Designing Highly Automated Safety-Critical Railway System and its Organization

by

Ryo Odajima

M.S. in Integrated Design Engineering, Keio University, 2012
B.E. in System Design Engineering, Keio University, 2010

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2019

© 2019 Ryo Odajima. All rights reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature of Author: _____

Ryo Odajima
System Design and Management Program
May 7, 2019

Certified by: _____

John P. Thomas
Research Engineer, Department of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: _____

Joan S. Rubin
Executive Director
System Design and Management Program

Designing Highly Automated Safety-Critical Railway System and its Organization

by

Ryo Odajima

Submitted to the System Design and Management Program on May 7, 2019
in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Engineering and Management

ABSTRACT

High-speed rail (HSR) has improved dramatically since its launch in 1964 in terms of its technical aspects such as speed and reliability, thanks to technical developments including the automation of the train operation. At the same time, safety has become an increasingly critical aspect as the severity of the accidents has become much more severe. Although the automation and newly developed software might have decreased the number of accidents that would not have been prevented without them, they also have introduced new types of hazards and accidents that did not exist before due to the increased level of complexity of the whole system. These hazards include system design errors, component interactions accidents, or software-related errors due to the increased number of interfaces and coordination among internal and external stakeholders and higher dependency on automation and software. Thus eliminating component failures should not be the only design consideration or priority, and more consideration should be given to eliminating coordination or design errors that would not be solved by redundancy for the sake of reliability improvement.

This thesis mainly focuses on analyzing the past accidents caused by systematic failures and provides recommendations and considerations for designing and operating highly automated complex safety-critical railway systems. Often, the accident analysis finishes once someone is found to be responsible, but this thesis focuses on figuring out why they behaved that way by using the STAMP framework, which is based on systems theory, documenting the systemic factors which contributed to the accidents. The analysis thus looks into not only physical systems but also organizational aspects, such as management, organization culture, and other social-technical aspects.

Two accident analyses revealed causal factors on every level of the organization, including policy makers, audit authority, management, human operators and engineers, physical systems, and so on. In addition, the analyses provide the conceptual explanation of how the systems migrate into an unsafe state over time. The set of knowledge learned through the analyses is summarized as 35 lessons learned. These lessons are of use for future considerations in designing highly-automated safety-critical railway systems and their organization.

Thesis Supervisor: John P. Thomas
Title: Research Engineer, Department of Aeronautics and Astronautics

(This page intentionally left blank)

ACKNOWLEDGEMENTS

In late Summer, 2014, in Shizuoka, Japan, I decided to go study abroad. At that time, I did not imagine that I would finally make it to the best place in the world to learn engineering and management as a young engineer. The process was harsh, however, and sincere help, especially from my employer and my family members, were integral parts of the success in achieving the goal.

MIT System Design and Management Program, which I finally joined in 2017, was filled with the intellectual and mindful people and the harsh but meaningful set of events. This was what I wanted to experience and be involved, but was far beyond my expectation for sure.

Here, I want to use this space to say thank you to people I got the special supports throughout my journey from Shizuoka to Cambridge.

First, thank you, my thesis advisor, John. When I first listen to your lecture in Spring 2018, I was surprised how insightful your lecture was. Soon after that, I decided to ask you to help me through my thesis work. Thank you to kindly accept my offer, and have given me a lot of insightful technical advises even in a hectic schedule. Your explanations were always clear and understandable, having made it easy for me to follow your advice.

Second, I would like to say thank you to my employer, Central Japan Railway Company, my supervisors, and professors in my school to give me a chance and tremendous supports to go study in MIT. I could not have even set such a dreamy goal without you.

Third, thank you SDM staffs, to give me intellectual and fun opportunities, starting from the SDM boot-camp in August 2017, to the final presentation of spring projects in 2018. The “system” you provided has really broadened my view and given me the confidence to navigate through my future career. Also, thank you SDM friends and people I interacted in classes, team projects, and any other occasions. You all made my life in MIT and Cambridge/Boston vibrant and fun.

Fourth, thank you my parents-in-law, grandmother-in-law, my mother, and my grandmother, for supporting us in every aspect, especially budgetary and parenting supports through the two years of the oversea life. We could not make it to this point without your help.

Fifth, thank you CBNS staffs to give Aoi a great opportunity to learn, play, and enjoy the activities you prepared. We are very lucky to get help from such mindful people.

Lastly, thank you, my dearest wife, Nakaha. You have been supporting me throughout this journey from Shizuoka to MIT. From the beginning, you were very supportive and always sacrificed yourself to give me time to prepare for studying abroad. Through this 5-year-long-journey, you gave birth to Aoi, and still have been supporting my work and study, while taking care of her. There is no question that I could not have been here without you. I cannot say thank you enough for your hard work. Also, thank you, my lovely daughter, Aoi. Your rapid and healthy growth made me always happy and surprised, giving me the extra energy to navigate through this journey.

Ryo Odajima
Cambridge, Massachusetts, April 2019

(This page intentionally left blank)

TABLE OF CONTENTS

TABLE OF CONTENTS 6

LIST OF TABLES 11

LIST OF FIGURES 13

LIST OF ACRONYMS AND ABBREVIATIONS 16

Chapter 1 Introduction 20

1.1 Motivation 20

1.1.1 Accidents related to Automated Systems 20

1.1.2 New Accident Analysis Technique 22

1.1.3 Development of HSR and Japanese SC-MAGLEV 22

1.2 Research Objectives 25

1.3 Research Methodology 25

1.4 Thesis Scope 26

1.5 Thesis Outline 26

Chapter 2 STAMP (System-Theoretic Accident Model and Processes) 29

2.1 Introduction – Why Do We Need Something Different? 30

2.2 Increased Complexity 32

2.3 Coping with Complexity 33

2.3.1 Analytical Decomposition (the traditional approach) 33

2.3.2 Systems Theory 39

2.4 STAMP (System-Theoretic Accident Model and Processes) Model 43

2.4.1 The Goal of CAST [6, Ch. 11] 44

2.4.2 General Steps of CAST [6, Ch. 11] 44

2.5 Conclusion 45

Chapter 3 CAST Analysis 1 – WMATA Accident in 2009 47

3.1 Summary of the accident 47

3.2 Washington Metropolitan Area Transit Authority (WMATA) 51
3.2.1 History and its Mission *51*
3.2.2 Financing System and Board Responsibilities *51*
3.2.3 Current Operation Information *52*
3.3 System Definition & Hazards 53
3.4 Safety Constraints and System Requirements Associated with Hazards 56
3.5 Safety Control Structure 56
3.6 Proximal Event Chain Leading to the Loss 65
3.6.1 Proximal Event Chain *65*
3.6.2 The responsibilities of ATP system and how it works *70*
3.6.3 How ATP system became incapable of detection *74*
3.7 Analyzing the Physical Process 75
3.8 Analyzing the Higher Levels of the Safety Control Structure 79
3.8.1 Operator-Physical System Level *79*
3.8.2 ATC Engineers-Physical System Level *97*
3.8.3 Upper Management, and Governmental and Audit Agencies Level *112*
3.9 Examining how Coordination and communication contributed to the Loss 123
3.10 Dynamics and Migration to a High-Risk State 124
3.10.1 Degradation of safety culture *124*
3.10.2 Degradation of Infrastructure *125*
3.10.3 Degradation of Safety *125*
3.10.4 Combining the Loops together: Multiplier Effects *125*
3.10.5 Policy Resistance: Investment on expansion over on safety *126*
3.10.6 Chronic problems are nearly irreversible in the short span *126*
3.11 Reviewing and Revealing the Weakness of Safety Control Structure 127
3.12 Generating Recommendations 132
3.13 Conclusion 136
Chapter 4 CAST Analysis 2 – Amtrak Derailment in 2015 139
4.1 Summary of the accident 140

4.2 The National Railroad Passenger Corporation (Amtrak) 142
4.2.1 History and its Mission *142*
4.2.2 Financing System and Board Members *143*
4.2.3 Current Operation Information *144*
4.3 Train Control Systems on the Northeast Corridor (NEC) 151
4.3.1 Train Control System Overview *151*
4.3.2 Positive Train Control Legislation - Railroad Safety Improvement Act *156*
4.3.3 Overview of Positive Control System Requirements set by RSIA08 ..... *157*
4.3.4 PTC on the NEC *157*
4.4 System Definition & Hazards 162
4.5 Safety Constraints and System Requirements Associated with Hazards 163
4.6 Safety Control Structure 163
4.7 Proximal Event Chain Leading to the Loss 172
4.8 Analyzing the Physical Process 174
4.9 Analyzing the Higher Levels of the Safety Control Structure 176
4.9.1 Signal and Train Control System Level *176*
4.9.2 Front-Line Human Controller Level *182*
4.9.3 Amtrak Management Level *192*
4.9.4 Governmental and Audit Organizations Level *206*
4.10 Examining how Coordination and communication contributed the Loss 212
4.11 Dynamics and Migration to a High-Risk State 213
4.11.1 Declining public utilization of railroad and government interest *213*
4.11.2 Aging Infrastructure *216*
4.11.3 Others *217*
4.12 Reviewing and Revealing the Weakness of Safety Control Structure 217
4.13 Questions Unanswered in the NTSB Accident Report 223
4.14 Generating Recommendations 223
4.15 Conclusion 227
Chapter 5 Lessons Learned from CAST Analysis 230

5.1 Literature Review – CAST Analysis for the Fukuchiyama Derailment in 2005 in Japan..... 230
5.1.1 Overview of the Fukuchiyama Derailment 230
5.1.2 Key Findings from CAST Analysis and comparison with those in this thesis 232
5.2 Lessons Learned 237
5.3 Conclusion 242

Chapter 6 Conclusion and Future Work 244

6.1 Answers to the Proposed Questions 244
6.1.1 Why and How Do Automated Railway Systems Behave in Unsafe Ways 244
6.1.2 What Kinds of Causal Factors Contribute to Railway Accidents Involving Automated Systems 245
6.1.3 What Kinds of Considerations Should be Taken During Both Design and Operation So As To Maintain Safe Operation 248
6.2 Conclusion of the Thesis 248
6.3 Future Work 249
6.3.1 Specific Solutions for Implementing the Recommendations 249
6.3.2 Database for the Results of Accidents Analyses 249

Appendix A Supplement Information for WMATA CAST Analysis 252

A.1 Time Line of Incident, Enactment of Procedures, and Actions Involving Truck Circuits..... 252
A.2 Actions Involving B2-304 Prior to the Accident 258
A.3 Causal Loop Diagrams for the Conceptual Idea of the Migration to the High-Risk State 261
A.3.1 Degradation of Safety Culture 261
A.3.2 Degradation of Infrastructure 262
A.3.3 Degradation of Safety 263
A.3.4 Combining the Loops together: Multiplier Effects 264

Appendix B Supplement Information for Amtrak CAST Analysis 266

B.1 Safety Culture of Amtrak [56], [77], [78] 266
B.2 "Lax" Design Requirements for PTC 267

References 269

(This page intentionally left blank)

LIST OF TABLES

Table 2- 1 Basis for a New Foundation for Safety Engineering 31

Table 3- 1 System Definition, Accidents, and Hazards 55
Table 3- 2 Safety Constraints and System Requirements 56
Table 3- 3 Safety-related Roles and Responsibilities 59
Table 3- 4 Proximal Event Chain Leading to the Loss 66
Table 3- 5 Analysis of the Physical Process (Track Circuit B2-304) 75
Table 3- 6 Analysis of the Physical Process (Trains) 78
Table 3- 7 Analysis of the Train Operators 81
Table 3- 8 Analysis of the ATP System 83
Table 3- 9 Analysis of the OCC Computers 87
Table 3- 10 Analysis of the OCC Operators 90
Table 3- 11 Analysis of the ATC Mechanics (Installation Team) 100
Table 3- 12 Analysis of the ATC Mechanics (Preventative Maintenance Team) 101
Table 3- 13 Analysis of the ATC Mechanics Supervisor 103
Table 3- 14 Analysis of the ATC Systems Engineer 106
Table 3- 15 Analysis of the Alstom 109
Table 3- 16 Analysis of the WMATA Management 114
Table 3- 17 Analysis of the Federal Government/FTA 117
Table 3- 18 Analysis of the Local Governments 119
Table 3- 19 Analysis of the TOC 120
Table 3- 20 Analysis of the Congress 122

Table 4- 1 Amtrak's Financial and Ridership Data 146
Table 4- 2 Cab Signal Indications on the Accident Site 154
Table 4- 3 How ATC and ACSES Satisfies the PTC Functional Requirements 160
Table 4- 4 How ATC and I-ETMS Satisfies the PTC Functional Requirements 161
Table 4- 5 System Definition, Accidents, and Hazards (Amtrak) 162

Table 4- 6 System-Level Safety Constraints and System Requirements (Amtrak)..... 163
Table 4- 7 Safety-Related Roles and Responsibilities (Amtrak) 166
Table 4- 8 Proximal Event Chain (Amtrak)..... 172
Table 4- 9 Analysis of the Physical Process (Amtrak)..... 174
Table 4- 10 Analysis of ATC System 177
Table 4- 11 Analysis of ACSES(PTC) System 180
Table 4- 12 Analysis of the Wayside Signal and Signage 181
Table 4- 13 Unanswered Questions at Signal and Train Control System Level 182
Table 4- 14 Analysis of the Train Operator..... 185
Table 4- 15 Analysis of the Train Dispatcher..... 187
Table 4- 16 Analysis of the Signal and Train Control System's Engineer 188
Table 4- 17 Analysis of the Manufacturer..... 190
Table 4- 18 Unanswered Questions at Signal and Train Control System Level 191
Table 4- 19 Analysis of the Operation Management..... 193
Table 4- 20 Analysis of the Signal and Train Control System Division Management..... 194
Table 4- 21 Analysis of the Design Management 197
Table 4- 22 Analysis of the Amtrak Management..... 200
Table 4- 23 Comparison of Maintenance Expenditure and Capital Investment between Amtrak and Japan Railway in FY2017 (Data sources: [61], [62], [63], [64]). 204
Table 4- 24 Unanswered Questions at Signal and Train Control System Level 205
Table 4- 25 Analysis of the Local Governments..... 207
Table 4- 26 Analysis of Federal Government/DOT/FRA 207
Table 4- 27 Analysis of Congress 209
Table 4- 28 Analysis of NTSB..... 210
Table 4- 29 Unanswered Questions at Signal and Train Control System Level 211

Table A- 1 Time line of Incident, enactment of procedures, and actions involving truck circuits.. 253
Table A- 2 Actions Involving B2-304 Prior to the Accident..... 258

LIST OF FIGURES

Figure 1- 1 Expansion of HSR in the World. 23
Figure 1- 2 Increase of the HSR's Top Speed. 24

Figure 2- 1 Mappings between Forms and Functions Assumed to be Direct and Known in Analytic Reduction 33
Figure 2- 2 Behavior is Modeled as Separate Events in the Chain of Events Model. 34
Figure 2- 3 Chain-of-Events Model Example1 (Pressurized Tank Rupture). 35
Figure 2- 4 Chain-of-Events Model Example 2 (Heinrich's Domino Model, left) and Example 3 (Reason's Swiss Cheese Model, right) 36
Figure 2- 5 Mars Polar Lander Loss. 37
Figure 2- 6 Three Categories of Systems. 39
Figure 2- 7 Emergent Properties Controlled by Enforcing Constraints. 42
Figure 2- 8 Types of STAMP-based Tools. 43

Figure 3- 1 Train 112 Struck Train 214 from its Rear. 47
Figure 3- 2 Metrorail's System map with two stations marked. 49
Figure 3- 3 Operation and financing information of WMATA. 52
Figure 3- 4 Level 1 High-Level Safety Control Structure of WMATA Metrorail System. 57
Figure 3- 5 Level 2 detailed Safety Control Structure of WMATA Metrorail System 58
Figure 3- 6 ATC's 2 Level Decomposition and Responsibilities of Subcomponents. 71
Figure 3- 7 Main Safety Responsibilities of ATP system 72
Figure 3- 8 How ATP System Detects Trains 73
Figure 3- 9 Oscilloscope displays of the receiver circuit module (Left) and 74
Figure 3- 10 Operator-Physical Interactions in the Safety Control Structure. 80
Figure 3- 11 Detailed View of Safety Control Structure 81
Figure 3- 12 OCC LCD Screen and an OCC Controller. 92
Figure 3- 13 OCC Display During the Accident Sequence (4:56:50 p.m.). 93
Figure 3- 14 OCC Display During the Accident Sequence (4:57:02 p.m.). 93

Figure 3- 15 OCC Display During the Accident Sequence (4:57:19 p.m.)..... 94
Figure 3- 16 OCC Display During the Accident Sequence (4:57:38 p.m.)..... 94
Figure 3- 17 OCC Display During the Accident Sequence (4:57:39 p.m.)..... 95
Figure 3- 18 OCC Display During the Accident Sequence (4:57:46 p.m.)..... 96
Figure 3- 19 OCC Display During the Accident Sequence (4:58:10 p.m.)..... 96
Figure 3- 20 Detailed View of ATC Engineers-Physical Interactions in the Safety Control Structure. 98
Figure 3- 21 Zoom-Up to Highest Level of Safety Control Structure. 113
Figure 3- 22 Safety Constraints Violated in the Highest-Level of Safety Control Structure. 128
Figure 3- 23 Safety Constraints Violated in the Operator-Physical System Level of Safety Control Structure..... 129
Figure 3- 24 Safety Constraints Violated in the ATC Engineers-Physical System Level of Safety Control Structure..... 130
Figure 3- 25 Ineffective Control Actions, Feedback, and Controllers. 131

Figure 4- 1 Amtrak Train 188 derailed in Philadelphia on Northeast Corridor..... 140
Figure 4- 2 Amtrak Northeast Corridor Route Overview..... 141
Figure 4- 3 Train 188's Route Through Philadelphia..... 141
Figure 4- 4 Amtrak National Network in FY 2017. 145
Figure 4- 5 NEC Key Operation Metrics. 147
Figure 4- 6 NEC Ridership growth, FY 1998 – FY 2017. 147
Figure 4- 7 NEC Ticket Revenue growth, FY 1998 – FY 2017. 148
Figure 4- 8 NEC Market Share growth, FY 2000 – FY 2017. 148
Figure 4- 9 State-Supported Service Key Operation Metrics. 150
Figure 4- 10 State-Supported Service Key Operation Metrics. 151
Figure 4- 11 Pyramid of Modern Signal Systems. 152
Figure 4- 12 Overview of Automatic Block Signal System. 153
Figure 4- 13 ACSES and I-ETMS on NEC. 158
Figure 4- 14 Level 1 High-Level Safety Control Structure (Amtrak). 164
Figure 4- 15 Level 2 detailed Safety Control Structure (Amtrak). 165

Figure 4- 16 Signal and Train Control System Level Safety Control Structure. 176
Figure 4- 17 Front-Line Controller Level Safety Control Structure. 183
Figure 4- 18 Amtrak Management Level Safety Control Structure. 192
Figure 4- 19 Governmental and Audit Organizations Level Safety Control Structure. 206
Figure 4- 20 US commuter modes' transition from 1970 to 2016. 213
Figure 4- 21 Comparison of Passenger Modal Share between US and Japan. 214
Figure 4- 22 Transition of US's Federal Investment on Construction as Share of GDP. 215
Figure 4- 23 Aged Vehicles of Amtrak 217
Figure 4- 24 Safety Constraints Violated in the Highest-Level of Safety Control Structure. 219
Figure 4- 25 Safety Constraints Violated in the Middle-Level of Safety Control Structure. 220
Figure 4- 26 Safety Constraints Violated in the Lowest-Level of Safety Control Structure 221
Figure 4- 27 Ineffective Control Actions, Feedback, and Controllers. 222

Figure 5- 1 Fukuchiyama Line and the Location of the Derailment. 231
Figure 5- 2 Accident Aftermath of the Fukuchiyama Derailment 232

Figure A- 1 Conceptual Representation of Degradation of Safety Culture in WMATA. 262
Figure A- 2 Conceptual Representation of Degradation of Infrastructure in WMATA. 263
Figure A- 3 Conceptual Representation of Degradation of Safety in WMATA 264
Figure A- 4 Conceptual Representation of Migration to a High-Risk State in WMATA 265

Figure B- 1 PTC stop the train only ahead of the interlockings 267

LIST OF ACRONYMS AND ABBREVIATIONS

ABSS	Automatic Block Signaling System
ACSES	Advanced Civil Speed Enforcement System
AIM	Advanced Information Management system
Alstom	Alstom Signaling Inc.
Amtrak	National Railroad Passenger Corporation
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
C	Contextual Factors/Context in which decisions made
CAP	Corrective action plan
CAST	Causal Analysis based on STAMP
CJR	Central Japan Railway company
Conrail	Consolidated Rail Corporation
DC	The District of Columbia
DOT	U.S. Department of Transportation
ETCS	European Train Control System
F	Failures and inadequate controls
FHA	Fault Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FRA	Federal Railroad Administration
FTA	Fault Tree Analysis
FTA	Federal Transit Administration
GPS	Global Positioning System, Global Positioning Satelite
GRS	General Railway Signal Company (The company, since acquired by Alstom Signaling Inc., provided the original Metrorail train control modules.)

HSR	High-speed rail
ICE	InterCity Express
I-ETMS®	Vital Electronic Train Management System
JR West	West Japan Railway company
LCD	Liquid-Crystal Display
MD	State of Maryland
Metrorail	Washington Metro
MMF	Mental Model (Flaws)
MOC	Maintenance Operations Center
MLIT	Japanese Ministry of Land, Infrastructure, Transport and Tourism
NASA	National Aeronautics and Space Administration
NEC	Northeast Corridor
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
OCC	Metrorail Operations Control Center
PMF	Process Model Flaws
PRA	Probabilistic Risk Assessment
PTC	Positive Train Control
R	Reinforcing feedback structure
ROCS	Rail Operation Computer System
RSIA08	Railroad Safety Improvement Act of 2008
SA	Situation Awareness
SC-Maglev	Super Conducting Magnetic Levitation system
SR	Safety Responsibilities/Safety Requirements and constraints
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
TGV	Train à Grande Vitesse
TOC	Tri-State Oversight Committee
TWC	Train-Wayside Communication

UCA	Unsafe (Decisions and) Control Actions
UD	Unsafe Decisions
UIC	International Union of Railways
US&S	Union Switch & Signal (The company, now known as Ansaldo STS USA, supplies the components that have begun to replace the GRS equipment originally installed on the Metrorail system.)
UQ	Unanswered Question
VA	Commonwealth of Virginia
WMATA	Washington Metropolitan Area Transit Authority

(This page intentionally left blank)

Chapter 1 Introduction

1.1 Motivation

1.1.1 Accidents related to Automated Systems

In 2018, a self-driving car struck and killed a pedestrian in Arizona [1] , where a human operator was onboard as an emergency backup. That is, she was essentially in charge of monitoring instead of driving by herself. The preliminary accident report shows that the automated system performed as designed, but it "relies on an attentive operator to intervene if the system fails to perform appropriately" [2].

Other transportation modes are also experiencing new types of hazards and accidents related to increased levels of automation. One example is the commercial aviation industry. For decades, automated systems have been added to airplanes so as to "help pilots set engine thrust, navigate with higher precision and even override the humans in the cockpit if they make mistakes [3]." As a result, automation-related accidents have been a growing concern in aviation [3].

According to the National Highway Traffic Safety Administration (NHTSA), there are four benefits of automating automobiles, that is, safety, economic and societal benefits, efficiency and convenience, and mobility [5]. However, it seems that the humans are still needed to support safe operation of the system such as monitoring the automation and intervening in emergency situations. Leveson argued that with the increased automation, humans have moved into "positions of higher-level decision making," and this led to new types of human errors such as mode confusion in which a human operator cannot perfectly anticipate the systems' behaviors [6, Ch. 1]. In addition, Parasuraman *et al.* argued that "automation can have both beneficial and negative effects on human performance." The negative effects include increasing mental workload, reduced situation awareness, and over-trust of automation (complacency) [7].

