Journal of King Saud University – Science (2011) **23**, 311–321

King Saud University
Journal of King Saud University – Science
www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Positive Train Control (PTC) failure modes [☆]

Mark Hartong [a,*], Rajni Goel [b,1], Duminda Wijesekera [c,2]

[a] *Federal Railroad Administration, 1200 New Jersey Ave SE, Washington, DC 20590, United States*
[b] *Howard University, Information Systems and Decision Sciences, School of Business, 2600 6th Street, Washington, DC, United States*
[c] *George Mason University, Department of Computer Science, MS 4A4, 100 University Drive, Fairfax, VA 22030, United States*

Received 14 September 2010; accepted 18 December 2010
Available online 25 December 2010

KEYWORDS
Railroad;
Positive Train Control;
Safety;
Risk Analysis;
Failure Modes

Abstract Positive Train Control (PTC) systems can eliminate the consequences of collision or derailment. However, prior to the full-scale deployment of these systems, the Federal Government must conduct a regulatory review and approve the risk analysis of the PTC system performance. The objective of this review is to ensure that the operating environment after installation of the PTC system is at least as safe as the operating environment before the system installation. This paper is intended to provide researchers an understanding of PTC, the reason for its use, the regulatory requirements for the required comparative risk analysis of the PTC system, the critical failure modes that the comparative analysis must address, and future work that would facilitate the risk assessment process.

1. Introduction

Rail operations are ubiquitous throughout the United States. They operate in every state in the US except Hawaii, across a network that exceeds 140,000 miles (BTS, 2003). The 559 freight railroads move over 1.7 trillion ton miles of freight (AAR, 2007). The 22 commuter railroads alone move 1.4 million people daily (APTA, 2007) and the Amtrak intercity passenger service adds over 75,000 more (BTS, 2008).

Failures in existing methods of rail operations can have catastrophic consequences. On September 13, 2008, for example, a safety violation known as a "Signal Passed at Danger (SPAD)" resulted in a collision between a Union Pacific freight train and a METROLINK commuter train, which occurred in Chatsworth, California (Melago, 2008). This collision resulted in the death of 26 people and injuries to 135 more. Another SPAD in Macadona, Texas in June 2004 resulted in 3 deaths and 30 injured when a BNSF freight train and a Union Pacific

---

[☆] The views and opinions expressed herein are that of the authors and do not necessarily state or reflect those of the United States Government, the Department of Transportation, or the Federal Railroad Administration, and shall not be used for advertising or product endorsement.

[*] Corresponding author. Tel.: +1 202 493 1332; fax: +1 202 493 6478.

E-mail addresses: mark.hartong@dot.gov (M. Hartong), rgoel@howard.edu (R. Goel), dwijesek@gmu.edu (D. Wijesekera).

[1] Tel.: +1 202 806 1649; fax: +1 202 797 6393.

[2] Tel.: +1 703 993 1578; fax: +1 703 993 1638.

Peer review under responsibility of King Saud University.
doi:10.1016/j.jksus.2010.12.003

Production and hosting by Elsevier

freight train collided (NTSB, 2006). A failure of a train crew to correctly line a switch in January 2005 in Graniteville, South Carolina resulted in a collision between two Norfolk Southern freight trains. The collision and subsequent release of chlorine gas caused the death of 9 people, injury to an additional 554, and the evacuation of 5400 for a period of 2 weeks (NTSB, 2005). All of these accidents, and the associated casualties, could have been prevented had a Positive Train Control (PTC) system been installed and operational.

Prior to a US railroad installing and operating a PTC system, the railroad must receive regulatory approval from the Federal Railroad Administration (FRA) of the US Department of Transportation (DOT). As part of that approval process, the PTC system must undergo a comprehensive risk analysis of its failure modes. The regulatory review and approval process is complicated by the fact that there is no formal specification of the failure modes that must be addressed in the risk analysis. Consequently each individual railroad specifies its own failure modes, and in the process may not address the critical issues of regulatory concern, or may address them in such a manner that is not clearly understood by the regulatory agency. In either case, the regulatory review process is extended in order to resolve these misunderstanding, adding both to the cost of the system approval process, as well as delaying the implementation of systems. This paper proposes an open common specification of critical failure modes that must be addressed when preparing the required failure analysis for regulatory review. Not only does it aid in preparing the required failure analysis, but also provides a mechanism for allowing the regulator to more effectively evaluate the risks associated with different proposed PTC system implementations.

