility exists that crews will become distracted in trying to recover functionality	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory	L–System will behave as if it is outside covered territory

Very Rare Failures

- *Onboard communications receiver (complacency)*—If the communications system is no longer receiving updates from the CADS (the assumed failure mode here), it is most probable that the PTC system will simply enforce the latest information it has received. Once the locomotive is outside the area that was protected by the system, it is possible that the crew will forget that protection is no longer provided. This is perhaps more of a concern with speed limits than authorities since it is likely that when the train reached the limit of its stored authority the system, not having been updated with new authorities, will enforce a penalty brake. It would be possible, however, for the train to enter a more restricted speed area after the failure but before reaching the end of its stored authority.
- *Onboard communications receiver (fixation)*—As with the earlier fixation failures, it is possible that the train crew will become preoccupied with trying to diagnose and restore the failed devices to operation.
- *Zone controller (complacency)*—Failure of the zone controller could lead to similar conditions as the failure of the onboard communications receiver (above), whereby the train crew fails to keep in mind the failed state of the PTC system and continues to rely on it for protection.

6. Summary

This work has demonstrated that the potential does exist for workload and workmode transitions to occur in the use of PTC systems and that these transitions do have the potential for contributing to the risks of accidents. This risk, however, is probably small when compared with the overall benefits of PTC systems. This is particularly noteworthy since many of the current types of train accidents are the result of workload and workmode transitions, as shown in Section 4.

The risks associated with workload and workmode transitions when using PTC systems can occur in two different conditions: when the PTC system is working normally and when failures in the PTC equipment occur.

When the PTC system is working normally, the dominant risk is the potential for human errors when the locomotive leaves the area covered by the PTC system. The possible failures that can occur include the following:

- *Complacency*, where the train crew has become over-reliant on the protection provided by PTC and simply forget that coverage is no longer being provided.
- *Skill loss*, where the train crew has lost some of the knowledge (speed limits, boundary limits, etc.) that are essential to safe handling of the train as a result of relying on the PTC system.
- *Primary/backup reversal*, where the crew look to use the PTC system as a normal information system (such as providing current location, indications of speed limits, etc.).

When failures in operation of the PTC system are considered, only one scenario creates the possibility of a high risk:

- *Complacency following failures of the onboard equipment*, where the crew, having isolated the system following its failure, now forgets that coverage by the system is no longer available.

While quite varied types of PTC systems are under development, two types exist whose potential for risks appear quite different—those systems that provide only a backup, or overlay, type of protection and those whose operation is a normal part of locomotive operations. A typical version of the overlay PTC system is the original CBTM system, where the PTC system is almost out of sight of the train crew by design, and only interacts with the locomotive engineer when approaching a condition that could result in a penalty brake. (CSX is reportedly undertaking design modifications that may lead the PTC display to be integrated into the engineer’s normal displays, but these have not been observed.) In contrast, the NAJPTC System has an integrated display that is necessary for high-speed operations and is one of the primary displays for the engineer in normal operations.

The opportunities for the high risk failures above is much greater with the systems that provide an overlay function and are virtually out of sight during normal operations. This is because the primary risks are associated with people's awareness of the system operating state being diminished and the tendencies of people to rely, in various ways, on equipment that is normally functioning and forget that it is inoperative. The more prominent the displays are about the status of the system, the less likely they are to forget that it is inoperable.

7. References

Billings, C. E. (1991). *Human-centered aircraft automation: A concept and guidelines* (No. NASA Technical Memorandum 103885). Moffett Field, CA: NASA-Ames Research Center.

Billings, C. E. (1996). *Aviation automation: The search for a human-centered approach*. Mahwah, NJ: Erlbaum.

Christoffersen, K., & Woods, D. D. (2002). How to make automated systems team players. In E. Salas (Ed.), *Advances in human performance and cognitive engineering research* (Vol. 2, pp 1-12). New York, NY: Elsevier Science.

Cook, R. I., & Woods, D. D. (1996a). Adapting to new technology in the operating room. *Human Factors, 38*, 593-613.

Cook, R. I., & Woods, D. D. (1996b). Implications for automation surprises in aviation for the future of total intravenous anesthesia (TIVA). *Journal of Clinical Anesthesia, 8,* 29s-37s.

Cook, R. I., Woods, D. D., McColligan, E., & Howie, M. B. (1991). Cognitive consequences of “clumsy” automation on high workload, high consequence human performance. In R. T. Savely (Ed.), *Fourth Annual Workshop on Space Operations, Applications and Research (SOAR '90) (NASA Report CP-3103).* Washington, DC: NASA.