In addition to the problems in automated systems in automotive and aviation domains, other industries such as railways are also facing issues associated with automation. In October 2018, in Taiwan, a train exceeded 100 kph (about 62 mph) where the restricted speed was 75 kph, and it derailed resulting in 187 injuries and 18 fatalities. It is reported that the automatic train protection

system was not activated at the time of the accident due to the motor's failure [8]. Also, the organizational structure of the operating company seems to have been problematic because the audit authority was not perfectly independent from the operation authority, presenting an apparent conflict of interest and making it difficult to effectively solve these issues [9].

That accident is reminiscent of a derailment in Spain in 2013, where a high-speed train was running at around 190 kph on a curve with a 80 kph speed limit, which resulted in 144 injuries and 80 fatalities[10]. Another derailment occurred in Japan in 2005, with a conventional train running at around 116 kph on a curve of 70 kph speed limit. It derailed, resulting in 562 injuries and 107 fatalities[11] . In each of these derailments, the speed protection device was not activated. For the case in Spain, the European Train Control System (ETCS) could have automatically activated brake but it was not activated because of "operating problems[10] ." For the latter case in Japan, the Automatic Train Stop System (ATS) was not installed at the accident site and there was no legislation forcing the train operators to install such a speed protection system [12]. These three accidents were not purely a problem of technology, but also a result of the managerial and political decisions about how to maintain safe operation of the rail systems with automated systems.

Another accident in the rail domain is the WMATA Metrorail crash in 2009, where an Automatic Train Control system (ATC) did not detect a stopped train due to the spurious signal generated in the track component. Non-zero speed commands were automatically sent to the following train, resulting in the crash. The components acted as designed but the specific behavior that occurred (parasitic oscillation) had not been considered in the design. The investigation report found that the lack of safety culture and ineffective safety oversight from management and audit authorities also contributed to the accident [13].

As Leveson argues, the traditional focus on increasing reliability of the component is not always effective [6] because the accidents we are facing today are not purely because of component failures. Decision making in management, politics, operation, design, and organizational structure and culture can also contribute to accidents, and these combinations of societal and technical factors are playing an increasing role in accidents in automotive, aviation, and rail systems. Therefore, we need to consider the societal aspects as well as technical aspects when designing and operating safety-critical automated systems.

1.1.2 New Accident Analysis Technique

As discussed earlier, automation is being increasingly adopted across transportation industries including automobile, aviation, and railway. As the systems become increasingly automated, new types of accidents and their causes have emerged. We need to understand how automated systems are causing new accidents and make sure lessons learned are applied to the future design and operation of these systems.

The author of this thesis was struck by the concept of STAMP (Systems-Theoretic Accident Model and Processes), which was first proposed by Nancy G. Leveson, a professor at MIT Department of Aeronautics and Astronautics. At the heart of STAMP is the idea that we should stop blaming human operators as a cause of the accident, and instead we should identify why they behaved that way with the feedback and other information they had at the time. In addition, STAMP-based approaches were intended to be used for today's complex socio-technical systems where both technical and social aspects play a role in the accidents [6]. However, compared to the amount of attention and research in both aviation and auto industries using STAMP-based analysis, less seems to have been carried out on the rail domain[1].

This thesis focuses on accident analysis in railway systems, specifically conventional rail, HSR, and SC-Maglev used for passenger transport. Thus freight trains are not within the scope of this thesis, although the methods and results in this thesis could be applicable there as well.

1.1.3 Development of HSR and Japanese SC-MAGLEV

Conventional rail has been spreading worldwide. Many stations built in 19th century are located in the center of large cities, serving as a junction for different transportation modes, and facilitating door-to-door trips. Compared to other transportation modes, the conventional rail is regarded as safer and more environmentally efficient. However, the other modes, that is, auto and aviation, have improved and negatively impacted the modal share of rail, especially for medium and

[1] There have been 14 publications in aviation and air traffic control, 7 in auto, and 3 in rail. (Source: http://sunnyday.mit.edu/STAMP-publications-sorted.pdf, accessed March 2nd, 2019.)

long-distance operations [14] .

As a measure to stop the decline of the modal share of the rail sector, the world's first HSR, Shinkansen, was born in Japan in 1964. This was followed by several European countries, especially TGV in France in 1981. After successful operation in Japan and France, the HSR network has spread further to Italy and Germany (ICE) in 1988, Belgium in 1997, the UK in 2003, and the Netherlands in 2009. In addition to these European countries, it spread to other regions too; China in 2003, South Korea in 2004, Taiwan in 2007, and Turkey in 2009. As of 2018, HSR systems have been constructed over more than 45,000 km in the world, especially due to China's tremendous investment after 2003 (See Figure1-1). In addition to its expansion into the world, its speed has also increased over time (See Figure 1-2) [14].

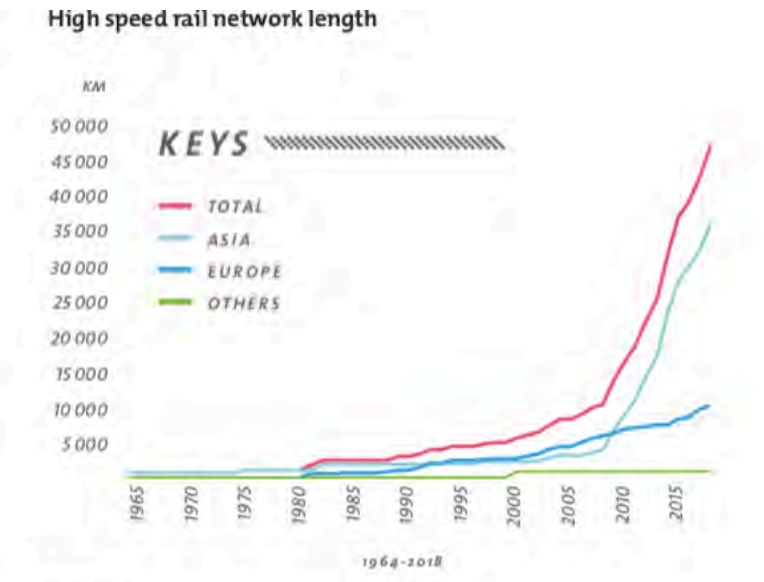


Figure 1- 1 Expansion of HSR in the World.

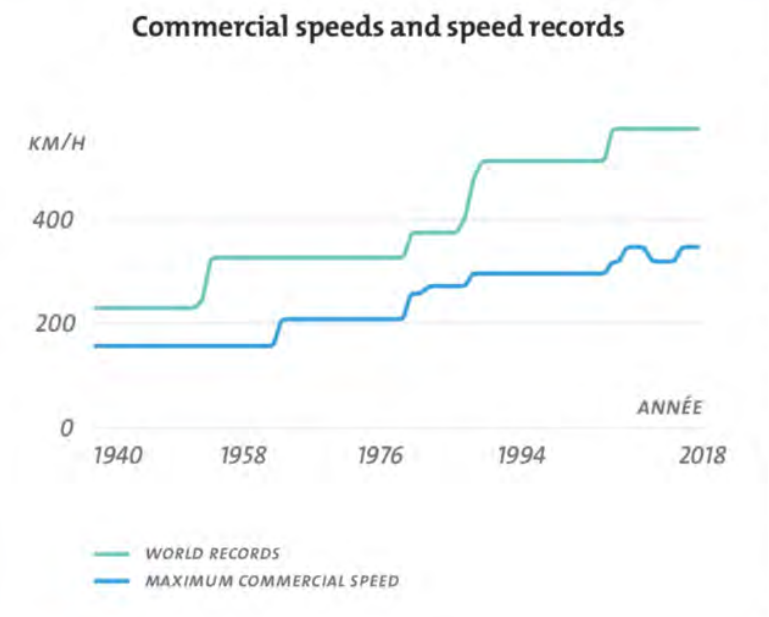


Figure 1- 2 Increase of the HSR's Top Speed.

(Both Adapted from International Union of Railways (UIC) [14])

A new type of rail transportation system, the Super Conducting Magnetic Levitation system (SC-Maglev), has been developed in Japan and is now planned to be constructed and operated by Central Japan Railway company (CJR) beginning in 2027 between Tokyo and Nagoya, a distance of 285.6 km (177.5 miles), with the maximum operation speed of 505 kph (314 mph) [15]. This system has many subsystems that are tightly interconnected by physical and information interfaces, requiring a lot of consideration not only in component design but also in how these components may operate together and achieve safe operation. In addition to this tightly coupled structure, the elimination of the onboard train operator adds a further challenge for the mechanical and electrical engineers, as all of the control is carried out automatically by pre-programmed software and ground electro-mechanical equipment instead of onboard equipment.

1.2 Research Objectives

As explained earlier, the automated systems we are dealing with today can result in accidents not only due to human errors or component failures, but also due to systemic factors including organizational structure, managerial decisions, and political decisions. In railway systems, the reliability of each component has increased due to an improved train control system or redundancy, but it seems less consideration has been given beyond the component level. Therefore, it is crucial to understand the mechanism of how those systemic factors interact and lead to loss events.

Thus, the main objective of this research is to understand and answer following questions:

1) why and how do automated railway systems behave in hazardous ways, resulting in accidents;
2) what kinds of causal factors contribute to railway accidents involving automated systems;
3) what kinds of considerations should be taken during both design and operation so as to maintain safe operation.

1.3 Research Methodology

This research analyzes past accidents for railway systems involving highly automated but ultimately unsafe behaviors due to problems in design, operation, organizational structure, managerial and political decisions, and any other systemic causes.

In order to analyze systemic factors in complex railway systems, the CAST (Causal Analysis based on STAMP) framework was utilized and adopted for two selected cases. These cases were selected based on following three criteria: (1) information availability, (2) automation-related accidents, and (3) non-component failures contributing to the accident. With these in mind, (1) WMATA Metrorail Crash in 2009, and (2) Amtrak Derailment in 2015 were selected as the case

studies.

After analyzing the past accidents, this thesis extracts important lessons for future consideration in design, operation, and decision making including managerial and political issues.

1.4 Thesis Scope

This thesis focuses on extracting general considerations in railway systems' design, operation, and decision making in management and politics. Thus, a system-specific solution would be outside of the scope of the thesis.

In addition, as is explained earlier, the main focus of this thesis is on conventional rail, HSR, and SC-Maglev used for passenger transport. Thus freight trains are not within the scope of this thesis, although the methods and results in this thesis could be applicable there as well.

1.5 Thesis Outline

This thesis will proceed as follows:

・Chapter 2 introduces the concept of STAMP, and its difference from traditional accident analysis models. This chapter also presents the basic steps of CAST accident analysis.

・Chapter 3 and 4 provide the results of CAST analysis for two railway accidents, that is, the WMATA Crash in 2009 (Chapter 3) and the Amtrak Derailment in 2015 (Chapter 4), respectively. The detailed examination of safety control structure, unsafe control actions, mental model flaws, and context reveals the systemic causes behind the accidents.

・Chapter 5 then summarizes the important lessons extracted from the CAST analysis results.

・Chapter 6 concludes the thesis findings and answers the questions highlighted in section 1.2.

Furthermore, possible future work is discussed.

The next chapter is the introduction of the STAMP, a new accident analysis model, and the STAMP-based accident analysis tool called CAST.

(This page intentionally left blank)

Chapter 2 STAMP (System-Theoretic Accident Model and Processes)[2]

"All models are wrong, but some are useful."

--- George Box (British statistician)

"Models are important because they provide a means for understanding phenomena like accidents or potentially hazardous system behavior and for recording that understanding in a way that can be communicated to others."

--- Professor Nancy G. Leveson [6, Ch. 2]

"The event-based models developed to explain physical phenomena are inadequate to explain accidents involving organizational and social factors and human decisions and software design errors in highly adaptive, tightly-coupled, interactively complex sociotechnical systems… these goals are achievable if models based on systems theory, rather than reliability theory, underlie our safety engineering activities."

--- Professor Nancy G. Leveson [6, Ch. 2]

In this chapter, the new accident causality model based on systems theory called STAMP (System-Theoretic Accident Model and Processes) [6], [17] is introduced. This model was proposed by Nancy G. Leveson, a professor of Department of Aeronautics and Astronautics in MIT, as a way to analyze and understand the mechanism of the types of accidents arising from the complex socio-technical systems we are dealing with today.

This chapter was prepared for understanding (1) what are the problems with the traditional accident analysis techniques, (2) what is the goal and capability of the STAMP-based accident analysis technique, and (3) the general steps for performing accident analysis, called CAST.

[2] This section is based on the knowledge of Professor Nancy Leveson and Dr. John P. Thomas in MIT, which are summarized in Leveson's book [6], lecture notes [16], and their STPA handbook [17].

2.1 Introduction – Why Do We Need Something Different?

While traditional hazard analysis frameworks had been working well for the simpler systems of the past, they are not well suited for the systems we are building today. Leveson proposes some of the reasons for the limitation of the traditional approach [6, Ch. 1]:

- Fast pace of technological change
- Reduced ability to learn from experience
- Changing nature of accidents
- New types of hazards
- Increasing complexity and coupling
- Decreasing tolerance for single accidents
- Difficulty in selecting priorities and making tradeoffs
- More complex relationships between humans and automation
- Changing regulatory and public views of safety

Leveson adds that:

> Incremental improvements in traditional safety engineering approaches over time have not resulted in significant improvement in our ability to engineer safer systems. A paradigm change is needed in the way we engineer and operate the types of systems and hazards we are dealing with today. … systems theory and systems thinking can be used to extend our understanding of accident causation and provide more powerful (and surprisingly less costly) new accident analysis and prevention techniques [6, Ch. 1].

She argues that the paradigm changes start with "questioning the basic assumptions underlying what we do today." The old assumptions rooted in traditional approaches and the new assumptions needed for the new technique are summarized in Table 2-1.

Table 2- 1 Basis for a New Foundation for Safety Engineering

Old Assumption	New Assumption
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur.	High reliability is neither necessary nor sufficient for safety.
Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chains of events leading to the loss.	Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.
Most accidents are caused by operator error. Rewarding safe behavior and punishing unsafe behavior will eliminate or reduce accidents significantly.	Operator error is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety.
Major accidents occur from the chance simultaneous occurrence of random events.	Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.
Assigning blame is necessary to learn from and prevent accidents or incidents.	Blame is the enemy of safety. Focus should be on understanding how the system behavior as a whole contributed to the loss and not on who or what to blame for it.

(Adapted from Leveson [6, Ch. 2])

First, Leveson argues that safety should be differentiated from a component's reliability. That is, the system can perform unsafely even when the components perform reliably. Second, the underling chains-of-events model in traditional methods, such as FTA (Fault Tree Analysis) or FMEA (Failure Modes and Effects Analysis), is not suitable for today's complex sociotechnical system, because those traditional methods were developed for far simpler electromechanical systems. Third, she maintains that the probabilistic risk analysis is not suitable for assessing and communicating safety information, as they are sometimes inaccurate or "made up" because of the difficulties in determining the probability of the events leading to the accident. Forth, she contends that "operator

error” can be caused by a broader control structure that makes it very difficult for a human operator to succeed. Fifth, she maintains that software reliability does not necessarily mean that software will perform safely. Even if software performs reliably as designed, accidents can happen. Sixth, she argues that systems are “dynamic” not “static” and can migrate over time into states of higher risk. She maintains that too often human operators are assigned blame, which causes problems for analysis. That is, if the accident analysis focuses on who should be blamed, then the potential lessons extracted and learned may be reduced. She argues that the focus should be on understanding why they behaved that way and on redesigning systems that would prevent the causal factors from happening again.

These questions and old assumptions are why a new model is needed for analyzing today’s complex socio-technical systems. These new assumptions led to the new accident causality model, called STAMP.

In the following sections, the difference between traditional analysis techniques and STAMP are explained. First, one of the limitations of the traditional approach, that is, limited ability in analyzing high-complexity systems, is explained.

2.2 Increased Complexity

Leveson argues that “increased complexity of all types makes it difficult for the designers to consider all the potential system states or for operators to handle all normal and abnormal situations and disturbances safely and effectively. In fact, complexity can be defined as intellectual unmanageability” [6, Ch. 1].

In the next section, different ways to cope with systems’ complexity are explained.

2.3 Coping with Complexity

2.3.1 Analytical Decomposition (the traditional approach)

In order to deal with complexity, systems are often decomposed into different subparts so as to examine the parts separately.

Physical aspects → Separate physical components[3] or functions[4]
Behavior → Events over time

This method is sometimes called *divide and conquer*, formally referred to as *analytic reduction*. The physical aspects are broken into distinct subcomponents, and assumed to be interacting in direct and known ways (See Figure 2-1). Please note that the mappings might be between functions and physical components (forms), and these mappings are assumed to be direct and known.

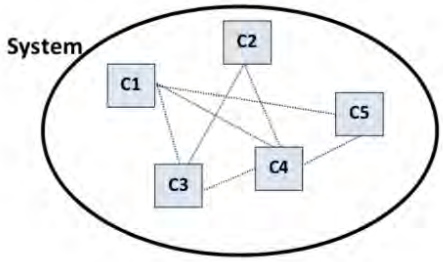


Figure 2- 1 Mappings between Forms and Functions Assumed to be Direct and Known in Analytic Reduction.

(Adapted from Leveson and Thomas [17])

In addition to physical aspects, behaviors can be divided into smaller parts. In traditional

[3] The examples for aircraft system include fuselage, engines, wings, stabilizers, nozzles, etc.
[4] The examples for aircraft system include propulsion, navigation, attitude control, braking, cabin environment control, etc.

models, behavior can be modeled as separate events over time where each event is the direct result of the preceding ones (See Figure 2-2). These events could be grouped into operational stages, such as for aircraft: pushback, taxi, take off, climb, cruise, approach, or touchdown.

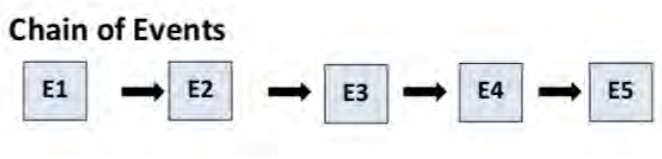


Figure 2- 2 Behavior is Modeled as Separate Events in the Chain of Events Model.

(Adapted from Leveson and Thomas[17])

However, this divide and conquer approach only holds if the separation and individual analysis do not distort the phenomenon or property of interest. This kind of approach only works when [17]:

- Each component or subsystem operates independently. If events are modeled, then they are independent except for the immediately preceding and following events.
- Components act the same when examined separately (singly) as when they are playing their part in the whole.
- Components and events are not subject to feedback loops and other indirect interactions.
- The interactions among the components or events can be examined pairwise and combined into a composite value.

The traditional hazard analysis methods are based on analytic reduction and thus based on these assumptions.

2.3.1.1 Chain of Events

In the chain of events model, chains of directly related physical or logical (functional) failure events leading to loss are identified. If one assumes that accidents are caused by a chain of failure events, then it makes sense to prevent accidents by eliminating events or putting barriers between the events. By doing so, it is assumed that one failure will not cause other failure events downstream in the chain.

Figure 2-3 below shows the tank explosion mechanism which is represented by a chain of events. Each event is annotated with typical accident prevention design techniques, which include redundancy, barriers, high component integrity, overdesign, or fail-safe design. For humans, these techniques include operational procedures, checklists, or training.

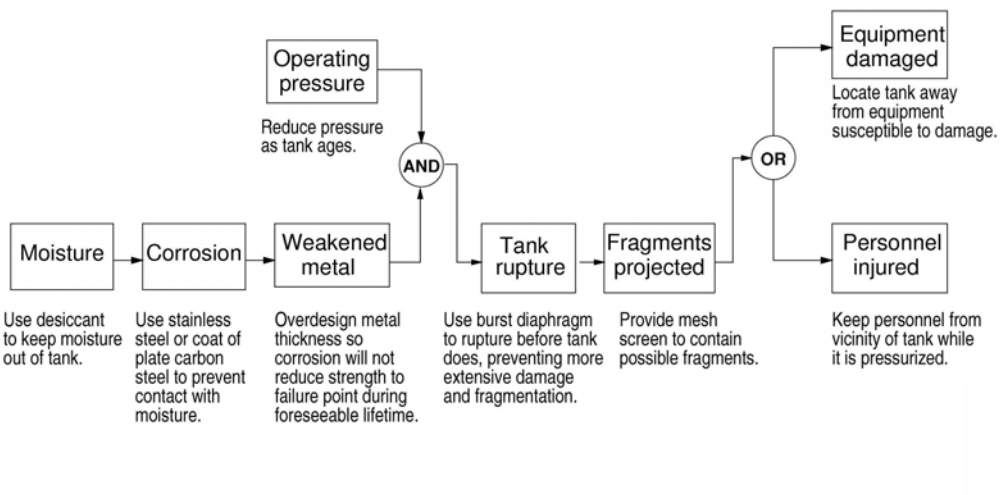


Figure 2- 3 Chain-of-Events Model Example1 (Pressurized Tank Rupture).

(Adapted from Leveson [18])

However, even this simple example, any consideration of factors indirectly related to the events are omitted. For instance, competitive or financial pressures to increase efficiency might result in not reducing the operating pressure as the tank ages. Also, changes over time of the planned design, such as requiring employees to spend time near the tank while it is pressurized, would also not be considered.

Some other models based on the chain-of-events include the Domino Model, which was first published and proposed by Heinrich in 1930, and the Swiss cheese model, proposed by Reason twenty years after the first Domino Model (See Figure 2-4).

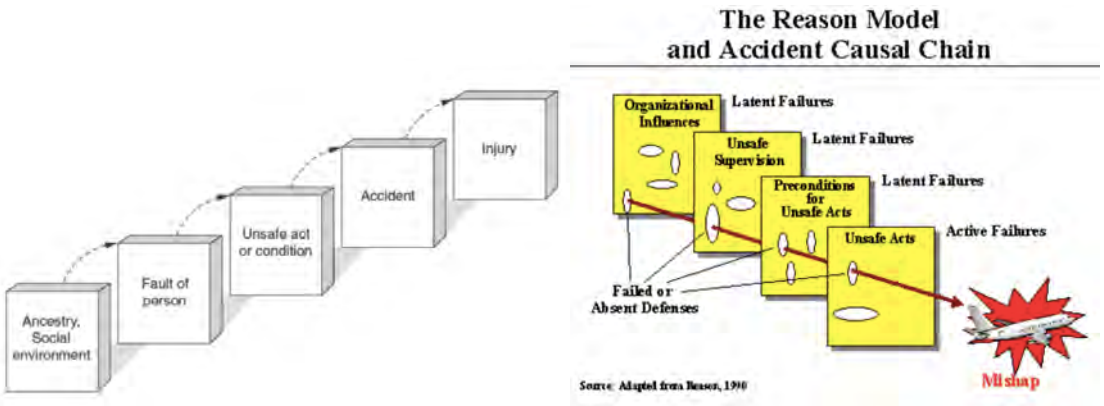


Figure 2- 4 Chain-of-Events Model Example 2 (Heinrich's Domino Model, left) and Example 3 (Reason's Swiss Cheese Model, right).

(Left: Adapted from Leveson [6, Ch. 2], Right: Adapted from Leveson [16]))

Although causality models based on the chains-of-events assumption are simple and straightforward, which makes them appealing, they are too simple for those who are dealing with today's complex systems who need to identify why accidents occurred (including indirect and systemic factors) and who need to identify effective ways to prevent them in the future.

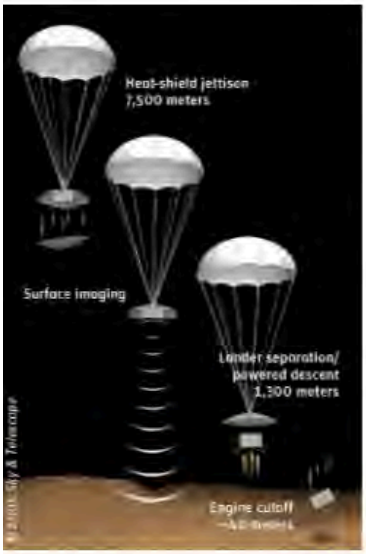
Some important limitations of chain-of-events models are: 1) requiring direct causality relationships; 2) subjectivity in selecting the events; and 3) exclusion of systemic factors.