This paper proceeds as follows. In Section 2, we will discuss current methods of rail operations, and their limitations, to establish a context for the development of PTC systems. Section 3 will discuss PTC systems, their functionality, and how it can augment or replace existing methods of operation. Section 4 will discuss the regulatory framework in which PTC systems are installed. Section 5 discusses related work as well as the proposed general failure mode model associated with PTC, which can adversely affect system safety in terms of Functional Fault Trees (FFT). Finally, Section 6 summarizes the preceding chapters and outlines future work we believe necessary to relate an FFT to the more natural language Use and Misuse Case descriptions of system behavior and failure modes.

2. Existing methods of operations and limitations

Existing methods of operations for the control of trains can be classified into four basic categories:

- verbal authority,
- mandatory directives,
- signal indications, and
- signal indications supplemented by cab signals, automatic train control, or automatic train stop systems.

When using verbal authority and mandatory directives, the aspects of wayside signals along the railroad do not control train operations. Instead, train operations are controlled by orders from the Train Dispatcher, who takes responsibility for knowing what trains are located where, and ensures that no two trains are issued authority to occupy the same location of track at the same time. The Dispatcher usually issues orders, mandatory directives, speed restrictions, as well as the location of any wayside work crew via two-way radio to the locomotive crew. The train crew are responsible for ensuring that they obey these orders, speed restrictions, and advisories. This is the traditional means of controlling operations in the United States, and roughly 40% of all tracks in the United States are controlled in this manner.

Train operations under signal indications constitute the remainder of the train control operations in the US. Track circuit based signal systems were first installed in the US in 1872, and by 1927 they were centrally controlled in the first "Centralized Traffic Control (CTC)" system and have remained basically unchanged since the 1930s. In CTC, authority for train movements is provided by signal indications. The train dispatcher at the control center determines train routes and priorities, and then remotely operates switches and signals to direct the movement of trains. Some CTC systems have been enhanced to provide direct indications of wayside signal aspects to the locomotive engineer inside the locomotive cab. Signal aspect is the appearance of the signal, as opposed to a signal indication, which is the information conveyed by the appearance of the signal. Further refinements called "Automatic Train Stop (ATS)" or "Automatic Train Control (ATC)" automatically cause the train to stop or reduce speed where an engineer fails to acknowledge a wayside signal.

Cab signals simply relay the external signal indications to a visual display inside the cab of the locomotive, making it easier for the crew to note the signal aspect and the associated order it conveys. Unless operated with ATS or ATC, the cab signal systems do not provide speed or authority enforcement. This approach has several significant technical limitations. First, the location of trains can only be determined by the resolution of a track circuit. If any part of a track circuit is occupied, that entire track circuit must be assumed as occupied. The track circuit's length can be made shorter, but adding additional track circuits requires additional wayside hardware. This imposes additional costs, causing a practical (and economical) limit to the number of track circuits that a railroad can install. Second, the information that can be provided to a train through a rail-based system is limited to a small number of wayside signal aspects or speed data.

In addition, the underlying signal systems to provide the required indications for cab, ATS, or ATC to operate are capital intensive. In 2003, the Class 1 railroads alone spent over $490 million in operation, administration, and maintenance of all types of communications and signaling systems with another $153 million in deprecation of the existing plant on approximately 65,000 miles of track (HR, 2003; STB, 2003). Consequently the deployment of these technologies is limited to those areas where rail throughput needs to be maximized. Less than 5% of route-miles in the US have systems in place, where signal indications are shown in the locomotive cab, on-board enforcement of the signal indications, or both (BTS, 2003).

At best, these traditional methods of train control provide for reactive enforcement of unauthorized train movements after a movement violation has occurred. The inability of cab signals, ATS, and ATC to effectively incorporate collision and accident avoidance measures with the current methods of operations has been the primary motivation for the US