DeKeyser, V., & Woods, D. D. (1990). Fixation errors: Failures to revise situation assessment in dynamic and risky systems. In A. G. Colombo & A. Saiz de Bustamante (Eds.), *System reliability assessment*. Dordrecht, The Netherlands: Kluwer Academic.

Dekker, S. W. A., & Hollnagel, E. (Eds.). (1999). *Coping with computers in the cockpit*. Aldershot, UK: Ashgate.

Dekker, S. W. A., & Woods, D. D. (1999). To intervene or not to intevene: The dilemma of management by exception. *Cognition, Technology and Work, 1*, 86-96.

Endsley, M. R., & Kiris, E. O. (1995). The out-of-the-loop performance problem and level of control in automation. *Human Factors, 37*, 381-394.

Ephrath, A. R., & Young, L. R. (1981). Monitoring versus man-in-the-loop detection of aircraft control failures. In J. Rasmussen & W. B. Rouse (Eds.), *Human detection and diagnosis of system failures*. New York, NY: Plenum.

Fitts, P. M. (1951). Engineering psychology and equipment design. In S. S. Stevens (Ed.), *Handbook of experimental psychology*. New York, NY: Wiley.

Gentner, D., & Stevens, A. L. (Eds.). (1983). *Mental models*. Hillsdale, NJ: Erlbaum.

Guerlain, S., Smith, P. J., Obradovich, J., Heintz, J., Rudmann, S., Strohm, P., et al. (1999). Interactive critiquing as a form of decision support: An empirical evaluation. *Human Factors, 41*(72-89).

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM)*. New York: Elsevier Science, Inc.

Huey, B. M., & Wickens, C. D. (Eds.). (1993). *Workload transitions: Implications for individual and team performance*. Washington, DC: National Academy of Science.

Hutchins, E. E. (1995). *Cognition in the wild*. Cambridge, MA: MIT Press.

IEEE. (1977). *IEEE guide to the collection and presentation of electrical, electronic, and sensing component reliability data for nuclear power generating stations, IEEE Std 500*. New York, NY: Institute of Electrical & Electronics Engineers.

Layton, C., Smith, P. J., & McCoy, E. (1994). Design of a cooperative problem-solving system for enroute flight planning: An empirical evaluation. *Human Factors, 36*, 94-119.

Malin, J. T., Schreckenghost, D. L., Woods, D. D., Potter, S. S., Johannesen, L., Holloway, M., et al. (1991). *Making intelligent systems team players: Case studies and design issues*. Houston, TX: NASA Johnson Space Center.

Moray, N., Inagaki, T., & Itoh, M. (2000). Adaptive automation, trust & self-confidence in fault management of time-critical tasks. *Journal of Experimental Psychology, Applied, 6*(1), 44-58.

Mumaw, R. J., Roth, E. M., Vicente, K. J., & Burns, C. M. (2000). There is more to monitoring a nuclear power plant than meets the eye. *Human Factors, 42*(1), 36-55.

Norman, D. A. (1981). Categorization of action slips. *Psychological Review, 88*, 1-15.

NTSB. (1996). *Collision of Washington Metropolitan Area Transit Authority train T-111 with standing train at Shady Grove passenger station, Gaithersburg, Maryland, January 6, 1996.* (Railroad Accident Report 96/04). Washington, DC: National Transportation Safety Board.

Obradovich, J., & Woods, D. D. (1996). Users as designers: How people cope with poor HCI design in computer-based medical devices. *Human Factors*, 38, 574-592.

Parasuraman, R., Bahri, T., Deaton, J., Morrison, J., & Barnes, M. (1997). Alarm effectiveness in driver-centered collision-warning systems. *Ergonomics, 40*, 390-399.

Parasuraman, R., Molloy, R., & Singh, I. (1993). Performance consequences of automation-induced “complacency.” *International Journal of Aviation Psychology, 3*(1), 1-23.

Parasuraman, R., Mouloua, M., & Molloy, R. (1996). Effects of adaptive task allocation on monitoring of automated systems. *Human Factors, 38*(665-679).

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics–Part A: Systems and Humans, 30*(3), 286-297.

Perkins, D., & Martin, F. (1986). Fragile knowledge and neglected strategies in novice programmers. In E. Soloway & S. Iyengar (Eds.), *Empirical studies of programmers*. Norwood, NJ: Ablex.

Reason, J. (1990). *Human error*. New York, NY: Cambridge University Press.

Rose, A. M. (1989). Acquisition and retention of skills. In G. R. McMillan (Ed.), *Application of human performance models to system design*. New York, NY: Plenum Press.

Sarter, N. B., & Amalberti, R. (Eds.). (2000). *Cognitive engineering in the aviation domain*. Mahwah, NJ: Erlbaum.