2.3.1.3 Confusion of Safety and Reliability [6, Ch. 2]

Another flawed assumption is assuming that accidents can be prevented by simply increasing component reliability. Safety and reliability are different properties, and safety is not assured by increasing reliability of system or components. Accidents occur even when no components

or systems fail. This flawed assumption is so prevalent that it is important to understand the differences between these two properties.

Accidents can occur not only due to component failures but also as a result of interactions between non-failed components. The loss of the Mars Polar Lander is a good example (See Figure 2-5). The onboard software received signals from touchdown sensors that were experiencing vibration, which was normal and expected, and interpreted the signal as indicating that landing had occurred (because software engineers were told to interpret the signals this way). The software was designed to respond to any touchdown indication by immediately shutting down the descent engines, which resulted in a free-fall and crash of the Mars Polar Lander. All the components, including legs, sensors, and software, functioned reliably and without failure to satisfy every individual component requirement. Instead, interactions between non-failed components led to the accident. The system designers had not accounted for the possible interactions between components, that is, between landing leg deployment and the descent engine control software.



This loss involved the Mars Polar Lander. It is necessary to slow the spacecraft down to land safely. Ways to do this include using the Martian atmosphere, a parachute and descent engines (controlled by software). As soon as the spacecraft lands, the software must immediately shut down the descent engines to avoid damage to the spacecraft. Some very sensitive sensors on the landing legs provide this information. But it turned out that noise (false sensor signals) are generated when the legs are deployed. This expected behavior was not in the software requirements. Perhaps it was not included because the software was not supposed to be operating at this time, but the software engineers decided to start early to even out the load on the processor. The software thought the spacecraft had landed and shut down the descent engines while the spacecraft was still 40 meters about the planet surface. Which spacecraft components failed here?

Figure 2- 5 Mars Polar Lander Loss.

(Adapted from Leveson and Thomas [17])

This example is a *component interaction accident*, which can occur due to interactions among non-failed system components, including electromechanical, digital, and even human controllers, rather than due to individual component failures. In contrast, *a component failure accident*, arises due to component failures, including multiple and cascading failures.

Component failure accidents have received significant attention across engineering disciplines, yet component interaction accidents are becoming more and more common as the level of the complexity of the system designs we are dealing with continue to increase.

In the past, system designs were not as complex and were more intellectually manageable, making it easier to plan, understand, anticipate, guard against, and test these interactions to eliminate design errors before the system is operated. The systems we deal with today do not have these properties, and system design errors are becoming more common and cause accidents even when no components have failed. Thus, we need methods to identify these contributions to accidents and to eliminate/mitigate unsafe interactions between components.

2.3.1.4 Problems with traditional Analytical Decomposition Approach

The assumptions underlying the analytical decomposition approach may be true or close enough for the electromechanical systems which we used to build, but the significantly increased level of complexity in our systems today has made such an approach much less effective in identifying and anticipating modern causes of accidents. Leveson argues that the traditional approaches do not handle [18]:

- Component interaction accidents
- Systemic factors (affecting all components and barriers)
- Software and software requirements errors
- Human behavior (in a non-superficial way)
- System design errors
- Indirect or non-linear interactions and complexity

- Migration of systems toward greater risk over time (e.g., in search for greater efficiency and productivity)

She claims that system theory can provide a new theoretical basis for analyzing today's tightly coupled, software intensive, highly automated, and interconnected complex systems. In the next subsection, systems theory is introduced and explained.

2.3.2 Systems Theory

Systems can be categorized into three types, that is, Organized Simplicity, Unorganized Complexity, and Organized Complexity (See Figure 2-6 below). These are categorized according to the degree of randomness and degree of "complexity." [6, Ch. 3]

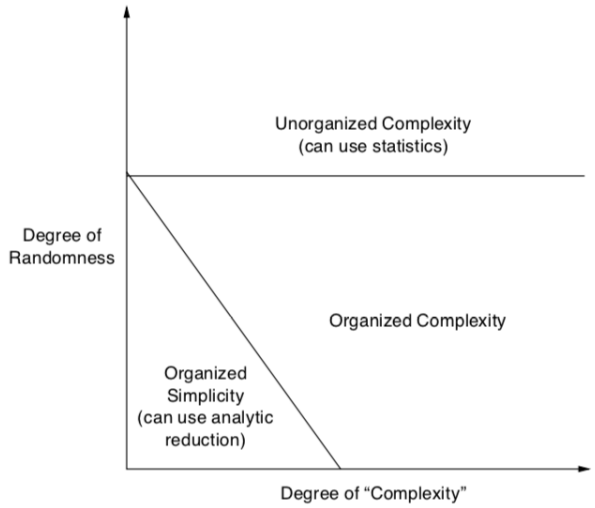


Figure 2- 6 Three Categories of Systems.

(Adapted from Leveson [6, Ch. 3])

One of the categories is called “unorganized complexity.” These systems may be complex, but their behavior is “regular and random enough” that they can be studied through statistics. By treating the systems as “a structureless mass with interchangeable parts” and describing them in terms of averages, the analysis can be done using statistics.

Another type of system is what system theorists call “organized simplicity.” Traditional approaches, which were based on analytic reduction, were suitable for systems with organized simplicity. This type of system can be “separated into non-interacting subsystems for analysis purpose.” The interactions between components are assumed to be known and can be treated as pairwise. Older engineered systems in the past have fallen into this category, thus approaches based on analytic reduction were more effective in the past.

However, the level of complexity in modern systems has increased and new causes of accidents have been appearing especially because of software and autonomy. The traditional approaches are becoming less effective. Leveson and others argue that this is because our systems today are categorized as “organized complexity,” which occurs when systems are [18]:

- Too complex for complete analysis using analytic reduction
  - Separation into (interacting) subsystems distorts the results
  - The most important properties are emergent
- Too organized for statistics
  - Too much underlying structure that distorts the statistics (the averages are deranged)
  - New technology and designs have no historical information

Thus, approaches based on analytic reduction or statistics have been less effective. System theory was developed for this third type of system. In system theory (systems approach) [6, Ch. 3][17]:

- Systems are taken as a whole, not on the parts taken separately.
  - “The whole is more than the sum of its parts”
- A primary concern is Emergence, or emergent properties
  - Emergent properties “emerge” at the higher levels in a hierarchy due to components interacting at lower levels.

  - Emergent properties do not exist at lower levels; they are meaningless at the component levels.
  - Emergent properties can be treated adequately only in their entirety, including all social and technical aspects.
- Emergent properties arise from the relationships between the parts of the system.

As explained here, emergence is an important concept in systems theory. Other important concepts are hierarchy, control, and constraints. One goal is to explain relationships between different levels in a hierarchy: "what generates the levels, what separates them, and what links them." "Emergent properties associated with a set of components at one level in a hierarchy are related to *constraints upon the degree of freedom* of those components." Thus, describing emergent properties requires a "language" at a higher level, which is different from the language describing the components themselves, that is, different ways of description are needed at different levels.

Leveson argues that in systems theory, the constraints at the higher level of hierarchy control the lower-level behavior. In addition, she maintains that "Hierarchies are characterized by control processes operating at the interfaces between levels." She referred to Checkland's statement[5] for explaining this idea [6, Ch. 3] :

> Control is always associated with the imposition of constraints, and an account of a control process necessarily requires our taking into account at least two hierarchical levels…. But any description of a control process entails an upper level imposing constraints upon the lower.

She maintains that safety, which is an emergent property of systems, should be differentiated from reliability, which is a component property. She argues that the limited focus on avoiding failures by increasing reliability, which is prevalent in safety engineering today, should be replaced by the larger concept of imposing constraints on system behavior to avoid unsafe events or conditions, that is, avoiding hazards.

[5] This is originally from Checkland, Peter. 1981. *Systems Thinking, Systems Practice.* New York: John Wiley & Sons.

The new accident causality model, called STAMP (System-Theoretic Accident Model and Processes) thus incorporates the basic idea of systems theory, where safety is treated as an emergent property at higher-levels and can be enforced by imposing constraints on the behavior of and the interactions among the components at a lower level (See Figure 2-7 below).

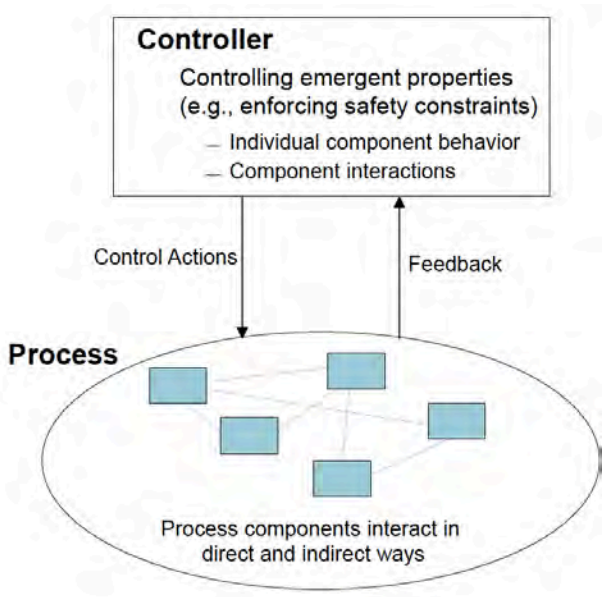


Figure 2- 7 Emergent Properties Controlled by Enforcing Constraints.

(Adapted from Leveson and Thomas [17])

In this new model, safety is thus treated as control problem where the goal is enforcing safety constraints. Accidents occur as a result of "inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system."

2.4 STAMP (System-Theoretic Accident Model and Processes) Model

STAMP is not a method for analysis, but a model about how accidents occur. STAMP is an alternative model to the chain-of-events model underling traditional safety analysis techniques.

There are some STAMP-based tools (methods) currently available as shown in Figure 2-8.

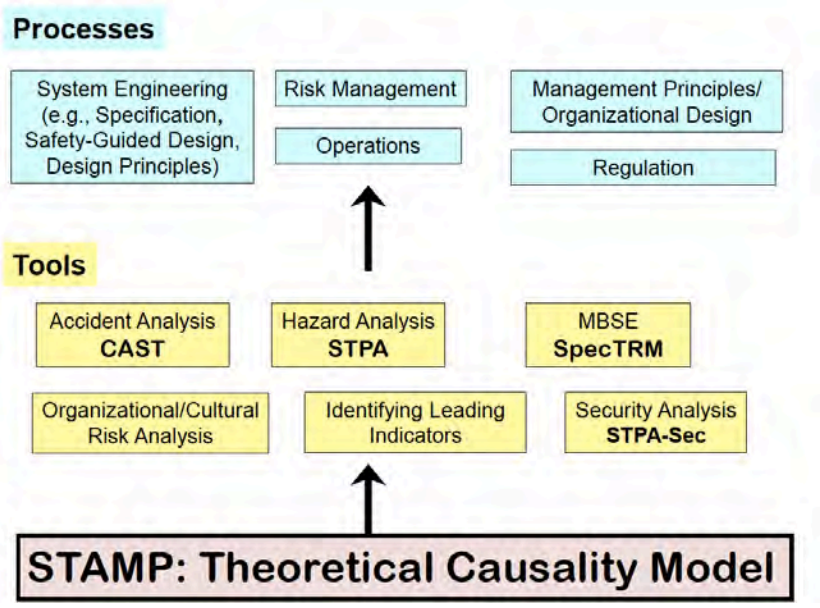


Figure 2- 8 Types of STAMP-based Tools.

(Adapted from Leveson and Thomas [17])

Among them, STPA (System Theoretic Process Analysis) and CAST are two widely used techniques. STPA is a proactive analysis method used for hazard analysis, whereas CAST is a retroactive analysis method used for analyzing past accidents. This thesis uses the CAST framework, and the basic CAST steps are presented below.

2.4.1 The Goal of CAST [6, Ch. 11]

Leveson argues that most accident are analyzed using chain-of-event-based models, and they almost always choose one or a few of the events as "root cause(s)" or "primary cause(s)." However, she contends, the analysis of why those events happened is usually not complete. She adds, the analysis often stops after "finding someone to blame – usually a human operator – and the opportunity to learn important lessons is lost."

She argues that an accident analysis technique needs to "provide a framework or process to assist in understanding the entire accident process and identifying the most important systemic causal factors involved." "CAST can be used to identify the questions that need to be answered to fully understand shy the accident occurred. It provides the basis for maximizing learning from the events." "The use of CAST does not lead to identifying single causal factors or variables. Instead it provides the ability to examine the entire sociotechnical system design to identify the weakness in the existing safety control structure and to identify changes that will not simply eliminate symptoms but potentially all the causal factors, including the systemic ones."

According to Leveson, the goals of CAST are:

- To get away from assigning blame, shifting the focus to why the accident occurred and how to prevent similar losses in the future.
- Minimizing hindsight bias, and determining why people behaved the way they did given the information they had at the time of the accident [6, Ch. 11].

2.4.2 General Steps of CAST [6, Ch. 11]

Here, the general steps of CAST are provided. The processes are not necessarily linearly applied, but may entail iterative processes where one may need to step back and revisit previous steps as more is learned about the accident.

1. Identify the system (s) and hazard (s) involved in the loss.

2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This includes the safety-related roles and responsibilities of each component, as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them to do this.
4. Determine the proximate events leading to the loss.
5. Analyze the loss at the physical system level.
6. Analyze the higher levels of the safety control structure.
7. Examine overall coordination and communication contributors to the loss.
8. Determine dynamics and migration to a high-risk state over time.
9. Generate recommendations.

2.5 Conclusion

In this chapter, the new accident causality model called STAMP was introduced. As explained in this chapter, STAMP is based on Systems theory and it treats safety as an emergent property of the system that arises from the interaction of components in the system. This idea is different from that of traditional accident causality models, which generally treats safety from a reliability perspective, that is, if the components' reliability is increased then the system will perform safely. However, this does not hold for today's complex socio-technical systems.

In following two chapters, the results of two accident analyses, which were carried out using CAST, are discussed. These case studies are used to generate recommendations based on the identified causal factors that contributed to the unsafe behavior of the whole system. These recommendations are important as tomorrow's safety-critical systems are designed and built.

(This page intentionally left blank)

Chapter 3 CAST Analysis 1 – WMATA Accident in 2009

This chapter applies CAST to a collision between two Redline trains of Washington Metropolitan Area Transit Authority (WMATA)'s Metrorail System in June 22, 2009. The accident happened when Automatic Train Control System (ATC) did not properly detect trains on the malfunctioned train circuit. There are many systemic causes that contributed to this accident, as well as component failures and unsafe design of safety-critical systems. The analysis of this accident using CAST framework can help explain (1) how an highly-automated system like this could fail to operate safely, (2) how the organization structure and safety culture may have affected the safety of the system.

Most of the information collected about this accident was from the official report [13]. Regarding the CAST methodology, the author mainly referred to the Leveson [6], her class notes in Fall 2017[6], and class notes carried out by Dr. John P. Thomas in Spring 2018 in conducting the CAST analysis. The author also referred to the other CAST analysis literature such as the work by Kawakami in 2014 [20] to understand each steps of the analysis.

3.1 Summary of the accident



Figure 3- 1 Train 112 Struck Train 214 from its Rear.

(Adapted from NTSB [13])

[6] The part of class notes in 2016 can be viewed online [19].

On Monday, June 22, 2009, about 4:58 p.m., eastern daylight time, inbound WMATA Metrorail train 112 struck the rear of stopped inbound Metrorail train 214. The accident happened on aboveground track on the Redline near the Fort Totten station in Washington, D.C. The lead car of train 112 struck the rear car of train 214, having caused the rear car of train 214 to telescope into the lead car of train 112. This resulted in a loss of occupant survival space in the lead car of about 63 feet, which was about 84 percent of its total length. Nine people aboard train 112, including the train driver, were killed. Emergency response agencies reported they transported 52 people to local hospitals. Damage to the train equipment was estimated to be $12 million. The picture of accident's aftermath is shown in Figure 3-1 and the Metrorail's system map is shown in Figure 3-2.



Figure 3- 2 Metrorail's System map with two stations marked.

(Adapted from NTSB [13]. Arrows and circles were added by the author.)

According to the NTSB report, the probable causes are (1) a failure of the track circuit modules manufactured by GRS/Alstom Signaling Inc., which caused ATC system to have failed to detect the train 214 (the struck train) and thus sent ATP speed commands to train 112 (the striking train) until the trains collided, and (2) WMATA's failure to make sure that the enhanced track circuit verification test (developed following the 2005 Rosslyn near-collisions) was institutionalized and utilized across the entity, which would have identified the faulty track circuit before the accident.

Contributing to the accident were (1) Lack of safety culture, (2) Failure to effectively maintain and monitor the performance of ATC system, (3) GRS/Alstom Signaling Inc.'s failure to provide a maintenance plan to detect spurious signals that could cause its track circuit modules to malfunction, (4) ineffective safety oversight by the WMATA Board of Directors, (5) the TOC's ineffective oversight and lack of safety oversight authority, and (6) FTA's lack of statutory authority to provide federal safety oversight.

Contributing to the severity of passenger injuries and the number of fatalities was WMATA's failure to replace or retrofit the 1000-series railcars after these cars were shown in a previous accident to exhibit poor crashworthiness.

3.2 Washington Metropolitan Area Transit Authority (WMATA)

3.2.1 History and its Mission

The US congress has declared the need of a coordinated system of rail rapid transit, bus transportation service, and highways in the National Capital Region in the National Capital Transportation Act of 1960 and 1965. In furtherance of this policy, Congress, in title Ⅲ of the National Capital Transportation Act of 1960, authorized the District of Columbia (DC), State of Maryland (MD), and Commonwealth of Virginia (VA) to negotiate a Compact for the establishment of the entity to operate public transportation systems in 1966 [21].

Accordingly, WMATA was created by an interstate compact between the three states in 1967 and the Metrorail system started in 1976. Its bylaws state that the mission of the WMATA is "to provide safe, equitable, reliable, and cost effective public transit. WMATA moves the region forward by connecting communities, improving mobility and stimulating economic development." [22]

3.2.2 Financing System and Board Responsibilities

The funding system for a public transportation system like WMATA is explained in the abovementioned National Capital Transportation Act of 1960 and 1965 such that the costs of the facilities are primarily financed by passengers and the remaining costs shared equitably among the Federal, State, and local governments. Thus, WMATA's funding sources are mostly from Federal and Regional governmental authorities except from the operational revenues.

The WMATA's board of eight directors are selected from the Federal government and the regional governments of DC, MD, and VA. Two members are selected from each entity. [23]. According to its bylaws, "The Board is primarily responsible for policy, financial direction, oversight and WMATA's relationships with its customers, jurisdictional partners and signatories." [22]

3.2.3 Current Operation Information

The basic operation and financing information are summarized in following Figure 3-3. The Washington Metro (Metrorail) is the second largest heavy rail transit system in the US after the New York City Subway system. The operation area of the Washington Metro is within three states (i.e. DC, MD, and VA).

The Capital budgets necessary to maintain and improve its transportation's safety are mostly covered by federal and local government's funds, summing up to more than 98 percent.

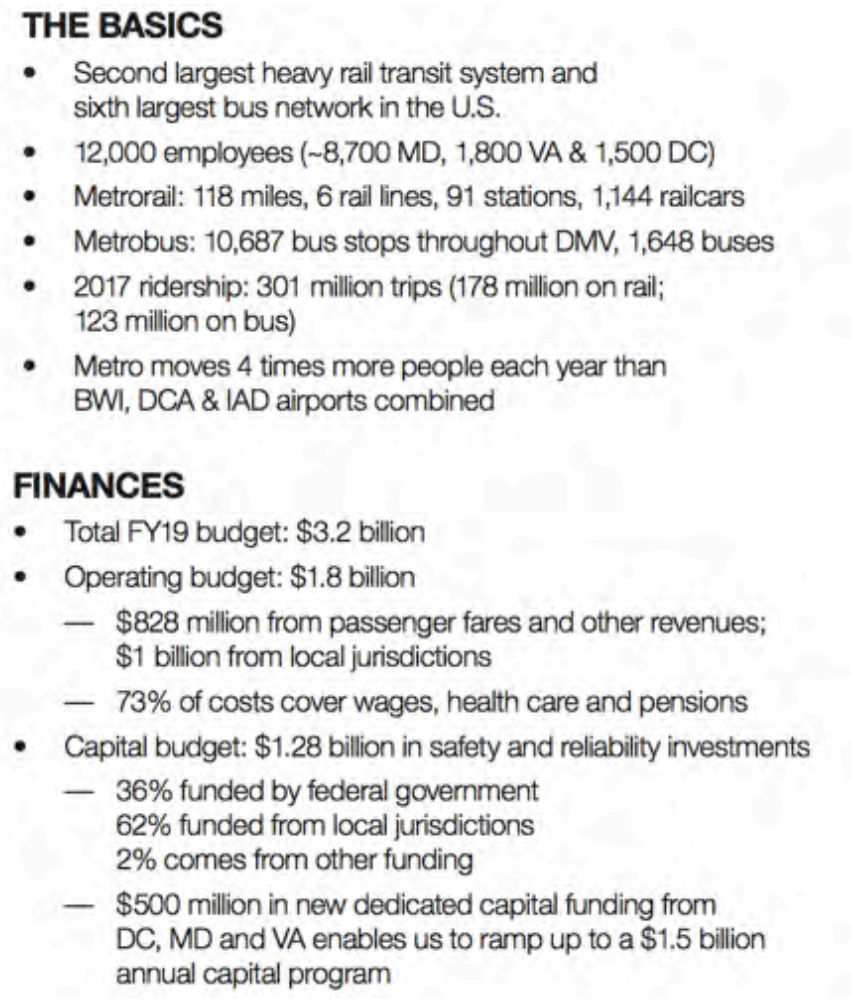


Figure 3- 3 Operation and financing information of WMATA.

(Adapted from WMATA [24])

3.3 System Definition & Hazards

The scope of this analysis includes WMATA's operations, designs, or development actions and its stakeholders within the company and its contractors. Governmental agencies or Audit authorities are also considered as part of the broader system. The evacuation activities are not the focus of this analysis and are considered outside the scope of this thesis.

Leveson [6, Ch. 7] explains that in System Safety engineering, as accident is defined as follows.

Accident: "An undesired or unplanned event that results in a loss of human life or human injury, property damage, environmental pollution, mission loss, etc."

Leveson also asserts that it is useful to assign priorities to the identified losses. In this thesis, Loss of life and injuries (A1) and Economic loss (A2) are considered as accidents, and these were not decomposed into separate accidents. That is, for example, the minor and major injuries might be considered as different Losses, but they are considered as within the same accident definition and not differentiated in this thesis.

According to Leveson, a Hazard is defined as follows.

Hazard: "A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident."

Importantly, a Hazard is not a condition in which the system would normally operate to achieve its goals. For instance, for air traffic control, the state of two planes in the air cannot be a Hazard, but the violation of minimum separation standards would be considered a Hazard.

Another important note about a Hazard is that Hazards should be within the design space of the system designer. That is, system designers, operators, or other controllers need to have control over the Hazards. Accidents can be caused not only by Hazards alone, but may also involve

environmental conditions that the system designers or operators have no control over. This can be expressed as follows:

Hazard + Environmental Conditions → Accident (Loss)

For example, a release of toxic chemicals from a chemical plant can lead to the Loss of human life, but only if there are people around or within the facility. If the worst-case conditions do not exist when the Hazards occur, then accidents may not occur.

Through this analysis, it appears that the most of the conditions that lead to the Losses in the WMATA accident were within the reach of the designers, operators, or other controllers within the system. As Table 3-1 shows, the Losses A1 and A2 could be caused by a combination of H1 and H3, or H2 and H3.

Table 3- 1 System Definition, Accidents, and Hazards

System Definition	・In this analysis, the humans and the non-human physical components such as Trains and Circuit tracks are all considered as part of the overall system. ・Both WMATA components and higher-ranked components, such as legislative authorities or audit authorities, are considered as part of the overall system. ・Operation, Design, and Development are all considered in an analysis. ・Evacuation activities after the accident occurred are not the focus of this analysis, and are considered out of scope.
Accidents	A1: Death and injury of people A2: Economic losses (e.g. Loss of money, property, facilities, etc.)
Hazards	H1: Trains do not maintain the safe distance from each other →Combined with H3 would lead to A1 and A2. H2: Train do not stay on the track (i.e. Train derailment) →Combined with H3 would lead to A1 and A2. H3: Train ejects passengers during a crash.

3.4 Safety Constraints and System Requirements Associated with Hazards

Next, Safety Constraints are identified that need to be enforced so as to avoid the Hazards (See Table 3-2).

Table 3- 2 Safety Constraints and System Requirements

Safety Constraints and System Requirements	SC1. Trains must not violate minimum separation distances → H1 SC2. Trains must not exceed safe speed limits → H1, 2 SC3. Trains must not eject passengers during a crash. →H3

3.5 Safety Control Structure

The high-level safety control structure is depicted in Figure 3-4. A more detailed safety control structure is in Figure 3-5. Non-human components are not colored and the human components are colored gray. More detailed versions of the safety control structure are provided in the following subsections if necessary for fully understanding the relationships between the subsystems.

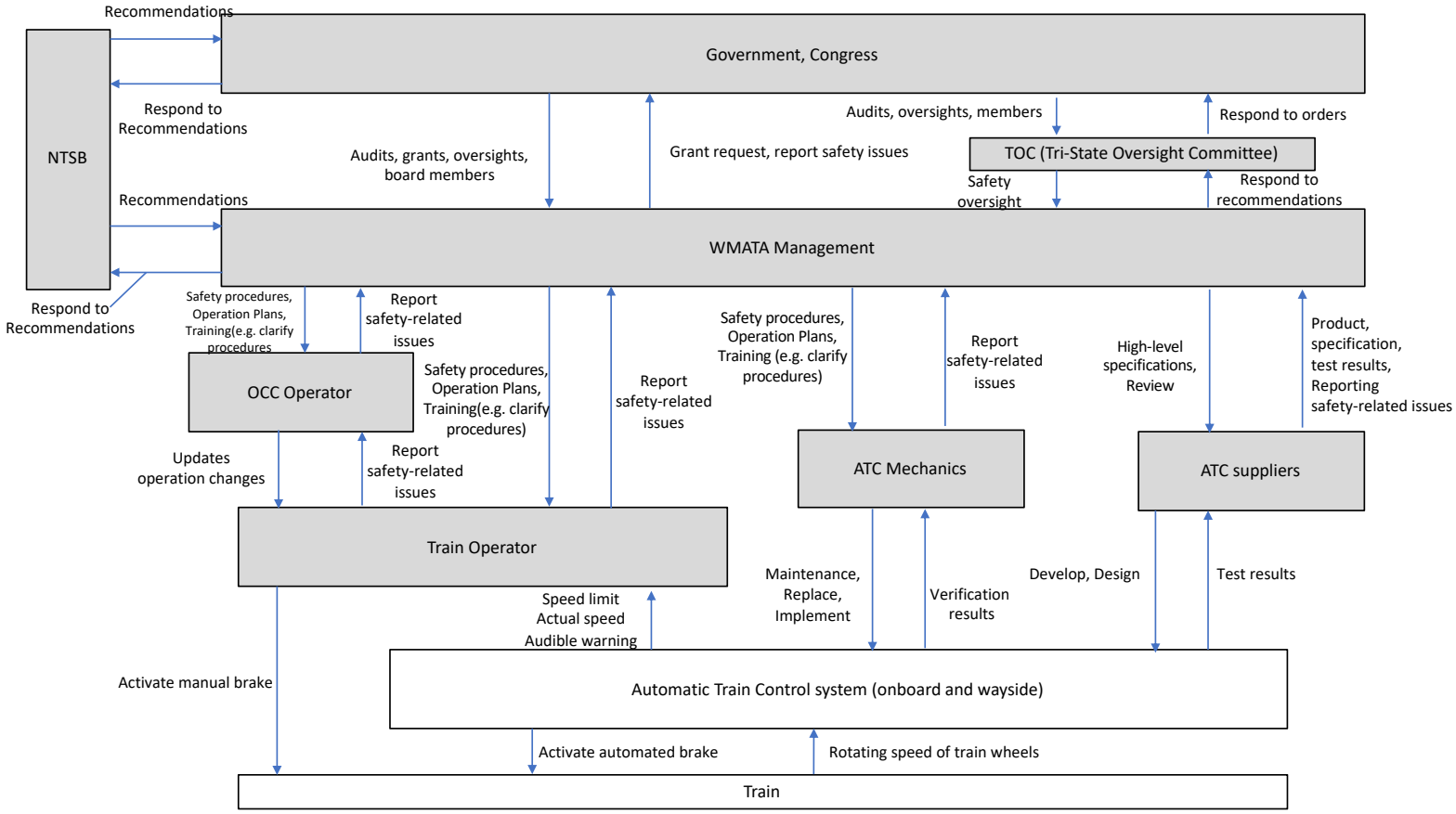


Figure 3- 4 Level 1 High-Level Safety Control Structure of WMATA Metrorail System.

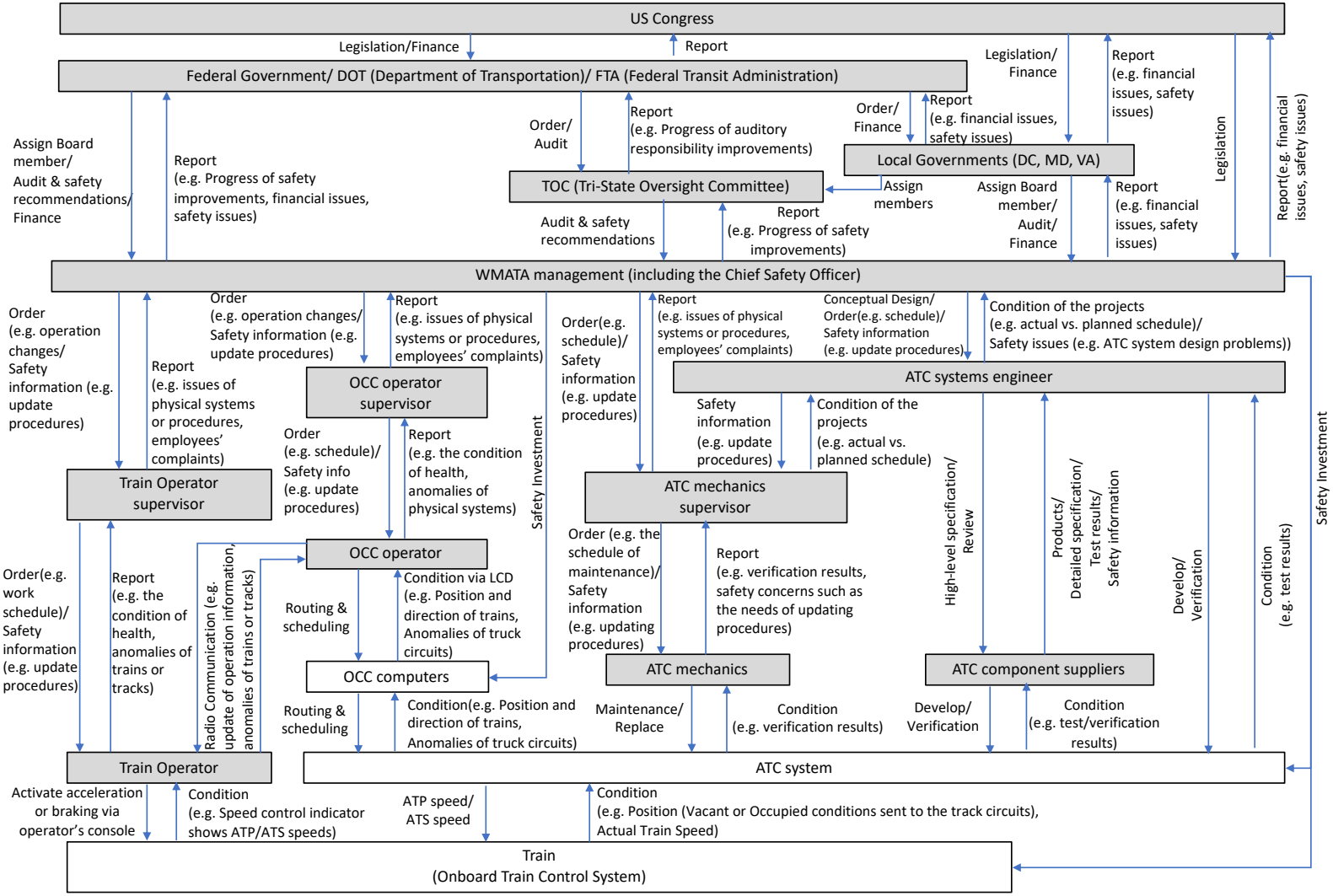


Figure 3- 5 Level 2 detailed Safety Control Structure of WMATA Metrorail System.

Next, the safety-related roles and responsibilities of the main controllers are provided in Table 3-3. The previously identified System Safety Constraints and System requirements must be mapped onto controller and component roles and responsibilities and enforced in the safety control structure [6, Ch. 11].

Table 3- 3 Safety-related Roles and Responsibilities

Controllers	**Safety-related Roles and Responsibilities**
US Congress	・Allocate budgets to governmental agencies ・Provide legislation that enables safe WMATA and governmental agency operations ・Monitor new safety-critical technologies, and allow operators to implement them. ・Monitor operators and ensure they are operating the systems safely ・Collect feedback from governmental and audit agencies and understand the effect of safety recommendations and safety-related regulations ・Ensure the budget allocation to governmental agencies does not prevent safe operations of transportation systems.
Governmental Agencies	・Determine budget allocation to WMATA ・Allocate Board Members to WMATA ・Conduct audits and monitor WMATA's system safety ・Conduct audits and monitor TOC's safety oversight over WMATA's safety, providing safety recommendations ・Make sure WMATA is following their safety recommendations and other safety-related regulations, giving feedback to congress if necessary ・Monitor the latest safety-related technologies, and allow operators to implement them. ・Monitor operators and ensure they are operating the systems safely

	・Make sure the budget allocation to WMATA does not adversely affect safe operation.
TOC	・Conduct audits and monitor WMATA's system safety, providing safety recommendations ・Make sure WMATA is following their safety recommendations and other safety-related regulations, providing feedback to the governmental agencies if necessary ・Monitor the latest safety-related technologies, and allow operators to implement them. ・Monitor operators and ensure they are operating the systems safely
WMATA management	・Make sure that the budgets and investments for maintaining and improving safety are sufficient and appropriately planned and distributed ・Follow and respond to recommendations from governmental agencies and TOC. ・Follow safety-related regulations. ・Create a company-wide safety policy, provide procedures and plans - Provide safety procedures, operation plans, and trainings (e.g. clarify procedures) - Update operation changes and safety procedures when necessary - Create and provide the conceptual design ・Create an effective safety culture ・Collect feedback from employees about any safety-related problems ・Make sure that the safety-related information is circulated, understood, and acted upon effectively and properly. ・Give feedback to upper-level controllers about safety-related issues

ATC Systems Engineer	・Develop and review the specifications of the track circuit replacement project, making sure that replacement or installation of ATC components will not adversely affect safety of train operations. ・Provide safety-related information (e.g. update ATC-related procedures, such as maintenance or implementation), and make sure that ATC mechanics are performing ATC-related component maintenance safely. ・Collect feedback from ATC maintenance teams about any safety-related concerns. ・Collect feedback to upper management about any safety-related concerns. ・Collect safety-related information from suppliers
ATC mechanics supervisor	・ Ensure that team members understand and perform maintenance procedures correctly. This includes making sure that they understand and act upon the latest safety-related notices ・Ensure that the ATC systems perform safely. ・ Collect feedback from his teams about any safety-related concerns. ・ Provide feedback to upper management and ATC system engineers about any safety-related concerns.
ATC mechanics	・Ensure that the ATC systems perform safely. ・ Follow and understand the instructions provided by upper management and supervisors. ・Monitor up-to-date safety-related information ・ Provide feedback to supervisors about any safety-related concerns.
ATC component suppliers	・Provide detailed specifications and carry out verification ・Ensure their components are designed to perform safely when equipped in the WMATA' system ・Provide safety-related information to WMATA

	・Ensure that recommendation are obeyed by WMATA
Train operator	・Maintain minimum distance from other trains by appropriately activating brake ・Monitor the conditions of the train (e.g. train speed) and system anomalies ・Activate manual brake when necessary so that the train speed does not exceed the speed limits. ・Communicate with the OCC operators when necessary to maintain safe operation (e.g. reporting anomalies in ATP speed commands to OCC operators)
OCC operator	・Monitor the whole operation via LCD screens and alarms ・Decide whether certain actions are required to make sure that operations are performed safely. ・Tailor system operation in response to unusual traffic conditions as necessary ・Provide recovery actions in the event of equipment failure or other unanticipated events. ・Send modified ATS speed manually (Can only be relayed to the train within a passenger station using Train-Wayside Communication (TWC)[7]. They cannot modify Automatic Train Protection (ATP)[8] commands, thus they cannot directly control the operations of trains running between stations using ATP system) ・Manually control train movement between stations by changing

[7] According to the official report: "The TWC system provides two-way data communication between carborne and wayside train control systems. This system provides for automatic door operation at stations and for carborne passenger information displays. The wayside system transmits signals to the train using track circuit transmitters. These signals are picked up by receiver coils mounted underneath the lead car of a train. A transmit loop mounted under the front of the lead car transmits information about the train to the wayside system." [13]

[8] According to the official report, "The ATP subsystem is a wayside, meaning along the rail, system designed to provide protection against collision and train overspeed through the automatic block signaling system. In addition, the ATP subsystem provides control of interlockings, route security through interlockings, and control of train door operations." [13]

	signals, alignment of interlockings, or through direct communication with train operators. ・Update operation changes to train operators.
OCC computers	・Monitor the wayside devices on time, and display to Metrorail Operations Control Center (OCC)[9] operators through Liquid-Crystal Display (LCD) ・Send the Automatic Train Supervision (ATS)[10] speed to trains as programmed or as controlled manually by the OCC operator when trains are within the stations ・Between stations, control train movement by changing signals and alignment of interlockings ・Provide alarm sounds and messages if necessary to avoid and correct unsafe conditions ・Record information and monitoring results into a database
ATC system	・Prevent train collisions and train overspeed[11] ・Determine routing and scheduling of trains ・Monitor train locations and the condition of interlockings ・Maintain train separation by transmitting and enforcing ATP speed, ATS speed, and the programmed station stop speed profile.

One way to analyze an existing organizational or social safety control structure is with a gap analysis, which can be used to "determine where the responsibility for implementing each

[9] According to the official report: "Train operations on the Metrorail system are carried out under the authority and supervision of the Metrorail operations control center (referred to in this report as the OCC), located in downtown Washington, D.C. The OCC is responsible for providing positive control over all station activities, train movements, and subsystems (power, ATC, automatic fare collection, and communications) necessary for the efficient movement of passengers. The OCC also manages all emergency situations, which includes contacting fire, police, and medical services as required." [13]

[10] According to the official report: "The automatic train supervision (ATS) subsystem is primarily a wayside system with some OCC inputs. The ATS system is designed to control train routing and scheduling. Scheduling is accomplished first by automatic equipment at the wayside, then, second, by computer programs at the OCC, which are automatically triggered when necessary to provide for minor schedule adjustments to maintain traffic flow and scheduling." [13]

[11] According to the official report: "the Metrorail ATC system … was designed to detect the presence of trains along the main line and to prevent collisions by transmitting speed commands that either stop or slow following trains in order to maintain safe separation." [13]

requirement rests." This analysis would "identify holes in the current design, that is, requirements that are not being implemented (enforced) anywhere" [6, Ch. 8.6].

In the following steps of WMATA accident analysis, the gap analysis idea is considered. If gaps are found, then the safety structure should be redesigned and these results can drive additional recommendations for WMATA.

3.6 Proximal Event Chain Leading to the Loss

3.6.1 Proximal Event Chain

The main events leading to the accident are listed in Table 3-4. Train 214, the struck train, was facing congested traffic and had been experiencing temporary slow-downs several times. Train 214 departed Takoma station and moved into track circuit B2-304. As B2-304 had malfunctioned and had not been detecting trains in the past 5 days, train 214 became invisible to the ATP system. Due to the design, train 214's operator console indicated 0 mph speed commands and automatically stopped, because the "invisible" trains do not receive speed commands. The operator had no reason to believe the ATC system is malfunctioning because it is very common to receive 0 mph speed signal during congested times.

Meanwhile, train 112, the striking train, departed from Takoma station after train 214. As her train was approaching train 214, the operator got a stop signal from the ATC system and stopped momentarily. As soon as train 214 stopped completely on the track circuit B2-304, she then received non-zero speed signal, because ATP system "believed" that there is no train on the B2-304, indicating that it is safe for train 112 to enter that track circuit. Although she activated emergency brake just after she saw the train 214, it was too late to prevent the collision.

Although track circuit B2-304 had been malfunctioning for days and consistently not detecting trains, no one had noticed and reported it before the accident.

Table 3- 4 Proximal Event Chain Leading to the Loss

Timeline	Train 214 (struck train)	Train 112 (striking train)	Track circuit B2-304		Other operators
5 days before the accident				The transmitter impedance bond of the track circuit B2-304 was replaced.	
				After the replacement of the track circuit components in 5 days before the accident, B2-304 consistently did not detect trains (ATP system believed that the track circuit was always "vacant")	・No OCC operator was recognizing and reporting the problem of the track circuit B2-304, although alarms would have been generated on the OCC LCD screen. ・No train operator was recognizing and reporting the problem of the track circuit B2-304, although the 0mph
June 22, 2009, 3:28 p.m.	The train operator of the struck train 214 reported for the Shady Grove station.				
3:50 p.m.		The train operator of the striking train 112 reported for Brentwood Yard.			
	Train 214 arrived and departed Silver Spring station				
4:33 p.m.		Train 112 departed Silver Spring			
	Train congestion caused train 214 to slow multiple times between Takoma and Fort				

	Totten stations.				ATP speed was generated on the operators' console when the train was traversing the track B2-304.
	Train 214 occupied track circuits B2-312 and B2-304.		Part of train 214 was on the track circuit B2-304. ATP was still recognizing the train presence, as part of the train was on the track circuit B2-312.		
4:56:41 p.m.		Train 112 stopped briefly just after leaving Takoma station, because the presence of train 214 caused ATP to send speed commands change train 112 from 55mph to 0mph.			

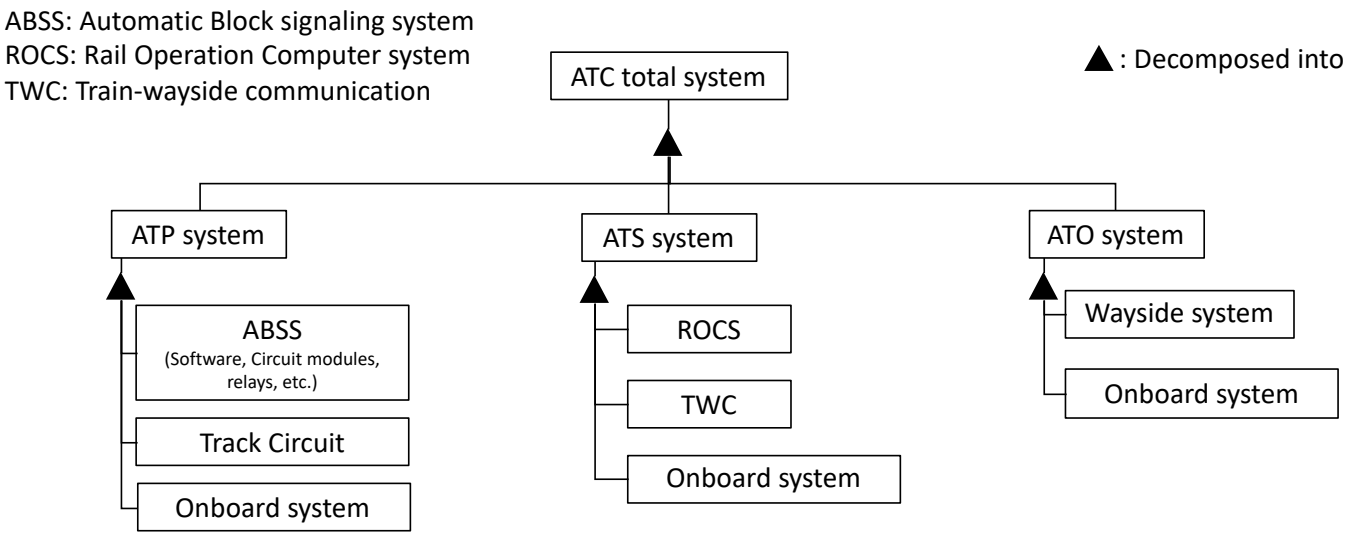
	Train 214 moved completely onto track circuit B2-304, and the track circuit did not detect its presence.		With all of train 214 within track circuit B2-304, the ATP system no longer detects its presence.		
	No ATP speed command is sent to train 214, because ATP only transmits speed signals to the detected trains. Thus, train 214 received 0mph as a default due to the design.				
	Train 214 was completely stopped on the track circuit B2-304.				
4:57:20 p.m.		As a result of the ATP system no longer detecting Train 214, train 112 was sent non-zero ATP speed commands. Train 112 started moving.			

		Once train 214 came into full view, train 112's operator activated the emergency brake.			
	Collision occurred. The train operator of train 214 felt a "big push" and heard noise toward the rear of his train.				
4:58:08 p.m.	Third-rail power was lost				

3.6.2 The responsibilities of ATP system and how it works

In order to properly understand this timeline, one would need to understand how the Automatic Train Protection (ATP) system, the component of the Automatic Train Control (ATC) system, works and what the track circuits' role is in accomplishing ATP's responsibility. The ATC's 2 level decomposition and the responsibilities of ATP, Automatic Train Supervision (ATS), and Automatic Train Operation (ATO)[12] are provided in Figure 3-6.

[12] According to the official report, "The ATO subsystem is primarily a wayside system. The ATO subsystem is designed to manage train startup and acceleration, maintain running speed en route, and stop the train smoothly at the proper position along the station platform. Running speed is based on the lower of three speeds: the maximum permitted (ATP) speed, the ATS speed, and the programmed station stop speed profile." [13]



ATP system's main responsibility

To protecting train collisions and train overspeed
BY Maintaining train separation by transmitting speed commands to each train. and
BY Monitoring train locations and the condition of interlockings

ATS system's main responsibility

To Routing and scheduling of trains
BY sending the speed commands to the train
USING TWC (Train-wayside communication) within the limits of a passengers station

ATO system's main responsibility

To Managing train startup and acceleration, maintaining running speed en route, and stop the train smoothly at the proper position along the platforms
BY enforcing the train to observe the lower of ATP speed, ATS speed, and the programmed station stop speed profile.

Figure 3- 6 ATC's 2 Level Decomposition and Responsibilities of Subcomponents.

Next, the detailed safety control structure of the ATP system and its subsystems' safety responsibilities are shown in Figure 3-7. Figure 3-8 explains how the ATP system detects trains.