Sarter, N. B., & Woods, D. D. (1994). Pilot interaction with cockpit automation II: An experimental study of pilots’ mental model and awareness of the Flight Management System (FMS). *International Journal of Aviation Psychology, 4*(1), 1-2.

Sarter, N. B., Woods, D. D., & Billings, C. E. (1997). Automation surprises. In G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (2nd ed.). New York, NY: Wiley.

Sheridan, T. B., Gamst, F. C., & Harvey, R. A. (1999). *Reliance and distraction effects in PTC automation* (White Paper No. STD-PTC-DEC-02-99). Cambridge, MA: John A. Volpe National Transportation Systems Center.

Sheridan, T. B., & Verplank, W. L. (1978). *Human and computer control of undersea teleoperators* (Technical report). Cambridge, MA: Man-Machine Systems Laboratory, Department of Mechanical Engineering, Massachusetts Institute of Technology.

Smith, P., Woods, D. D., McCoy, E., Billings, C. E., Sarter, N. B., Denning, R., et al. (1998). Using forecasts of future incidents to evaluate future ATM system designs. *Air Traffic Control Quarterly, 6*(1), 71-85.

Sogame, H., & Ladkin, P. (1996). *Aircraft Accident Investigation Report 96-5. China Airlines Airbus Industrie A300B4-622R, B1816, Nagoya Airport, April 26, 1994 [On-line* *version at http://sunnyday.mit.edu/accidents/nag-contents.html]*. Tokyo, Japan: Aircraft Accident Investigation Commission, Ministry of Transport, Japan.

Wickens, C. D. (Ed.). (1998). *The future of air traffic control: Human operators and automation*. Washington, DC: National Academy Press.

Wickens, C. D., & Kessel, C. (1979). The effects of participatory mode and task workload on the detection of dynamic system failures. *IEEE Transactions on Systems, Man and Cybernetics, SMC-9*, 24-34.

Wickens, C. D., & Kessel, C. (1981). Failure detection in dynamic systems. In J. Rasmussen & W. B. Rouse (Eds.), *Human detection and diagnosis of system failures*. New York, NY: Plenum.

Wiener, E. L. (1988). Cockpit automation. In E. L. Wiener & D. C. Nagel (Eds.), *Human factors in aviation*. San Diego, CA: Academic Press.

Wiener, E. L., & Curry, R. E. (1980). Flight-deck automation: Promises and pitfalls. *Ergonomics, 23*, 995-1011.

Woods, D. D. (1988). Coping with complexity: The psychology of human behavior in complex systems. In L. P. Goodstein, H. P. Andersen & S. E. Olsen (Eds.), *Tasks, errors and mental models*. New York, NY: Taylor & Francis.

Woods, D. D. (1996). Decomposing automation: Apparent simplicity, real complexity. In R. Parasuraman & M. Mouloua (Eds.), *Automation and human performance: Theory and applications*. Mahwah, NJ: Erlbaum.

Woods, D. D. (2002). *Steering the reverberations of technology change on fields of practice: Laws that govern cognitive work (Plenary Address).* Paper presented at the 24th Annual Meeting of the Cognitive Science Society, Fairfax, VA.

Woods, D. D. (2003). Discovering how distributed cognitive systems work. In E. Hollnagel (Ed.), *Handbook of cognitive task design*: Erlbaum.

Woods, D. D., Johannesen, L., Cook, R. I., & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers, and hindsight*. Dayton, OH: Crew Systems Ergonomic Information and Analysis Center, WPAFB.

Woods, D. D., & Tinapple, D. (1999). *W3: Watching human factors watch people at work. Presidential Address, 43rd Annual Meeting of the Human Factors and Ergonomics Society, September 28, 1999*, from http://csel.eng.ohio-state.edu/hf99/.

Woods, D. D., Tittle, J., Feil, M., & Roesler, A. (2004). Envisioning human-robot coordination for future operations. *IEEE Transactions on Systems, Man and Cybernetics, 34*, 210-219.

Wreathall, J., Roth, E., Bley, D. C., & Multer, J. (2003). *Human reliability analysis in support of risk assessment for positive train control* (DOT/FRA/ORD-03/15). Cambridge, MA: U.S. Department of Transportation, John A. Volpe National Transportation Systems Center.

Acronyms

ASES	advanced speed enforcement system
ATC	automatic train control
ATP	automatic train protection
ATS	automatic train stop
CBTM	communications-based train management
CTC	central traffic control
FRA	Federal Railroad Administration
GPS	global positioning system
HRA	human reliability analysis
ITCS	incremental train control system
NAJPTC	North American Joint Positive Train Control
PTC	positive train control
RAIRS	railroad accident/incident reporting system