Main Safety Responsibilities of ATP system

ATP total system

- Maintaining train separation by transmitting speed commands to each train.
- Protecting collision and train overspeed

ABSS (Automatic Block Signaling System)

- Detecting the location of trains and selecting the proper command to be transmitted to the train
- The speed commands are calculated **based on the instantaneous track conditions ahead of the train.** Note that the algorithm used for computation does not consider any information regarding the past status of track occupancies or speed commands **(i.e. even if the train suddenly disappear as in this accident, the system does not generate and send 0mph commands to the following trains).**
- Sending the speed commands to the train via train circuit
- Ensuring that trains observes speed limits and the trains are separated safely

Track Circuit

- Interpreting whether trains are on it or not by observing the condition of the track relay, sending this information to ABSS
- Sending the speed commands to the trains

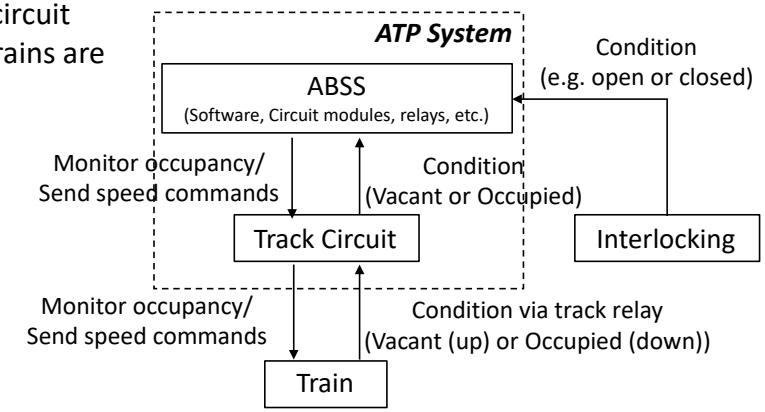


Figure 3- 7 Main Safety Responsibilities of ATP system.

Track relay[1]



Note

1. **This track relay is not the one used in WMATA**

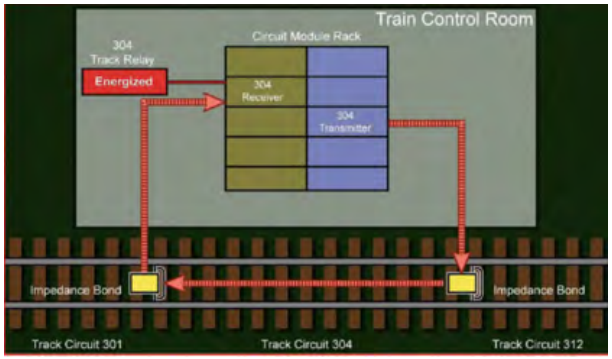
Source: https://www.railroadsignals.us/support/relays/#US&S_Relays_

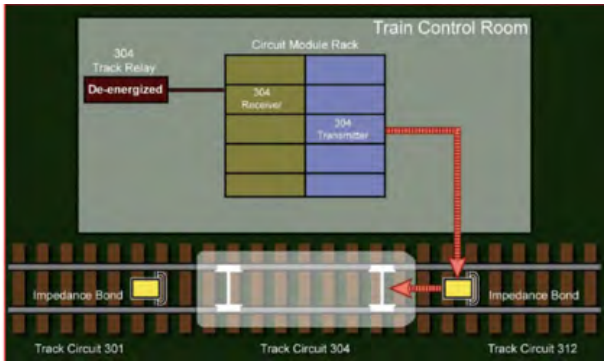
Track circuit module



Impedance bond







When the track circuit is not occupied by a train (Left picture)

- Track circuit modules are located in a control room at the nearest train station.
- The transmitter module sends a signal to the corresponding transmitter impedance bond.
- The signal passes through the rails to the adjacent receiver impedance bond.
- From there, the signal travels back to the control room to the receiver module and energizing the track relay.
- ATP would allow following trains to enter this track.

When the track circuit is occupied by a train (Right picture)

- The train's wheels create an alternate path for the electrical signal.
- The signal never reaches the receiver module, and the track circuit de-energizes, indicating it is occupied.
- ATP would never allow following trains to enter this track.

Figure 3- 8 How ATP System Detects Trains[13].

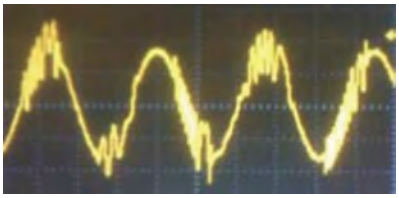
[13] The two pictures in the bottom of the figure are retrieved from NASA's presentation [25].

3.6.3 How ATP system became incapable of detection

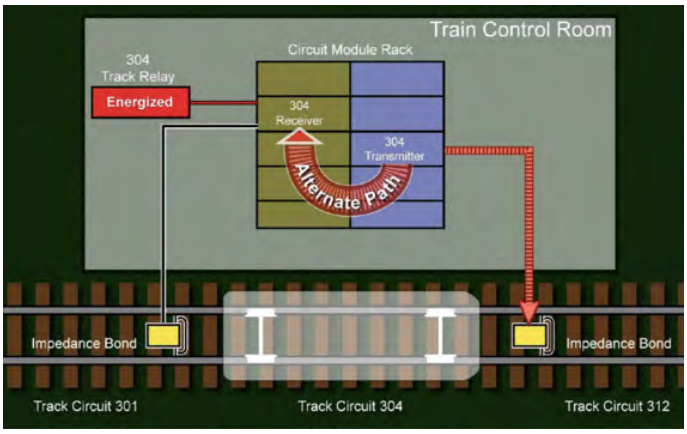
Now that the track circuit and ATP system is understood, it's the time to understand what caused the ATP system to stop detecting trains. The schematic explanation is shown in the following Figure 3-9.



Healthy Oscillation found in a receiver module



The spurious signal from the transmitter circuit is superimposing to the clean audio waveform of a receiver module, causing the irregular thickened portions.



・Spurious signal generated in the transmitter circuit module migrated through the rack structures into the receiver circuit module via unintended alternate path

・The track relay was always energized even when the train was on the track.

Figure 3- 9 Oscilloscope displays of the receiver circuit module (Left) and The schematic explanation of how ATP system became incapable of detecting trains (Right).

(Left: Adapted from NTSB [13], Right: Adapted from NASA [25])

First, the power output transistors of the track circuit module transmitter were producing parasitic oscillation. Secondly, this oscillation enabled the signal to travel an unintended alternate path through the rack structures to the respective receiver module. Thirdly, the oscillation was coupled to the receiver module for that track circuit, producing a decaying pulse that was synchronized with the track circuit audio frequency. If the decaying pulse were sufficiently high amplitude to drive the receiver module, the track relay would be energized, falsely informing ATC system that the actually occupied track circuit was vacant.

3.7 Analyzing the Physical Process

Next, the physical processes are analyzed. The main physical systems in this accident are two trains (train 112 and train 204) and train circuit, which is a part of the ATP system. The Safety responsibilities, Physical Controls, Failures and Inadequate Controls, and Contextual Factors are summarized in following Table 3-5 and Table 3-6.

Table 3- 5 Analysis of the Physical Process (Track Circuit B2-304)

Safety responsibilities (what must it do)
SR1. (Violated) Notify ATP whether trains are on the track circuit or the track circuit is vacant. SR2. (Violated) Notify operators when a malfunction has occurred SR3. (Violated) When components malfunction, provide a fail-safe condition
Physical Controls: Partial List (what design features were meant to fulfill the safety responsibilities)
For operation ・Transmitter impedance bond ・Receiver impedance bond ・Train Circuits modules ・Cables ・Track Relay ・Alarms on the OCC consoles when the train circuits are malfunctioned
Failures and inadequate controls (what went wrong)
F1. After the **receiver** bond was replaced in December 12, 2007, B2-304 began falsely de-energizing its track relay intermittently. The historical data shows this had been continuing until

when the **transmitter** bond was replaced (Non-direct cause of the accident)

F2. After the **transmitter** impedance bond was replaced in June 17, 2009, B2-304 began always incorrectly energizing its track relay, and **ATC was always indicating that the track circuit was vacant.**

Contextual Factors (why did those things go wrong)

C1. B2-304 was not maintained properly so that the ATP software can detect trains as required.

- Firstly, B2-304 began bobbing[14] and sometimes incorrectly indicated occupancy after the US&S's new **receiver** impedance bond was installed in 12/12/2007 (No analysis is provided about why B2-304 did not indicate occupancy). The bobbing problem was not solved over 1.5 years leading up to the 5 days before the accident (6/17/2009). Importantly, B2-304 did not be incapable of detecting trains at this point. →F1

- Secondly, as a part of the installation of the transmitter impedance bond in 6/17/2009, the power level of the circuit module was increased. As a result, the parasitic oscillation was emerged in the transmitter module. Then, the spurious signals migrated through the equipment rack structure, which was an unintended path, finally reaching out to the receiver module. This caused the track relay to be in "up" position (i.e. indicating "vacant"), and B2-304 began not detecting a train. →F2

C2. An ATC mechanics team, who was in charge of installing the transmitter bond, verified that the B2-304 was properly functioning and detected trains properly using 3-position-shunt-test. However, contrary to their statement, the historical data shows that the track began not detecting trains after the installation. →F2

C3. Another ATC mechanic team, in charge of preventative maintenance, verified that the B2-304 was functioning properly using only 1-position-shunt-test. The historical data shows the track continued being incapable of detecting trains after verification. →F2

[14] Bobbing refers to the case where the train detection is transitioning from (1) vacant (2) and then to occupied, (3) and finally back to vacant again without any trains present.

C4. No train operators reported a loss of speed commands when the trains were traversing the track B2-304. →F2

C5. It seems that no OCC operators noticed a false vacancy indication (and alarms), which would have been displayed on the LCD Display. This is at least partially because such alarms were identified as "minor", in which alarm messages appear only briefly and deleted automatically without human intervention. →F1, F2

C6. The replacement of the receiver bond was part of the "traction power upgrade program", which was needed to increase the train capacity for the increased ridership

C7. The replacement of the transmitter bond was part of the "track circuit replacement program", which was needed because of the aging, parts availability, and failing parts.

C8. The ATP speed is generated locally, at a nearby train control room. OCC cannot manipulate or intervene the ATP speed generation.

As explained in the previous subsection, the track circuit B2-304 had malfunctioned and did not detect trains on it because (1) parasitic oscillation was generated in the transmitter module, (2) it was migrated through the unintended alternate path through the receiver module, and (3) the amplitude of the spurious signal was high enough to mimic the real signal.

The safety responsibility of the track circuit B2-304 was not met as it did not generate and send proper decision-making information to an ATP software.

B2-304 was falsely energizing its track relay after the transmitter bond was replaced in June 17, 2009, 5 days before the accident (F2). B2-304 also had not been properly de-energizing its track relay after the receiver bond was replaced in December 12, 2007, a year and half before the accident (F1).

There are many contextual factors which affected the failures. These include (1) The increased power level of the circuit module, (2) incorrect verification test's procedure by two different ATC mechanic teams, (3) ineffective circulation of the latest safety-related information, and (4)

downgrading the alarm category for malfunctioned ATC system from “major” to “minor”.

Table 3- 6 Analysis of the Physical Process (Trains)

Safety responsibilities
SR1. (Violated) Maintain safe distance from other trains by appropriately activating brake
Physical Controls: Partial List
・Onboard train control system ・Acceleration and Braking ・ATC system (ATC’s subsystems are mainly Wayside system. But subsystems of ATP, ATS, and ATO include onboard equipment) ・Radio communicating system with COO
Failures and inadequate controls
F1. Did not have enough strength (Crashworthiness) so that the trains could protect passengers in the train **F2.** Applied emergency brake too late (Train112) **F3.** Did not maintain safe distance from other trains (Train112)
Contextual Factors
C1. ATP system provided unsafe information to both trains (0mhp to the train 214, and non-zero speed commands to the train 112).

In this accident, trains were functioning correctly as designed. The train’s safety was largely dependent on the ATP system, which became incapable of operating safely, thus the trains were in an unsafe condition. The inadequate crashworthiness of the train might have increased the severity of the accident (F1). The emergency brake was applied by the human operator but it was too late (F2).

3.8 Analyzing the Higher Levels of the Safety Control Structure

In this section, components in the higher levels are analyzed step by step. They are analyzed in terms of (1) Safety Requirements and Constraints, (2) Unsafe Control Actions (UCAs), (3) Mental Model Flaws, and (4) Context in which Decisions Made.

3.8.1 Operator-Physical System Level

3.8.1.1 Analysis of the Operator-Physical System Level

Firstly, the components in Operator-Physical System Level are examined. In the Safety Control Structure, these components are located at the bottom of the Structure as colored red in following Figure 3-10.

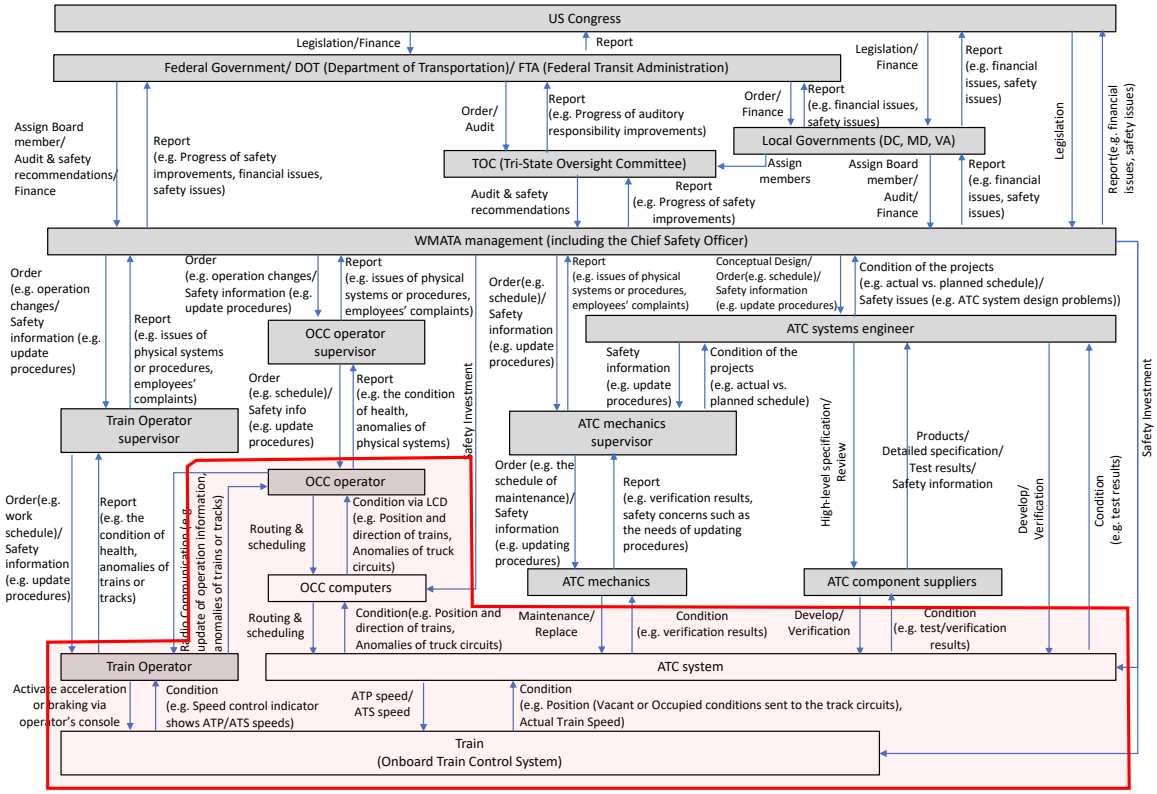


Figure 3- 10 Operator-Physical Interactions in the Safety Control Structure.

A detailed version of the Safety Control Structure is shown in Figure 3-11. The analysis was carried out for the four components in this level, each having important roles in this accident. Specifically, these are: 1) ATP system; 2) Train Operator; 3) OCC Computers; and 4) OCC operator. These are numbered and highlighted in red in Figure 3-11.

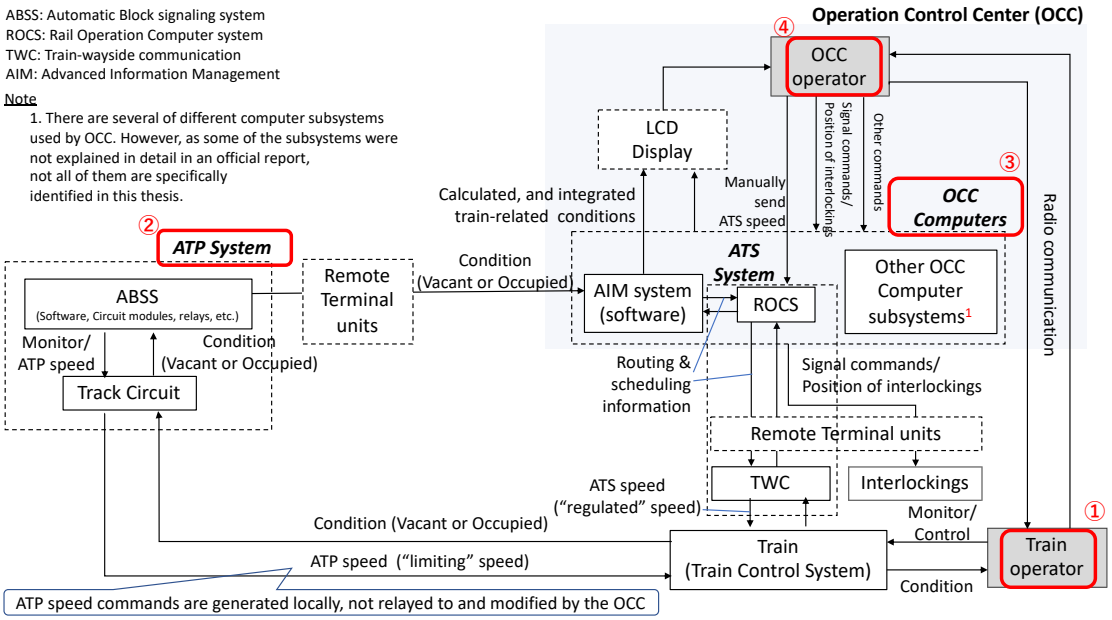


Figure 3- 11 Detailed View of Safety Control Structure (Operator-Physical System Interactions).

(1) Train Operators

First, Train operators were examined and the results are shown in Table 3-7.

Table 3- 7 Analysis of the Train Operators

Safety Requirements and Constraints (What goals they should achieve)
SR1. (Violated) Maintain safe distance from other trains by appropriately activating the brake **SR2.** (Violated) Activate manual brake when needed so that the train does not exceed speed limits. **SR3.** (Violated) Communicate with the OCC operators if necessary to maintain safe operation (e.g. reporting the

anomalies in ATP speed commands to OCC operators)
Unsafe Control Actions (What they did that was unsafe)
UCA1. (Train operator of train 112) Train operator of train 112 applied emergency brake too late → SR1 **UCA2.** (Train operators other than train 112 and 214) Previous train operators did not report and/or realize the anomalies in the ATP speed command when traversing the malfunctioned track circuit B2-304 → SR2,3
Mental Model Flaws (What did they believe about the system that explains their actions)
MMF1. Believed that the ATP speed signal was correct and there is no malfunction in the track circuits nor the ATP system.
Context in which Decisions Made (What other factors - pressures, incentives, history, etc. - explain their actions)
C1. ATP system provided unsafe speed signals to both trains (i.e. 0mhp to the train 214, and non-zero speed commands to the train 112). **C2.** Low quality safety culture[15] **C3.** There may have been no clear procedure or training about what the train operators needed to do when the ATP speed signal changes suddenly from non-zero to zero, then back to non-zero,

[15] The official report explains low quality of safety culture as follows: "The report also discusses how shortcomings in WMATA's internal communications, its recognition of hazards, its assessment of risk from those hazards, and its implementation of corrective actions are all evidence of an ineffective safety culture within the organization. Examples described in the report include the low priority that WMATA Metrorail managers placed on addressing malfunctions in the train control system before the accident, which likely influenced the inadequate response to such malfunctions by automatic train control technicians, operations control center controllers, and train operators; and the fact that before the accident the position of chief safety officer lacked the necessary resources and authority, within the organizational structure of WMATA, to adequately identify and address system safety issues and ensure the distribution of safety-critical information throughout the organization." [13]

which could indicate a malfunction of the ATC system. →MMF1

(2) ATP System

The ATP system was analyzed and the results are shown in Table 3-8. Please note that most of the analysis results for this component are similar or the same as that of Track Circuit B2-304 as analyzed previously. This is because the track circuit is a subsystem of ATP system. The reason the ATP system is analyzed here is that the ATP system has software that the track circuit does not have, thus its Process Model Flaw contributed severely to this accident, meaning it is worth examining ATP system separately from track circuit.

Table 3- 8 Analysis of the ATP System

Safety Requirements and Constraints
SR1. (Violated) Protect against collision and train overspeed by automatically applying brakes when necessary **SR2.** (Violated) Monitor train locations and the condition of interlockings **SR3.** (Violated) Maintaining train separation by transmitting appropriate speed commands (ATP speed commands) to each train
Unsafe Control Actions
UCA1. The ATP system did not generate or send 0mph speed command to the train 112 (the striking train) even though train 214 had suddenly disappeared a second ago. Instead, it sent non-0-speed to the train 112. →SR1,3
Process Model Flaws
PMF1. The software of the ATP system believed that train 214 was not on track B2-304 because the track relay was in "up" position when train 214 was in the middle of the track circuit. That

is, it believed that the track circuit B2-304 was vacant→UCA1, SR2

PMF2. ATP software generates a train speed command based on the instantaneous track occupancy conditions ahead of the train. It believed that if it sees there is no train on the track B2-304 from the current relay position, it can conclude that there is no train even if there was a train a second ago. →PMF1

Context in which Decisions Made

C1. B2-304 was not maintained properly so that the ATP software can detect trains as required.

- Firstly, B2-304 began bobbing and sometimes incorrectly indicated occupancy after the US&S's new **receiver** impedance bond was installed in 12/12/2007 (No analysis is provided about why B2-304 did not indicate occupancy). The bobbing problem was not solved over 1.5 years leading up to the 5 days before the accident (6/17/2009). Importantly, B2-304 did not be incapable of detecting trains at this point.
- Secondly, as a part of the installation of the transmitter impedance bond in 6/17/2009, the power level of the circuit module was increased. As a result, the parasitic oscillation was emerged in the transmitter module. Then, the spurious signals migrated through the equipment rack structure, which was an unintended path, finally reaching out to the receiver module. This caused the track relay to be in "up" position (i.e. indicating "vacant"), and B2-304 began not detecting a train. →PMF1

C2. An ATC mechanics team, who was in charge of installing the transmitter bond, verified that the B2-304 was properly functioning and detected trains properly using 3-position-shunt-test. However, contrary to their statement, the historical data shows that the track began not detecting trains after the installation. →C1

C3. Another ATC mechanic team, in charge of preventative maintenance, verified that the B2-304 was functioning properly using only 1-position-shunt-test. The historical data shows the track continued being incapable of detecting trains after verification.→C1

C4. No train operators reported a loss of speed commands when the trains were traversing the

track B2-304→PMF1

C6. It seems that no OCC operators noticed a false vacancy indication (and alarms), which would have been displayed on the LCD Display. This is at least partially because such alarms were identified as "minor", in which alarm messages appear only briefly and deleted automatically without human intervention.→PMF1

C7. The replacement of the receiver bond was part of the "traction power upgrade program", which was needed to increase the train capacity for the increased ridership

C8. The replacement of the transmitter bond was part of the "track circuit replacement program", which was needed because of the aging, parts availability, and failing parts.

C9. The ATP speed is generated locally, at a nearby train control room. OCC cannot manipulate or intervene the ATP speed generation.

(3) OCC Computers

Third, OCC computers are analyzed and the result is shown in Table 3-9. The important point here is that OCC computers were functioning as designed but could not achieve the Safety Requirement of ensuring safe operation of the trains (SR1). In addition, it generated too many alarms due to substantial number of track circuit malfunctions (8,000/week), and one can argue that the OCC operators were hardly capable of responding to every alarm. Even worse, because of the high number of alarms, WMATA decided to categorize the alarms caused by track circuit malfunctions as “minor,” so that the alarms were deleted without human intervention.

Due to the high occurrence of bobbing problems with the track circuit, a “ghost train,” which could be generated on the OCC computers by falsely interpreting bobbing track circuit as an actual train, was designed to be deleted within 30 seconds and without any alarms. This feature of

Advanced Information Management (AIM) [16] system, a subsystem of OCC computers, was problematic as even when there is an actual train on the next track circuit, and the next track (in this case, track B2-304) is not detecting the trains properly, the AIM system deletes the train image from the LCD display. In this accident, the track circuit B2-304 was determined to be occupied at first, then indicated unoccupied, when the train completely stopped within the track circuit B2-304. This made the AIM system believe that this is a false virtual train (it may have been recognized as ghost train), and the icon was deleted (See Figure 3-15, 3-16, and 3-17 to see how train 214 was deleted from the OCC LCD display just before the accident happened). Although it seems it was only the AIM system that detected the anomalies in the track circuit, this system could be designed differently based on the risk that the actual train was still on the track. The AIM system was not designed to stop train operations by, for example, sending zero ATP speed to every train around the area of the questionable track circuit.

It is not perfectly clear from the available information how the AIM system algorithm worked, but the algorithm concluded that the train indicator of the train 214 was a false train indication. As explained earlier, possibly because the track circuit B2-304 (the malfunctioned track) was identified as bobbing and the previously indicated train image on the track B2-304 was determined to be a "ghost train". The algorithm decided delete the train indication even though the previous track circuit B2-312 was indicating it was occupied (for detail, see Figure 3-15, 3-16, and 3-17).

This thesis does not dig into the specific solutions for the algorithm design because the available information is insufficient, such as a detailed design for the current algorithm. But this thesis can provide some basic recommendations for the algorithm and the system design:

1. Redesign the AIM system such that it will request the OCC operators to take actions (e.g. stop trains) or automatically stop trains if necessary (e.g. if the computer is suspicious about the incapability of track circuits detecting trains).

[16] According to the official report: "The software used to manage the data transmitted to the OCC from remote terminal units in the field was developed by Aeronautical Radio, Inc., and is known as the Advanced Information Management (AIM) system. Using AIM data, a graphics package called "Animator" creates the information displayed on OCC controller LCD screens. The AIM display was designed to provide controllers with the information they need to manage traffic flow around the rail system and to recognize and respond to one-time events such as isolated equipment failures." [13] See the NTSB official report for more detail in section "Data Management and Train Status Display," beginning in its page 26 [13].

- Evaluate the design of the new algorithm for the AIM system to distinguish between actual “ghost trains” (false positive detection) and the track circuit anomalies that may prevent detection of trains (false negative detection). The current algorithm may simply delete trains from LCD display any time detection is lost, making it too difficult for the OCC operators to recognize and acknowledge anomalies in the track circuits. The AIM system is already equipped with the ability to monitor the track circuit function (e.g. bobbing or not detecting trains), thus the new design should be able to utilize the AIM’s monitoring capability. By redesigning the algorithm, a malfunctioning track circuit like B2-304 could be recognized as having anomalies by, for example, tracing the historical data of the track occupancy of a train (i.e. in this accident, the train 214). By doing so, the new algorithm would recognize that train 214 was valid for a long period of time before disappearing suddenly, and could conclude that the track circuit B2-304 had some anomalies and was not detecting trains.
- Evaluate the operation strategy of sending stop signals (i.e. zero ATP speed signal) to the following trains when the track circuit is classified as “suspicious to be incapable of detecting trains” (i.e. when the algorithm determines that the track circuit is not (just) bobbing, but not detecting trains). The stop signal should be sent either automatically by the OCC computer or by the OCC operators’ input.

2. Identify and evaluate the ways ATP speed can be manipulated and overridden by a human operator and/or OCC computer if necessary. For example, a potential design change of the OCC computer may directly send ATP speed to the trains between stations and also provide OCC operators with the capability of manipulating ATP speed via OCC computers.

Table 3- 9 Analysis of the OCC Computers

Safety Requirements and Constraints
SR1. (Violated) Make sure that trains are operated safely and timely **SR2.** Monitor the wayside devices on time and display to OCC operators through LCD Display

SR3. Send the ATS speed to trains as programmed[17] or as controlled manually by the OCC operator when trains are within the stations

SR4. Between stations, control train movement by changing signals and alignment of interlockings

SR5. (Violated)
Provide alarm sounds and messages when necessary to avoid and correct unsafe conditions

SR6. Record real-time information and monitoring results into a database

Unsafe Decision and Control Action

UCA1. OCC Computer made too many track-circuit alarms (more than 8,000 alarms per week), which would have made OCC controllers less sensitive to the track circuit malfunctions.
→SR1,5

UCA2. OCC Computer (AIM system) did not recognize that the train 214 disappeared suddenly when the train entered malfunctioned track B2-304, and did not generate the zero ATP speed commands to the following trains. This is because AIM system was not designed to do track train movements over time and send zero ATP speed when the track circuit has anomalies (***Design problem***).

Process Model (Flaw)s

PMF1. The computer believed that the conditions categorized as "minor" or "ghost train" are not affecting safe operation when the human operator does not intervene within 30 or 60 seconds. (This is because it was designed to do so.)

PMF2. The computer believed it was not required to send 0mph commands to the following trains even when proceeding trains suddenly disappears. (This is because it was designed to do so.)

[17] "programmed" refers to the situation when OCC computers act based on its pre-programmed algorithm, whereas "controlled" refers to that when human operators (OCC operators) input the ATS speed command onto the OCC computers.

→UCA2
Context in which Decisions Made
C1. There were many track-circuit-related malfunctions across Metrorail. →UCA1 **C2.** Because of the high occurrence of not detecting trains and incorrectly detecting trains, the associated errors and alarms had been categorized as "minor". The minor alarms would automatically be deleted by computer without human intervention. These alarms were generated about 8,000 times per week. →MMF1 **C3.** Because of the high occurrence of the "ghost train" generated by the bobbing circuit track, if the track circuit is bobbing (changed its status from vacant, to occupied, to vacant again with no consistent train traffic present), the AIM software was designed to delete the train image without generating an alarm within 30 seconds. The causes of the bobbing were not specifically mentioned in the report. The ghost trains were deleted by AIM system more than 1,000 times per week. →MMF1 **C4.** OCC computers cannot modify speed commands of the trains between stations, thus even if the train suddenly disappears as in this accident, the system does not generate and send 0mph commands to the following trains (***ATC design problem***).→MMF2 **C5.** The detection malfunctions of B2-304 would have generated alarms, but it was programmed to cancel itself without any intervention from OCC controllers in 30 or 60 seconds. (***ATC operation problem***) → MMF1 **C6.** The algorithm used in the AIM system did not track the history of how trains had been moving. The train 214 was occupying previous track B2-312, and suddenly disappeared when it entered B2-304. Thus, if it tracked the history of train movements, it could have detected that the train has falsefully disappeared due to track circuit anomalies. It also was not programmed to take actions in response, like stopping other trains around the questionable track circuit by sending zero ATP speed signals. (***ATC algorithm design problem***) →MMF2

(4) OCC Operators

Finally, OCC operators are analyzed and the result is shown in following Table 3-10.

They are in charge of monitoring the whole operations of trains and infrastructures. The OCC computers alarmed the anomalies in the track circuits, including the B2-304, but those were too prevalent to deal with all of them properly in a timely fashion. The managerial decision of making those alarms as “minor” seems to be problematic but considering the high occurrence of alarms and human capability to deal with malfunctions, it might have been a last resort for the managers. The other problem for OCC operators seems to be the unavailability of changing the ATP speed manually by the operators (***ATC design problem***).

The situation where OCC could not deal with the unsafe on-site situation seems to be caused by WMATA’s unsafe managerial decisions and its low-quality safety culture.

Table 3- 10 Analysis of the OCC Operators

Safety Requirements and Constraints
SR1. (Violated) Monitor the overall operation via LCD screens and alarms, and decide what actions are required to make sure that overall operation is maintained safely. **SR2.** If necessary, adjust system operation in response to unusual traffic conditions **SR3.** (Violated) Provide recovery actions in the event of equipment failure or other unanticipated events. **SR4.** Send modified ATS speed manually (This can be relayed to the train only within passenger stations using TWC. Operators cannot modify ATP commands, thus they cannot directly control the operations of trains running between stations using ATP system.)

SR5. (Violated) Manually control train movement between stations by changing light signals for train operators, alignment of interlockings, or through direct communication with train operators. **SR6.** Update operation changes to train operators.
Unsafe Control Actions
UCA1. The OCC operators did not instruct the train operator of train 112 to stop manually (It seems the radio communication system was the only way for OCC operators to stop train 112 at the time) → SR1,3,5
Mental Model Flaws
MMF1. There were many alarms and the operators may have believed they did not have to pay close attention to every alarm. →UCA1 **MMF2.** They believed that B2-304 was functioning properly and detected trains correctly. →UCA1
Context in which Decisions Made
C1. There were many track-circuit-related malfunctions across Metrorail. Thus it would be difficult to notice the alarm due to track circuit B2-304's alarm and how urgent it is.→MMF1 **C2**. Because trains were frequently not detected or incorrectly detected, the associated errors and alarms were designed to be categorized as "minor". The minor alarms would automatically be deleted by computer without human intervention. The two categories of errors happened about 8,000 times per week. →MMF1 **C3.** Because "ghost trains" were frequently generated by the bobbing circuit track, any time the track circuit is bobbing (changed its status from vacant, to occupied, to vacant again with no train traffic present), the AIM software was designed to delete the train image without generating an alarm within 30 seconds. The causes of the bobbing were not specifically mentioned in the report. The ghost trains were deleted by AIM system more than 1,000 times per week. →MMF1

C4. OCC operators cannot modify speed commands of the trains between stations, thus even if the train suddenly disappeared as in this accident, the system does not generate and send 0mph commands to the following trains. →C6

C5. Low quality safety culture → affected almost every unsafe actions and mental model flaws

C6. The ATC system design did not provide OCC operators with any functions to send 0mph speed commands to the train 112 (***ATC design problem***). → SR1

C7. There was no clear procedure to specify what actions the OCC operators must take when they recognize the alarms.

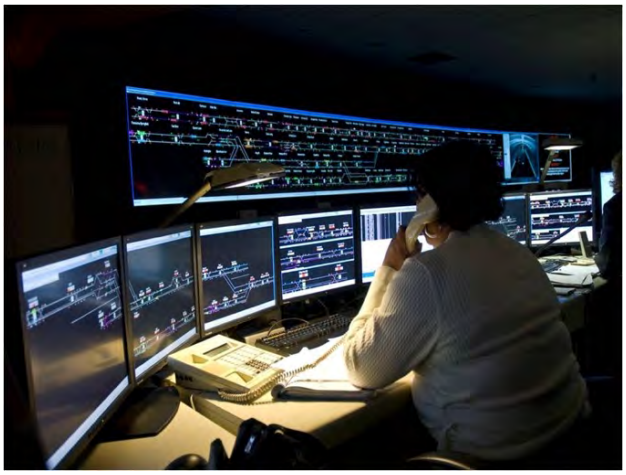


Figure 3- 12 OCC LCD Screen and an OCC Controller.

(Adapted from NTSB [13])

Actual LCC display size relative to OCC controllers can be seen in Figure 3-12 above. The images below from Figure 3-13 through Figure 3-19 are the OCC's screen display during the accident sequence. These are the enlargements of a small portion of a whole LCC display thus do not represent the actual view from the OCC controllers. All the information about OCC display sequence provided

here are from NTSB official report [13].

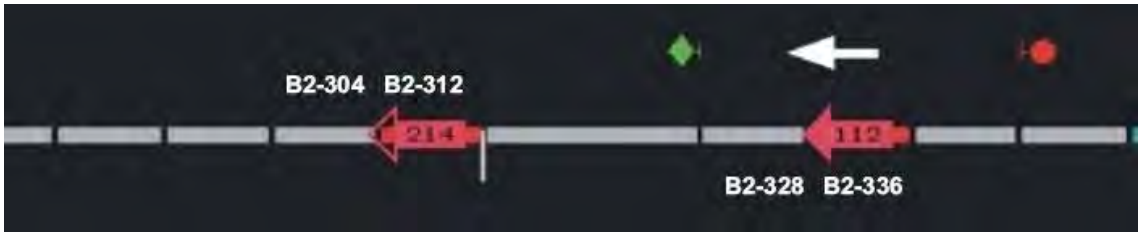


Figure 3- 13 OCC Display During the Accident Sequence (4:56:50 p.m.).

(Adapted from NTSB [13])

Train 214 (struck train) is detected occupying track circuit B2-312, which is next to malfunctioned B2-304. The train 112 is several blocks behind, and it is on the track circuit B2-336. Red track circuit symbols represent track occupancy. Performance data indicated that the front of train 214 was actually at the track circuit B2-312. The front of train 112 was at the track circuit B2-336.



Figure 3- 14 OCC Display During the Accident Sequence (4:57:02 p.m.).

(Adapted from NTSB [13])

Both trains have moved forward into the next block in their direction of travel. Track occupancy is being detected on track circuits B2-304 and B2-312 for train 214 and on track circuits B2-328 and B2-336 for train 112. Performance data indicated that the front of train 214 was at the track circuit B2-312. The front of train 112 was at the track circuit B2-328.

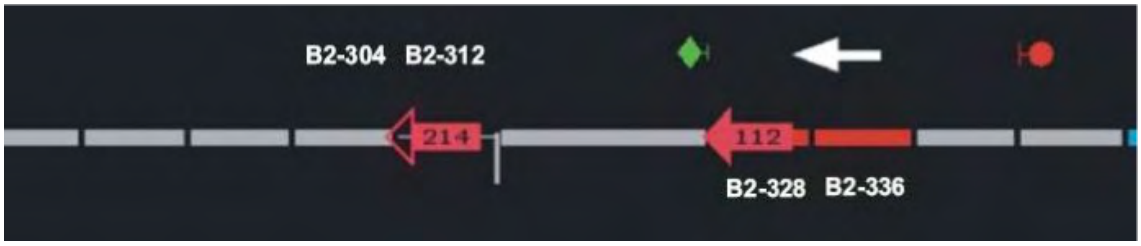


Figure 3- 15 OCC Display During the Accident Sequence (4:57:19 p.m.).

(Adapted from NTSB [13])

Train 214 is represented as occupying a single track circuit (B2-312) that is shown as a non-reporting block (a track circuit that reports as vacant when Advanced Information Management system (AIM) computer algorithms determine that it should be occupied). Track circuit B2-304 displays as an unoccupied, normally reporting block. Performance data indicated that train 214 was stopped at this time and that the front of train 214 was actually at the track circuit B2-304. The front of train 112 was at the track circuit B2-328. **Track circuit B2-304 displays as a normally reporting, unoccupied block even though performance data indicated that train 214 was fully within that track circuit. Performance data also indicated that at this time train 112 had begun receiving speed commands of 55 mph.**

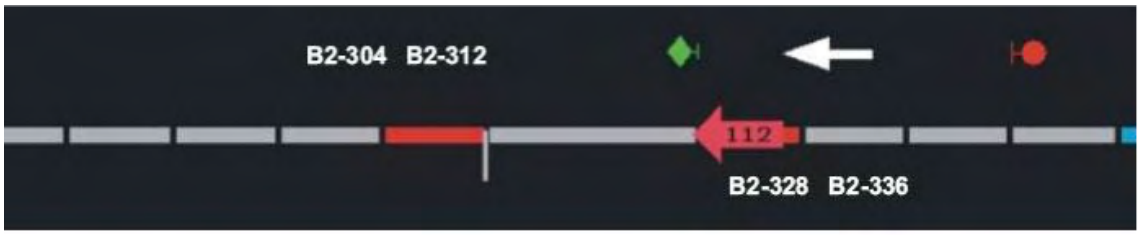


Figure 3- 16 OCC Display During the Accident Sequence (4:57:38 p.m.).

(Adapted from NTSB [13])

Track circuit B2-304 represents as it is unoccupied even though performance data indicated that the front of train 214 was at the track circuit B2-304. Track circuit B2-312 is now

displaying as an occupied, normally reporting block. **The tag for train 214 has been dropped from the display as a result of preprogrammed AIM algorithms designed to eliminate false train indications (It was not clearly mentioned in the NTSB report, but it was probably because train 214 was interpreted as the "ghost train")**[18]**.** The front of train 112 was at the track circuit B2-328.



Figure 3- 17 OCC Display During the Accident Sequence (4:57:39 p.m.).

(Adapted from NTSB [13])

Train 214 is disappeared from the LCD display. Train 112 is displayed as occupying a single track circuit (B2-312), which is now reporting as an unoccupied block. At this time, performance data indicated that the front of train 214 was at the track circuit B2-304. The front of train 112 was at the track circuit B2-328. Track circuit B2-328 is displayed as an occupied block. The intervening track circuit (B2-322) is displayed as an unoccupied, non-reporting block. Track circuit B2-304 is displayed as unoccupied even though all of train 214 is occupying that track circuit.

[18] "In the event that all track occupancy indications disappear under a virtual train and do not reappear within 30 seconds, the AIM software will delete the virtual train image without generating an alarm. This feature is designed to eliminate nuisance, or "ghost," trains (virtual trains created by the train tracking system that have no coincidence with actual trains) that are created as a result of bobbing track circuits. Additional algorithms not described in this report are used to eliminate ghost trains. According to OCC records, the AIM system creates and then deletes more than 1,000 ghost trains each week." [13]

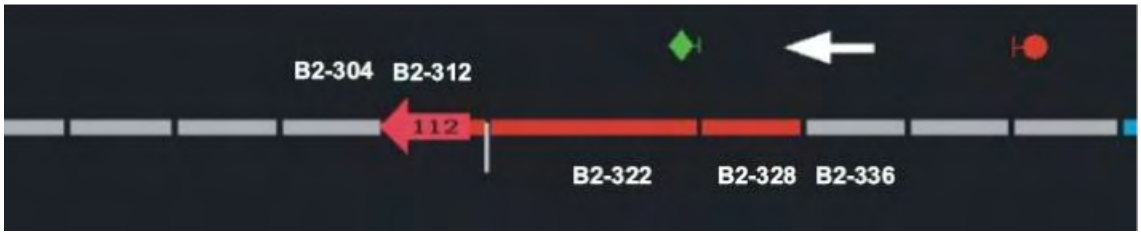


Figure 3- 18 OCC Display During the Accident Sequence (4:57:46 p.m.).

(Adapted from NTSB [13])

Train 112 is represented as it is occupying three track circuits, all of which are displayed as normally reporting blocks. Performance data indicated that the front of train 214 was actually at the track circuit B2-304. The front of train 112 was at the track circuit B2-322.

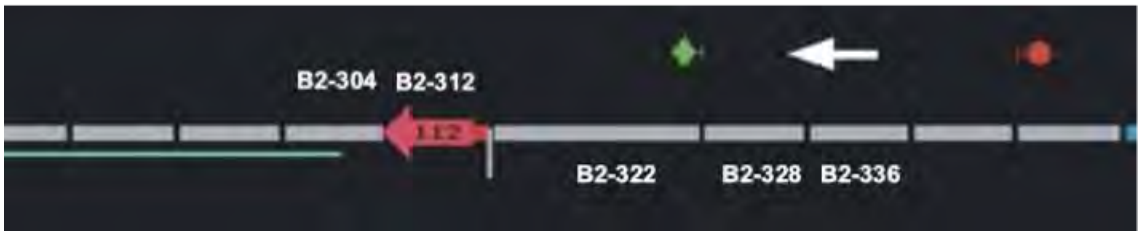


Figure 3- 19 OCC Display During the Accident Sequence (4:58:10 p.m.).

(Adapted from NTSB [13])

Train 112 is represented as occupying a single track circuit (B2-312). All track circuits are now displayed as normally reporting blocks. The green line indicates that third-rail power is down ahead of B2-312. Performance data indicated that the front of train 214 was actually at the track circuit B2-304. The front of train 112 was also at the track circuit B2-304.

3.8.1.2. Problems in the Safety Control Structure (Operator-Physical System Level)

There are several problems in the Safety Control Structure at this level:

- No effective direct controls from OCC computers or OCC operators over the train movement between the station in the case of system anomalies such as track-circuit malfunctions. That is, there is an ***ATC design problem***.
  - No direct controls from OCC computers or OCC operators into the ATP speed manipulation. The ATP speed is generated locally and cannot manipulated by these two higher-level components.
  - Considering the fact that OCC computer has the ability to detect the anomalies (e.g. loss of train detection), it should have direct control to manipulate the train movement through ATP speed commands.

- The safety-critical anomalies in the track circuit were categorized as “minor”. This is an ***ATC operation problem***.
  - Too many malfunctions of track circuits caused this decision.
  - The alarms were deleted without any human intervention within 30 or 60 seconds.
  - This led to the OCC operators’ habitually ignoring the alarms.

3.8.2 ATC Engineers-Physical System Level

3.8.2.1 Analysis of the ATC Engineers-Physical System Level

Next, the components in ATC Engineers-Physical System Level are examined. In the Safety Control Structure, these components are colored red in following Figure 3-20.

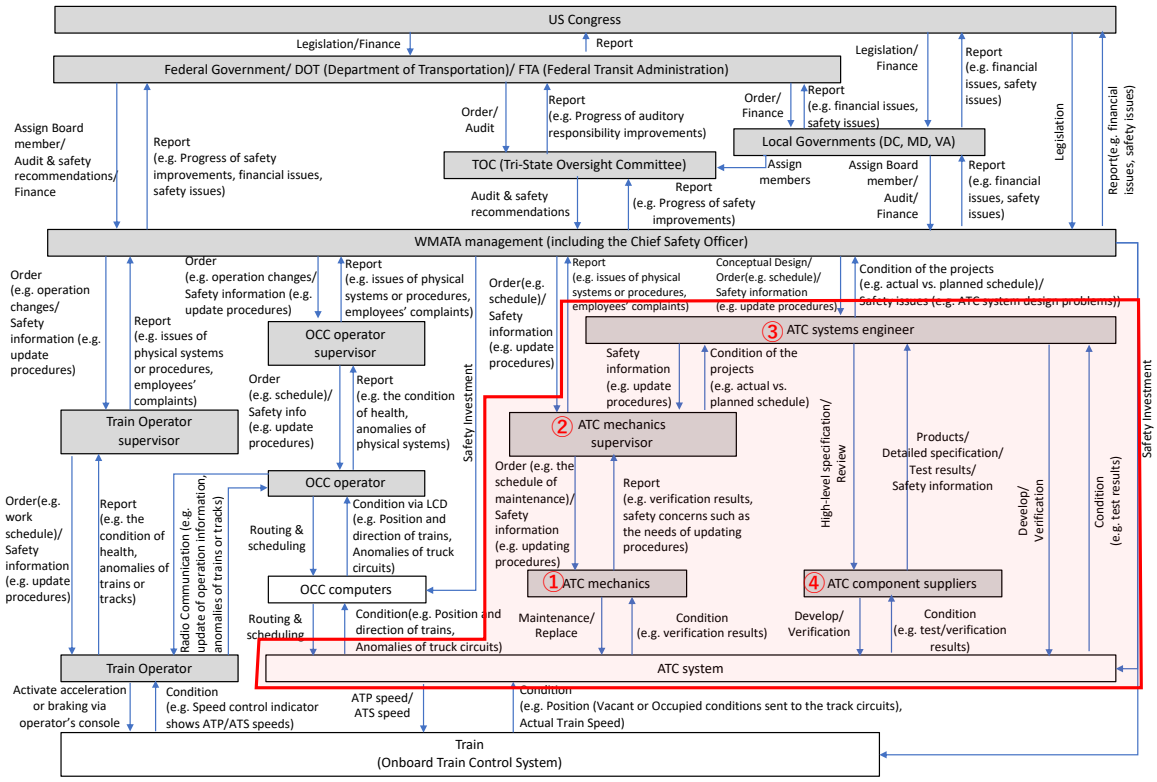


Figure 3- 20 Detailed View of ATC Engineers-Physical Interactions in the Safety Control Structure.

(1) ATC Mechanics

First, two ATC mechanics teams are analyzed and the results are shown in Table 3-11 and Table 3-12.

Five days before the accident, the installation team was carrying out the replacement of the old GRS's transmitter bond with the new US&S's one. During the verification procedure, they needed to increase the power level of the circuit module. In hindsight, this caused the parasitic oscillation's amplitude to be high enough to mimic the correct signal, thus the track circuit B2-304 no longer detected trains thereafter.

This team performed the verification test, but it had two problems. First, they carried out "originally-invented" shunt test (verification test). The leader thought the officially required one-point-shunt test, which is written in PMI 11000, was not preferable and carried out three-point-shunt

test. The main problem was that she did not obey the instruction and did not check with her supervisor whether it's ok to change the procedure. Secondly, they did not notice the renewal of the official procedure. The procedure for the shunt test was actually renewed in October 6th, 2006 as a form of engineering bulletin. This requires shunt test in three positions, that is, at each end and the middle of the circuit. Although the leader mentioned she performed three-point-shunt test, it was her "originally-invented" shunt test, and was not the correct three-point-shunt test procedure.

The next day of the installation, the other ATC mechanics team carried out the scheduled preventative maintenance activity on the B2-304. As with the installation team, they did not know the updated procedure. They carried out 1-point-shunt-test as required by PMI 11000.

In hindsight, if the latest procedure updated in 2006 was followed correctly by either of these two teams, the anomalies in the track circuit B2-304 might be detected and the accident could be prevented. But it is important to note that this lack of understanding of new procedures seems to have been prevalent across the company. The other track circuit, track circuit B1-245, also did not detect trains after the impedance bond was replaced and verified. That is, the ATC crew members[19] carried out the shunt test and verification but that track circuit also did not detect trains afterward. This happened in 2006, which means that these crew members were also not aware of and not following the new procedure enacted in 2006.

There are several reasons why they performed that way, including: 1) ***inefficient communication methods*** within the company; 2) lack of well-established ***safety culture*** within the company; 3) the Supervisor's instructions were not following the latest procedure; 4) the checklist form was not effective to mandate proper shunt test; 5) the manufacturer did not provide a maintenance plan which can detect parasitic oscillation; and 6) the maintenance activities were probably carried out under time pressure[20].

The detailed timeline for the enactment of the procedures, and detailed ATC mechanics' actions are provided in the Appendix A.

[19] Note that these members are probably not same ones who performed implementation or maintenance as has been discussed in this thesis.

[20] According to the news article, after 2007, WMATA started midnight operation until 3 a.m. This means that "a work crew sometimes gets as little as 90 minutes of actual repair time" [26].

Table 3- 11 Analysis of the ATC Mechanics (Installation Team)

Safety Requirements and Constraints
SR1. (Violated) Perform maintenance activities so that ATC systems perform safely. **SR2.** (Violated) Follow and understand the instructions provided by upper management and supervisors. **SR3.** (Violated) Monitor changes to procedures and understand the latest safety-related updates to procedures **SR4.** (Violated) Provide feedback to their supervisors and/or OCC about any safety-related concerns. **SR5.** (Violated) Obtain approval before executing modified actions that violate procedure.
Unsafe Decisions and Control Actions
UCA1. The mechanics of the ATC installation team performed 3-position-shunt-test described by the leader of the team without referring to any official procedure. She maintains she performed "3-position-shunt test," but it was probably not the proper one, as she did not refer to any official procedures. →SR1,2,3,4,5 **UCA2.** The leader of the ATC installation team did not obtain approval from her supervisor about changing the procedure. →SR1,2,3,4,5 **UCA3.** The leader of the ATC installation team increased transmitter power level, which resulted in creating spurious signal. →SR1
Mental Model Flaws
MMF1. Believed that PMI 11000 was the latest instruction for the verification procedure, and the one-position shunt test was the required procedure→UCA1,2 **MMF2.** The team leader believed that her "individually invented" three-position test was better than the official procedure for the test. →UCA1,2

MMF3. As the higher-level setting of the transmitter power level was well within the specification, she believed it would not cause the unsafe condition. She never thought this would cause an unsafe spurious signal. →UCA3
Context in which Decisions Made
C1. Mechanics were not aware of the 2006 bulletin and notices which require shunt test to be performed in 3 positions→MMF1 **C2.** The team leader[21] worked for WMATA when the bulletin and notices were circulated around the company in 2005 and 2006 but did not notice or remember them. This fact implies ***ineffective communication methods*** and possibly a poor ***safety culture*** within the company. →C1, MMF1, 2 **C3.** The team leader received instruction from her supervisor which only requires 1-point-shunt-test. The procedure was referring to PMI 11000. →C1, MMF1, 2 **C4.** The checklist form PM-1, used under PMI 11000, only indicated the column for transmitter and/or receiver end, not for the middle of the track[22]. →C1, MMF1, 2 **C5.** GRS/Alstom did not provide a maintenance plan that would detect anomalies such as parasitic oscillation. →MMF3 **C6.** The maintenance team may have been operating under time pressure. **C7.** Low quality safety culture → affected almost every unsafe actions and mental model flaws **C8**. The ATC mechanics supervisor instructed his subordinates that the train operation should be started even with the bobbing circuit.

Table 3- 12 Analysis of the ATC Mechanics (Preventative Maintenance Team)

Safety Requirements and Constraints
SR1. (Violated) Perform preventative maintenance activities so that ATC systems perform safely. **SR2.** (Violated) Follow and understand the instructions provided by upper management and supervisors.

[21] Note that it is not clear from the official report about other members in a team.
[22] This means that the PM-1 was implying either 1-position or 2-position test, not the correct 3-position test.

SR3. (Violated)

Monitor changes to procedures and understand the latest updates to safety-related information

SR4. (Violated)

Provide feedback to supervisors and/or OCC about any safety-related concerns.

Unsafe Decisions and Control Actions

UCA1. The ATC mechanics of the preventative maintenance team used PMI 11000 and conducted shunt test on only 1 position, thus did not properly verify that the circuit functions correctly→SR1,2,3

UCA2. The ATC mechanics of the preventative maintenance team did not report the bobbing problem to the OCC→SR4

Mental Model Flaws

MMF1. Believed that PMI 11000 was the latest instruction for the verification procedure, and the one-position shunt test was the required procedure→UCA1

MMF2. They did notice the bobbing problem, but believed other teams would resolve it (***Coordination Problem***). →UCA2

Context in which Decisions Made

C1. Maintenance workers were not aware of the bulletin and notices which require shunt test to be performed in 3 positions→MMF1

C2. Maintenance workers were not aware of the open work order regarding the bobbing track circuits→UCA1

C3. Maintenance workers worked for WMATA when bulletin and notices were circulated around the company in 2005 and 2006 but did not notice or remember the contents of them. This common factor implies inefficient communication methods and poorly established safety culture within the company. →MMF1

C4. The checklist form PM-1, used under PMI 11000, did only indicate the column for transmitter and/or receiver end, not for the middle of the track. →MMF1

C5. GRS/Alstom did not provide a maintenance plan that would detect anomalies such as parasitic oscillation. →UCA1

C6. The maintenance team may have been operating under time pressure. **C7.** Low quality safety culture → affected almost every unsafe actions and mental model flaws **C8**. The ATC mechanics supervisor instructed his subordinates that the train operation should be started even with the bobbing circuit.

(2) ATC Mechanics Supervisor

The ATC Mechanics Supervisor is examined and summarized in Table 3-13. He was unaware of the newest procedures explained in the bulletin in 2006. He thought that there was no specific procedure for the maintenance and invented his own procedure without checking with upper-level controllers. Some of them lied to the upper management that the frontline workers incorporated the loss-of-shunt-tool into their regular maintenance activities. They did not get feedback from ATC engineers about safety concerns. They even ordered their subordinates to prioritize the operation over fixing the bobbing track circuits. These are indicative of their low-sensitivity to the safety degradation and implies the low safety culture within the company.

Table 3- 13 Analysis of the ATC Mechanics Supervisor

Safety Requirements and Constraints
SR1. (Violated) Ensure that the team members understand and perform procedures correctly. This includes making sure that they understand and act upon the latest safety-related notices **SR2.** (Violated) Ensure that their teams perform necessary maintenance activities so that ATC systems perform safely. **SR3.** (Violated) Collect feedback from maintenance teams about any safety-related concerns.

SR4. (Violated)
Provide feedback to upper management or ATC system engineers about any safety-related concerns.

Unsafe Decisions and Control Actions

UCA1. The ATC mechanics supervisor developed an inadequate improvised procedure that requires the shunt test be performed on only 1 position, and instructed his subordinates to use that improvised procedure. →SR1,2,4

UCA2. The ATC mechanics supervisor did not instruct his subordinates to perform the verification test correctly using the latest procedure to ensure the truck circuits functions properly →SR1,2

UCA3. Some of the previous ATC mechanics supervisors incorrectly informed WMATA management that the loss-of-shunt-tool was used monthly or weekly, although the data shows contrary. →SR4

UCA4. The leader of the installation team may have thought the 1-position-shunt-test was not enough for verification. In that case, the ATC mechanics supervisor may not have sought feedback from her about the concern of the procedure. That is, he may not have created a comfortable atmosphere where mechanics could report concerns without fear. →SR3

UCA5. The ATC mechanics supervisor instructed his subordinates that the train operation should be started even with the bobbing circuit. →SR2

Mental Model (Flaw)s

MMF1. The supervisor was aware of the existence of the updated procedure in 2005 and 2006 requiring 3 position tests, but believed they were not applicable to the regular impedance bonds like the one in this case. He mistakenly believed that it referred only to high-current bonds. →UCA1,2

MMF2. He believed that there are no official instructions for the procedure, and that the

improvised procedure contained sufficient information to perform the proper shunt test. →UCA1,2, SR4 **MMF3.** He believed that continuing operation of the train service is more important than fixing the bobbing circuit. He said, “the mentality now is move trains.” →UCA5 **MMF4.** He believed that because the system has not experienced serious safety problems even with bobbing track circuits and other anomalies, it would be acceptable to tolerate track malfunctions (the NTSB report explains this mentality as "The apparent tendency among many managers to tolerate various failures and malfunctions in the ATC system was also likely influenced by their perceptions of past system performance." [13]). →UCA5
Context in which Decisions Made
C1. The supervisor worked for WMATA when bulletin and notices were circulated around the company but did not understand or remember the contents of them correctly. This fact implies the ineffective communication methods and possibly a poor safety culture within the company. →MMF1,2 **C2.** GRS/Alstom did not provide a maintenance plan that would detect anomalies such as parasitic oscillation. →SR2 **C3.** Low quality safety culture → affected almost every unsafe actions and mental model flaws

(3) ATC Systems Engineer

The ATC Systems Engineer is analyzed below in Table 3-14. The ATC Systems Engineer was in charge of specification development for the track circuit replacement project. He did allow the GRS equipment to be installed with non-GRS equipment when the manufacturer (Alstom) did not recommend it. One could argue that it can be excused because the parasitic oscillation could happen even when all GRS-manufactured equipment are installed, but their attitude of not following the

manufacturer recommendations seems to be a symptomatic indication of low sensitivity to safety-related concerns on safety-critical systems like the ATC system.

He did not make sure that the notice in 2006 that required the 3-point-shunt-test was circulated around the company. Frontline workers and their supervisors were not aware of and did not follow that procedure. One factor is a poor-quality safety culture in which front-line workers were less sensitive to the notices. Also, those workers might have been under the time pressure because of the limited maintenance time.

Table 3- 14 Analysis of the ATC Systems Engineer

Safety Requirements and Constraints
SR1. (Violated) Develop and review the specifications of the track circuit replacement project, making sure that replacement or installation of ATC components do not adversely impact safety of train operations. **SR2.** (Violated) Provide safety-related information like procedures and make sure that ATC mechanics are performing ATC-component-related actions safely. **SR3.** (Violated) Collect feedback from ATC mechanics teams about any safety-related concerns. **SR4.** (Violated) Provide feedback to upper management about any safety-related concerns. **SR5.** (Violated) Collect safety-related information from suppliers
Unsafe Decisions and Control Actions
UCA1. The ATC systems engineer provided a design with components that could experience parasitic oscillation. →SR1,2

UCA2. The ATC systems engineer did not make sure ATC mechanics were aware of and following the engineering bulletin which requires the three-place-shunts-test. →SR1,2

UCA3. The ATC systems engineer did not provide a procedure or test that would prevent or detect parasitic oscillation. →SR1,2

Mental Model Flaws

MMF1. He had noticed that the use of US&S bonds with GRS modules would require changing transmitter power, but he believed that GRS modules would not generate any anomalies when increasing the power level. →UCA1,3

MMF2. He believed ATC mechanics were aware of and would follow a bulletin published in 2006. He believed that ATC mechanics did notice, understand, and performed under the engineering bulletin in 2006, which requires 3-place-shunt-test when using components from different manufactures. →UCA1, 2

MMF3. He understood the recommendation from Alstom about concerns regarding using GRS and non-GRS components together, but he believed if he could demonstrate the same system performance then there is no problem to use GRS and non-GRS components. →UCA1,3

Context in which Decisions Made

C1. Alstom, the manufacture of the GRS components, had never provided the knowledge that GRS modules could generate parasitic oscillation. Nor did they provide maintenance advice about how to check the presence of anomalies such as parasitic oscillation. →MMF1, SR5

C2. During bench-testing using a GRS module and US&S bond, the ATC systems engineer found no significant deviation from what would be expected from a circuit using all GRS components. →MMF3

C3. Although not specifically mentioned from whom, he was told that the track circuits were being verified using the new procedure with three shunts. →MMF2

C4. According to Alstom, WMATA received the letter from Alstom not to use non-GRS components with GRS components together in 2004, But this was not well recognized by the person in charge of receiving that letter and it was not distributed to related engineers.

C5. There may not have been a policy to obey supplier recommendations for components that are safety-critical. →MMF3

C6. Low quality safety culture → affected almost every unsafe actions and mental model flaws

C7. Although the ATC systems engineer was advised by Alstom manager not to use GRS and non-GRS components, he did not follow this advice and specified track circuits operated with US&S bonds and GRS modules. →C6

C8. The ATC systems engineer may not have checked with or requested approval from upper management about whether he could allow the use of non-GRS components and GRS components together, although he was recommended by a supplier not to do so. →C6

(4) Alstom (ATC component supplier)

Alstom is analyzed in Table 3-15. The official report concludes that a contributing factor is Alstom not providing a maintenance plan for detecting parasitic oscillation. This is true. However, they carried out the verification and made the specifications based on what was known. Due to lack of adequate information, this thesis could not examine Alstom's own safety control structure in more detail.

Table 3- 15 Analysis of the Alstom

Safety Requirements and Constraints
SR1. (Violated) Provide detailed component specifications and perform component verification -Ensure their components can perform safely when equipped in the WMATA' system **SR2.** (Violated) Provide necessary safety-related information to WMATA
Unsafe Decisions and Control Actions
UCA1. Alstom did not provide any information to WMATA about how parasitic oscillation would affect ATC's fail-safe design →SR1, 2 **UCA2.** Alstom did not provide a maintenance procedure to WMATA for detecting parasitic oscillation →SR1
Mental Model Flaws
MMF1. Believed that if WMATA use all-GRS equipment together, without using other manufactures' components together with GRS's, then track circuit would perform safely. → UCA1,2 **MMF2.** Believed that their notice (e-mail) to WMATA in Sep 7, 2004, which recommended

not using other manufactures' equipment together with theirs, was well understood and circulated to the related employees in WMATA. →UCA3 **MMF3.** May have believed that the parasitic oscillation in the track circuit module would do no harm to the ATC system's fail-safe design→MMF1
Context in which Decisions Made
C1. Prior to the accident, Alstom was aware of previous cases with continuous parasitic oscillation, but they had never been known to affect train detection[23] → MMF3

[23] According to the accident report: "Parasitic oscillation is a known potential problem with any amplifier circuit, which could result in the generation of unwanted additional signals, along with the intended amplified output signal. According to the manufacturer, prior to the accident it was aware of previous cases with continuous parasitic oscillation, but they had never been known to affect train detection and were considered harmless." [13]

3.8.2.2. Summary of problems in the Safety Control Structure (ATC Engineer-Physical Interactions)

There are several problems in the Safety Control Structure at this level. This section discusses and summarizes the findings so far regarding the ATC-Engineer-Physical Interactions in Table 3-11 ~ 3-15.

Safety did not seem to be their first priority. The priority seems to be maintaining operation. The Bobbing problem, which was one of the common track circuit malfunctions, was happening everywhere and often those remained unfixed. Workers believed the operation should be continued even with the bobbing problem on the track circuit. The ATC mechanics supervisor said, "the mentality now is move trains" (***Emphasis on maintaining operations over safety***). The preventative maintenance team did not report the bobbing problem to the MOC because the weather was deteriorating. They also thought others would fix the problem (***coordination problem***).

The safety culture does not seem to have been very strong. The track circuits' malfunction was prevalent and happened 8,000 times per week. The operational decision was not to fix them, but to make those alarms "less annoying" (OCC operation decision problems). The malfunction problems were not only for the track circuit, but also for other equipment[24]. This caused frontline workers to realize that malfunctions are prevalent everywhere without impacting safety (yet), and therefore it was not seen as urgent to fix them. The frontline workers seemed not to routinely report on-site problems to the upper controllers, and they even changed the safety-related procedures without getting approval.

The facilities were aging facilities due to inadequate budget allocations. The metro system

[24] There are more than 100,000 insulators along Metro's tracks, and one of them fails, on average, twice a month …."We are not back in 1976 [when Metro opened]. We're a 40-year-old system," Wiedefeld says. "Track is just one of the issues we have to deal with. We have system issues. We have power issues. We have lighting issues. Those are just ongoing issues that we will have to deal with" [26].

was 40-years old and accidents happened everywhere. The upper management' decision for budget allocation towards safety improvement or maintenance seems to be inadequate. It seems the speed of maintenance and replacements were not keeping up with the normal degradation of the system. The capacity improvement projects, even in the overwhelming situation where malfunctions were everywhere, were indicative of upper management's inadequate mental model.

Each problem seems to be interconnected with similar aspects. This indicates that the accident was probably not a fluke or an isolated case, but a symptomatic case due to systematic deficiencies within the system's safety structure and company structure. Some of these factors are examined in the next section.

3.8.3 Upper Management, and Governmental and Audit Agencies Level

3.8.3.1 Analysis of Upper Management, and Governmental and Audit Agencies Level

Finally, the highest level in the safety control structure are examined as highlighted in Figure 3-21.

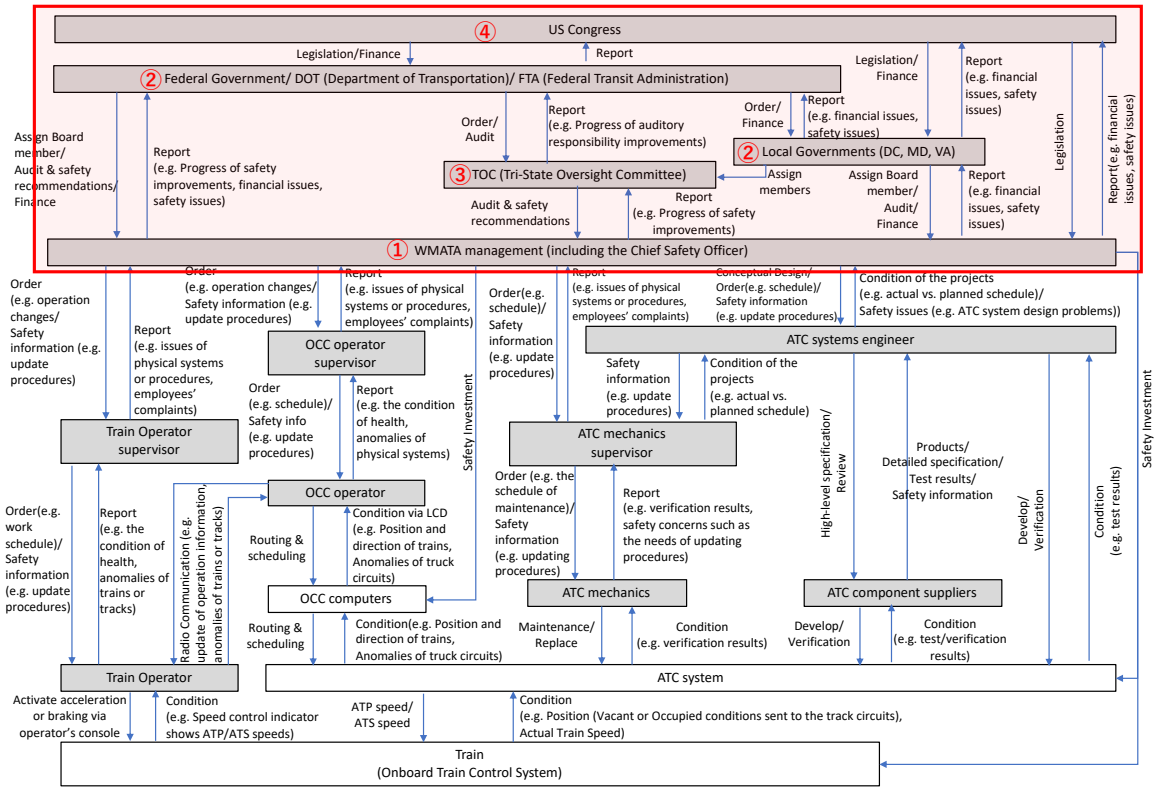


Figure 3- 21 Zoom-Up to Highest Level of Safety Control Structure.

(1) WMATA Management

WMATA Management is examined and summarized in Table 3-16. They were managed by governmental authorities at the federal level and three local municipalities. Each of them was prone to politics and some may have emphasized profit over safety. One could argue this is supported by the fact that they lengthened operation hours so that they could accommodate more passengers, rather than making sure the malfunctioned track circuits were repaired and safe operation was assured. Tri-State Oversight Committee (TOC)[25], the state audit agency, was composed of members from each

[25] According to the accident report: "The state safety oversight agency for WMATA Metrorail is the Tri-State Oversight Committee (TOC), which was established in 1997 by a memorandum of understanding (MOU) between the Virginia Department of Rail and Public Transportation and the departments of transportation of Maryland and the District of Columbia. The MOU specifies that TOC comprise six representatives, two from each of the aforementioned agencies. The secretary of transportation for the state of Virginia, the secretary of

municipality and was almost a “relative” to WMATA. TOC and FTA did not have statutory power and WMATA has not been following their recommendations. These background problems led WMATA to have an ineffective safety culture, and important safety-related information (like new procedures) were not well distributed within the company.

Table 3- 16 Analysis of the WMATA Management

Safety Requirements and Constraints
SR1. (Violated) Ensure that the budgets and investments for maintaining and improving safety of the system are sufficient and appropriately distributed **SR2.** (Violated) Follow safety-related regulations and recommendations from governmental agencies and TOC. **SR3.** (Violated) Define and follow an effective company-wide safety policy - Provide safety procedures, operation plans, and training (e.g. clarify procedures) - Update operation changes and safety procedures - Create and provide conceptual designs **SR4.** (Violated) Collect feedback from employees about any safety-related problems, and provide feedback to upper-level controllers about safety-related issues. **SR5.** (Violated)

transportation for the state of Maryland, and the director of transportation for the District of Columbia select their respective members. The MOU does not address either the appropriate qualifications for members of TOC or the length of their terms of service. The MOU specifies that TOC members must select a chair and a vice chair who serve in those capacities for 1 year. At the end of the 1-year term, the vice chair becomes the chair, and a new vice chair is selected by the TOC members. The MOU also permits each agency to designate an alternate representative.” [13]

Ensure that the safety-related information is circulated, understood, and acted upon effectively and properly.
Unsafe Decisions and Control Actions
UCA1. WMATA management did not respond and follow safety-related recommendations made by audit agencies[26] → SR1,2,3,4,5 **UCA2.** WMATA management did not institutionalize and employ system-wide the enhanced track circuit verification testing developed following the 2005 Rosslyn near-collisions. → SR1,2,3,4,5 **UCA3.** WMATA management did not provide a clear procedure that specifies what actions are needed from the OCC operators when alarms occur.→ SR5 **UCA4.** WMATA management did not provide effective safety oversight, including providing effective procedures and training to clarify the new procedures and other safety-related issues on-site. → SR3,4,5 **UCA5.** WMATA management did not establish an effective safety culture in which lower-level employees could report safety-related issues without fear, such as too many malfunctions of track circuits and ineffective alarms of OCC computer, and have confidence they would be addressed → SR3,4,5 **UCA6**. WMATA management did not establish an effective communication channel for safety-related issues. → SR3,4,5

[26] As of early 2010, TOC had identified 48 CAPs that were still classified as open from previous TOC safety audits of WMATA, some of them dating from 2004 [13].

UCA7. WMATA management lengthened the system's operation time until 3 a.m. and added 40 miles of track (15 percent of the track) compared to 1998. These changes resulted in less down time available to perform maintenance activities, while the amount of maintenance work needed would increase. → SR3

UCA8. WMATA management did not establish an effective safety policy to prevent unsafe compromises between profit and safety. → SR3

UCA9. WMATA management did not allocate sufficient budget to maintenance or improving safety[27]. → SR1,2,3

Mental Model (Flaw)s

MMF1. May have believed that allocating budget to expanding the operation capacity is more important than spending budget on maintenance or safety improvements. →UCA1,2,7,8,9

MMF2. May have believed that Metrorail's system safety is not so degraded to the level that more investment in safety improvement is needed →UCA1,3,4,5,6,7,8,9

MMF3. May have believed the recommendations given by audit agencies are not so important to consider thus could be ignored →UCA1

Context in which Decisions Made

C1. WMATA management was prone to politics related to governmental decisions.

- Local governments are very important stakeholders. As the local government wanted to meet the needs from local owners to lengthen the operation time so that workers and customers could stay in their facilities (e.g. restaurant, night clubs) longer, WMATA was pushed to meet those demands.
- WMATA's board members are from local governments and federal government. This means their decisions are heavily affected by the needs of local government (as opposed to internal

[27] After this accident, the congress pledged to spend $1.5 billion over a decade on capital improvements, for maintaining or replacing its aged facilities. Even with these funds, Metro continuously suffered from several incidents or accidents. This implies that their budget allocation to safety had been not enough and/or it was too late to cover the degradation of the safety with this amount of money [25].

needs like safety improvements).

- Local governments would get more tax revenue and a good reputation if they could maintain longer operation hours.
- In addition to local government influence, WMATA's budget is also dependent on the federal government and on congress [27].

→MMF1

C2. The recommendations by audit agencies did not have statutory power →UCA1, MMF3

C3. The limited budget available and the nature of the oversight above made it easier for WMATA management to compromise safety investments when other non-safety investments were prioritized [27] →MMF1,2,3

(2) Governmental Agencies

Federal and Local governmental agencies are examined in Table 3-17 and Table 3-18. The main issues related to these authorities are that: 1) they did not make sure that audit agencies recommendations are followed by WMATA; and 2) they did not allocate enough budget to WMATA for maintaining safety.

Table 3- 17 Analysis of the Federal Government/FTA

Safety Requirements and Constraints
Federal Government
SR1. (Violated) Decide upon, and allocate sufficient budget to WMATA to enable safe operation.
SR2. (Violated) Provide oversight, making sure FTA is carrying out its oversight responsibility

FTA

SR3. (Violated)

Provide oversight of TOC and WMATA

- Ensure TOC and WMATA are following and responding to safety-related recommendations (e.g. with auditing)

Unsafe Control Actions

UCA1. (FTA)

FTA did not provide effective safety oversight, and did not make sure that the WMATA is following recommendations →SR3

UCA2. (federal government)

The federal government did not equip the FTA and TOC with statutory power over WMATA's operation, which would have made following recommendations mandatory. →SR2

UCA3. The federal government and FTA did not invest enough to ensure the safe operation of WMATA system. →SR1

Mental Models

MMF1. Federal government and FTA possibly believed investing in safety improvement of WMATA is not as pressing compared to other issues

Context in which Decisions Made

C1. Federal government and FTA were prone to politics, and having lots of stakeholders (e.g. Lobby group)

C2. FTA was not given the authority to directly enforce any regulations.

C3. The extent of the FTA's efforts to this point had been to "encourage" recipients to adhere to industry best practices and recommendations made by the NTSB.

Table 3- 18 Analysis of the Local Governments

Safety Requirements and Constraints
SR1. (Violated) Decide upon and allocate sufficient budget to WMATA to enable safe operation. **SR2.** (Violated) Allocate Board Members to WMATA, ensuring that the selected board members can manage the company well enough to maintain safe operation of the system. **SR3.** (Violated) Allocate members of TOC, making sure they can perform oversight actions to ensure safe operation.
Unsafe Control Actions
UCA1. The local governments did not allocate enough budget to WMATA→SR1 **UCA2.** The local governments did not provide effective financial oversight and did not check and make sure WMATA's finance and budget is sufficient to maintain and improve the safety of Metrorail operation →SR2,3 **UCA3.** The local governments did not provide effective safety oversight, and did not make sure the members of WMATA board and TOC are working effectively toward maintaining and improving WMATA's system →SR2,3
Mental Model (Flaw)s
MMF1. Local governments may have believed that making profit via expanding capacity is more pressing than investing on safety improvement of the WMATA operation →UCA1 **MMF2.** Local governments may have knowing that there are some malfunctions in WMATA Metrorail system but not so severe to require investing more →UCA1
Context in which Decisions Made
C1. Prone to politics, and having lots of stakeholders (e.g. Lobby group) →MMF1,2, UCA1,2,3

(3) TOC

Next, TOC was examined and summarized in Table 3-19. Their organization structure was problematic because the members of TOC were elected from local governments, who had significant managerial power over WMATA. This means that WMATA was audited by their "relatives", making it difficult to appropriately enact the audit power. This issue can be seen in other transit authorities too. For example, in Taiwan, a bullet train crashed because a train engineer ran a vehicle over a speed limit [28]. There had been more than seven derailments within the last two years before the accident, but no measure was provided to prevent the hazards. The incidents had been investigated by an outside audit agency but the members were composed mainly of the executives from the train operation company [9].

Table 3- 19 Analysis of the TOC

Safety Requirements and Constraints
SR1. (Violated) Provide safety oversight over WMATA, making sure WMATA is following the recommendations and safety-related regulations - Annually review and approve WMATA's system safety program plan, including any changes to the plan. - Require WMATA to conduct safety reviews and to submit the findings to TOC for review - Conduct on-site safety reviews every 3 years to determine whether WMATA's safety practices and procedures are in compliance with the system safety program plan. Any areas that are identified as those in need of corrective action are incorporated into a corrective action plan (CAP)
Unsafe Control Actions
UCA1. TOC did not provide effective safety oversight, and did not make sure that WMATA is following and responding to their recommendations. →SR1 - A large number of recommendations remained open and unresolved[28]

[28] As of February 3, 2010, a total of 48 CAPs from previous triennial audits were still classified as open, that

UCA2. TOC did not properly carry out their own investigations and sometimes delegated its tasks to WMATA itself. →SR1
Mental Model Flaws
(Inadequate information available)
Context in which Decisions Made
C1. TOC was prone to a conflict of interest because TOC members are assigned from each regional government (Organization Design Problem). →UCA1,2 **C2.** The FTA does not, and cannot, provide the oversight agency with the authority to promulgate and enforce safety regulations or standards. →UCA1,2 - TOC cannot establish or enforce standards of performance for WMATA with respect to safety-critical areas of performance such as operations, equipment, track, signal, hours of service, and equipment crashworthiness. - TOC lacks the authority to compel WMATA to comply with its own rules, standards, and procedures, or to take significant action should WMATA not to comply with an element of its system safety program plan. **C3.** Staffing limitation made it difficult for TOC to carry out thorough investigation. →UCA1,2 **C4.** Lack of expertise made it difficult for TOC to carry out thorough investigation. →UCA1,2

(4) Congress

Finally, the US Congress was analyzed and the result is shown in Table 3-20. The congress is in charge of maintaining or renewing laws so that the transit agencies can operate its transportation

is, unresolved. This included 9 CAPs from events in 2004, 6 from 2005, 6 from 2006, 11 from 2007, and 13 from 2008 [13].

systems effectively and safely. Therefore, they have control over how much money would be allocated to the safety improvement or maintenance of the WMATA. These would be allocated in the forms of grants or other forms of governmental support funds. In order to adequately allocate budgets to transit agencies, they would need to update their mental models about the actual financial situation or the system safety of transit agencies such as WMATA.

Their mental model may have recognized that there exist some safety problems in WMATA, but they may have felt that WMATA should improve safety by their own efforts and using what they have now. Congress may have believed that congress does not need to spend more money for WMATA and that there are other more important issues. In addition, the public rail operation may not have been deemed very important for the US economy, so more money could be allocated to other areas.

They may not have updated their mental model so reflect the need for congress to make sure WMATA can improve their system safety. Congress could, but did not, pass bills to pay more grants to WMATA or give audit agencies the necessary statutory power.

Table 3- 20 Analysis of the Congress

Safety Requirements and Constraints
SR1. (Violated) Allocate budgets to governmental agencies, making sure the budget allocation to governmental agencies are adequate to ensure the safe operation of transportation systems. **SR2.** (Violated) Ensure the current law structure is sufficient for safety of the transit operation. **SR3.** (Violated) Collect feedback from governmental and audit agencies and monitor whether operators are following safety recommendations and safety-related regulations.
Unsafe Control Actions
UCA1. Congress did not pass a bill (legislation) to provide regulatory safety oversight with audit

authorities →SR2 **UCA2.** Congress did not pass bills to increase the safety budget for WMATA → SR1
Mental Model (Flaw)s
MMF1. Congress may have known that there are some malfunctions in WMATA operation but may have believed it is not so severe to require investing more - May have believed that there were other more important and urgent issues which need budget allocation →UCA2
Context in which Decisions Made
C1. Prone to politics, and having lots of stakeholders (e.g. Lobby group)

3.9 Examining how Coordination and communication contributed to the Loss

This section examines whether some coordination or communication problems contributed to the hazardous states. This thesis concludes that the WMATA safety control structure clearly did not have effective communication channels as follows:

・effective feedback channel and reporting culture
・effective safety-related information circulation

These contributed because they accelerated the degradation of the safety culture, the overall degradation of safety, and degradation of infrastructure. More detailed explanations are provided in the next sections.

3.10 Dynamics and Migration to a High-Risk State

In this section, the dynamics and migration of the system's state into an unsafe condition over time is discussed.

3.10.1 Degradation of safety culture

Considering their aggressive expansion compared to the insufficient maintenance activities, WMATA management's priority of Safety seems to have been less than its priority of expanding its capacity. Over time, this seems to have eroded the Safety Culture. The characteristic of effective safety culture is well documented in the official report:

> (1) an *informed culture* in which those who operate and manage the system have knowledge about the human, technical, organizational, and environmental factors affecting the safety of the system; (2) a *reporting culture* in which people are able and encouraged to report safety concerns, errors, and near-misses; and (3) a *just culture* in which people are encouraged and rewarded for providing safety-related information without fear of blame [13, p. 102].

The WMATA's internal environment clearly did not have and effective communication channel. This led to the situation where on-site ATC engineers and their supervisors were not aware of the latest procedure for verification of ATC components. Low-level employees also seem to have been reluctant to report their concerns to upper-level controllers, such as the individually-improvised verification method and procedures. As a result, the quality of maintenance degraded over time. These aspects support the idea that WMATA lacked an effective Safety Culture. WMATA management's perceived importance of Safety (mental model) cannot be updated when the lower-level controllers hesitate to report the on-site problems. It would have taken time for their mental model to have degraded because of the underling delays in the system structure, but no effective measures seem to have been provided

to change that structure.

3.10.2 Degradation of Infrastructure

As WMATA's infrastructure was 40 years old, malfunctions were everywhere. On top of the scheduled preventative maintenance, the on-site workers had to deal with these malfunctioning components. While the operation time was lengthened because management teams believed it would generate more profit, the time allocated for maintenance activities were shortened so that the speed of degradation far outreached that needed to catch up. Even worse, the volume of scheduled maintenance was increased as the total track circuit was lengthened and the vehicles per operational train increased so that WMATA could accommodate more passengers.

3.10.3 Degradation of Safety

Over time, the infrastructure has aged and there are more malfunctions than in the past. The aged infrastructure needs to be maintained properly and replaced before it's too late. The on-site worker's mental model about the importance of track circuit malfunctions, for example, has deteriorated over time as malfunctions have come to be an almost normal occurrence. This led to the degraded quality of maintenance and degraded safety culture. As management did not take sufficient actions against the aged infrastructure and degraded safety culture, the situation got worse over time. Even in this unsafe situation, the on-site workers might have been thinking that malfunctioned track circuit have not led to many more accidents, and therefore they could leave them as they are.

3.10.4 Combining the Loops together: Multiplier Effects

The abovementioned three reinforcing structures were mutually connected and had a multiplier effect. Because of the management priority of expansion over safety, the situation quickly

got worse. Even when the system is brand new and there are not many troublesome events, the management should make sure that they have high-quality safety culture, safety-oriented budgetary policy, and the infrastructure is well maintained and replaced with appropriate timing. If they did not do so, on-site workers' perceived level of safety would degrade over time and it would be not an easy task to change their mindset.

3.10.5 Policy Resistance: Investment on expansion over on safety

The management's reductionist view was that expansion would make a profit and would make the stakeholders happy. However, their decisions actually made the speed of degradation of the infrastructure much higher. Because of the longer trains (more vehicles per one operational train), the damage to the infrastructure accelerated. Because of the longer operational hours, the actual time available for maintenance became shorter. With the longer tracks, the workload of maintenance got worse. As a result, they had to stop operations several times because of the malfunctioned infrastructure, and the operational revenue suffered further[29]. This seems to be one example of *Policy Resistance*, where the policies implemented to address problems not only do not solve them, but also make them worse or even cause them [30, p. 23].

3.10.6 Chronic problems are nearly irreversible in the short span

After this accident, the WMATA management seems to have gradually been changing their attitude toward Safety and started investment in maintenance and replacement activities. However, they have still been experiencing several equipment problems. In 2013, an arcing insulator caused two trains to stop inside a tunnel, stranding 250 passengers for an hour, including a woman who had

[29] "Poor service, including outages and delays, has cost WMATA hundreds of thousands of riders, exacerbating its economic problems. During fiscal year 2016, which ended in June, total rail and bus ridership fell to 321 million trips. Budget documents described this as "a decrease of 20 million or six percent compared to the prior year." The numbers are even more sobering given that they do not include the start of the SafeTrack maintenance program" [29].

a seizure problem. In January 2015, a smoke-filled train was stopped in a tunnel, and one woman died and 91 other people were injured. In March 2016, a similar fire made WMATA stop the whole subway operation for a day to conduct inspections and repairs [26].

In order to carry out an comprehensive infrastructure improvement, WMATA started a year-long track replacement plan called SafeTrack in 2016 [31]. After SafeTrack, the ridership of the Metrorail has dropped 125,000 average daily trips over the past decade, and management says they have no clear vision how to fix it [32].

The problem in WMATA is very systematic. It seems that the management decision of more investment in safety improvement was a good choice. As Sterman argues, "High leverage policies often cause worse-before-better behavior," the better situation will come later. However, as the actions are irreversible in complex systems, "doing and undoing have fundamentally different time constants" [30, p. 25]. Thus, turning the current situation back into a healthy state may take much longer time than it took for the system to migrate into the current unhealthy state.

3.11 Reviewing and Revealing the Weakness of Safety Control Structure

In this section, the analysis results are summarized in the safety control structure, which explain each controllers' safety constraints, UCAs, Mental Model Flaws, and Context.

Figure 3-22, 3-23, and 3-24 show Safety Constraints Violated in the different level of safety control structure respectively. Figure 3-25 shows the simplified and consolidated version of Figure 3-22 ~ 3-24. The dotted red line indicates what was ineffective and contributed to the accident, whether control actions, feedback, or controllers. As is revealed so far, every controller contributed accident, and there are many ineffective control actions and feedback.

From these figures, one can see how many UCAs and violated safety constraints are found in the different level. This means that there is no "root cause," but there are many causes and factors. These causes should be prevented by enforcing more appropriate safety constraints at each level. As these revealed causes should be documented and passed on to future system designs, these are translated into the form of recommendations in the next section.

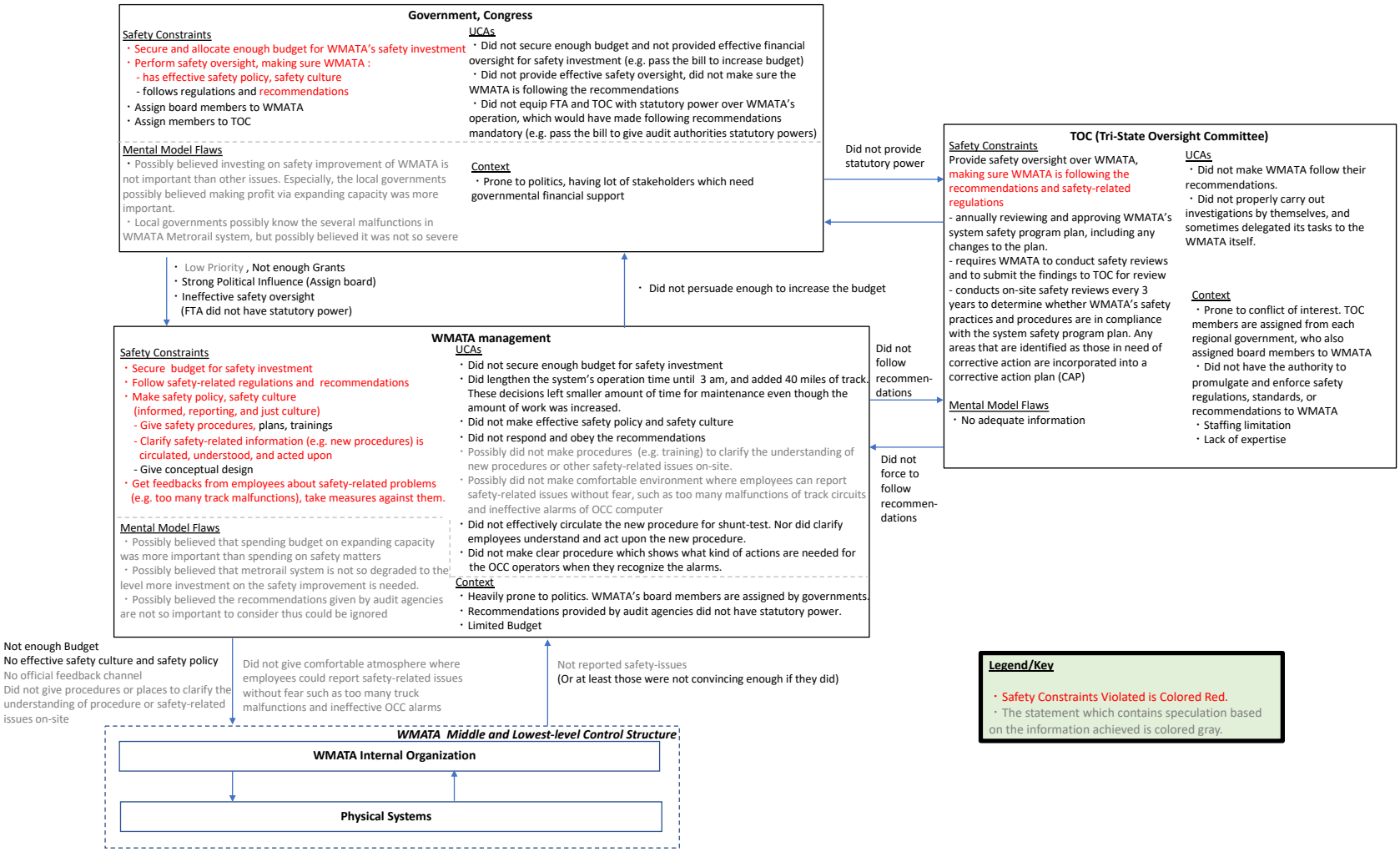


Figure 3- 22 Safety Constraints Violated in the Highest-Level of Safety Control Structure.

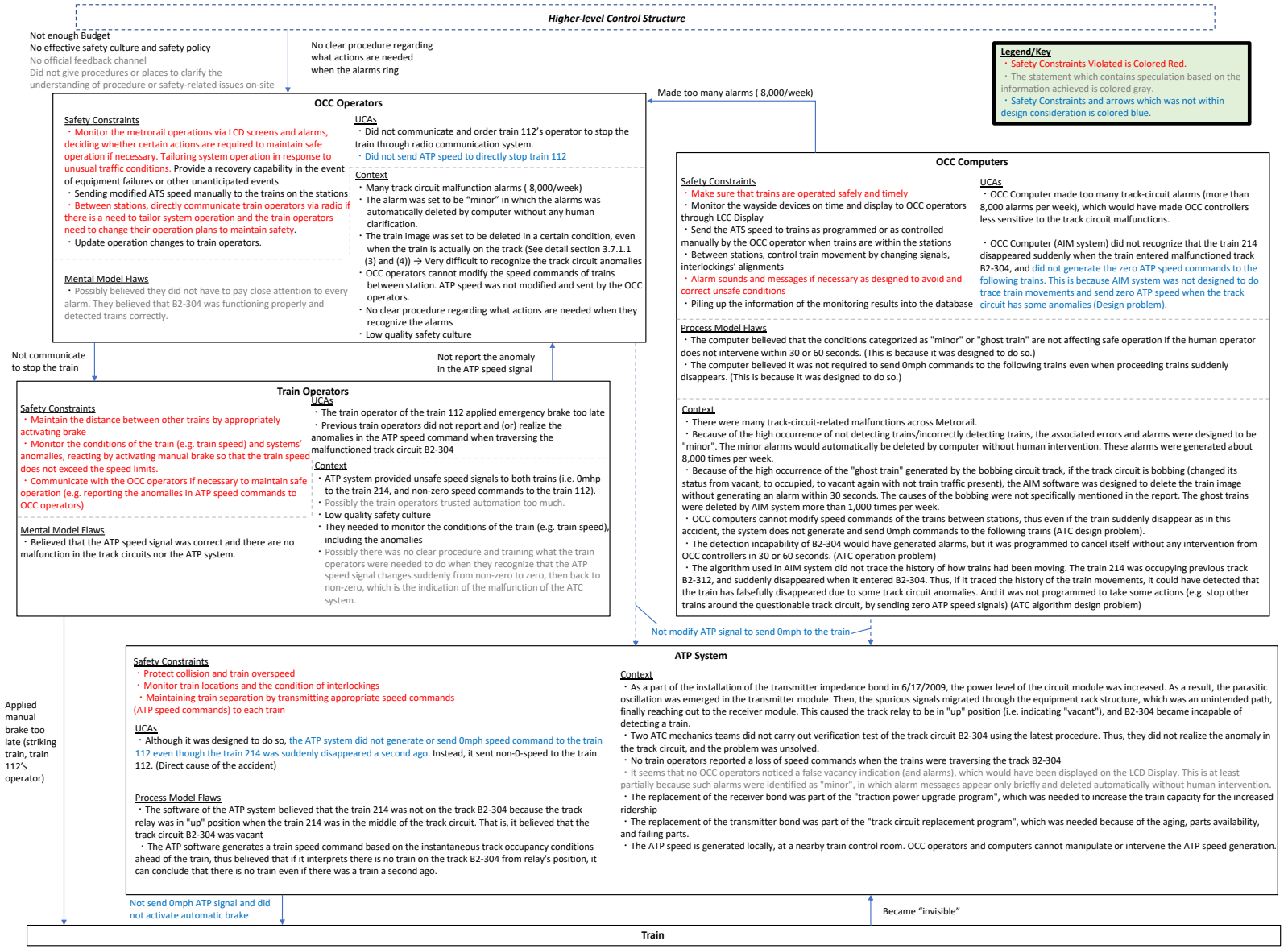


Figure 3- 23 Safety Constraints Violated in the Operator-Physical System Level of Safety Control Structure.

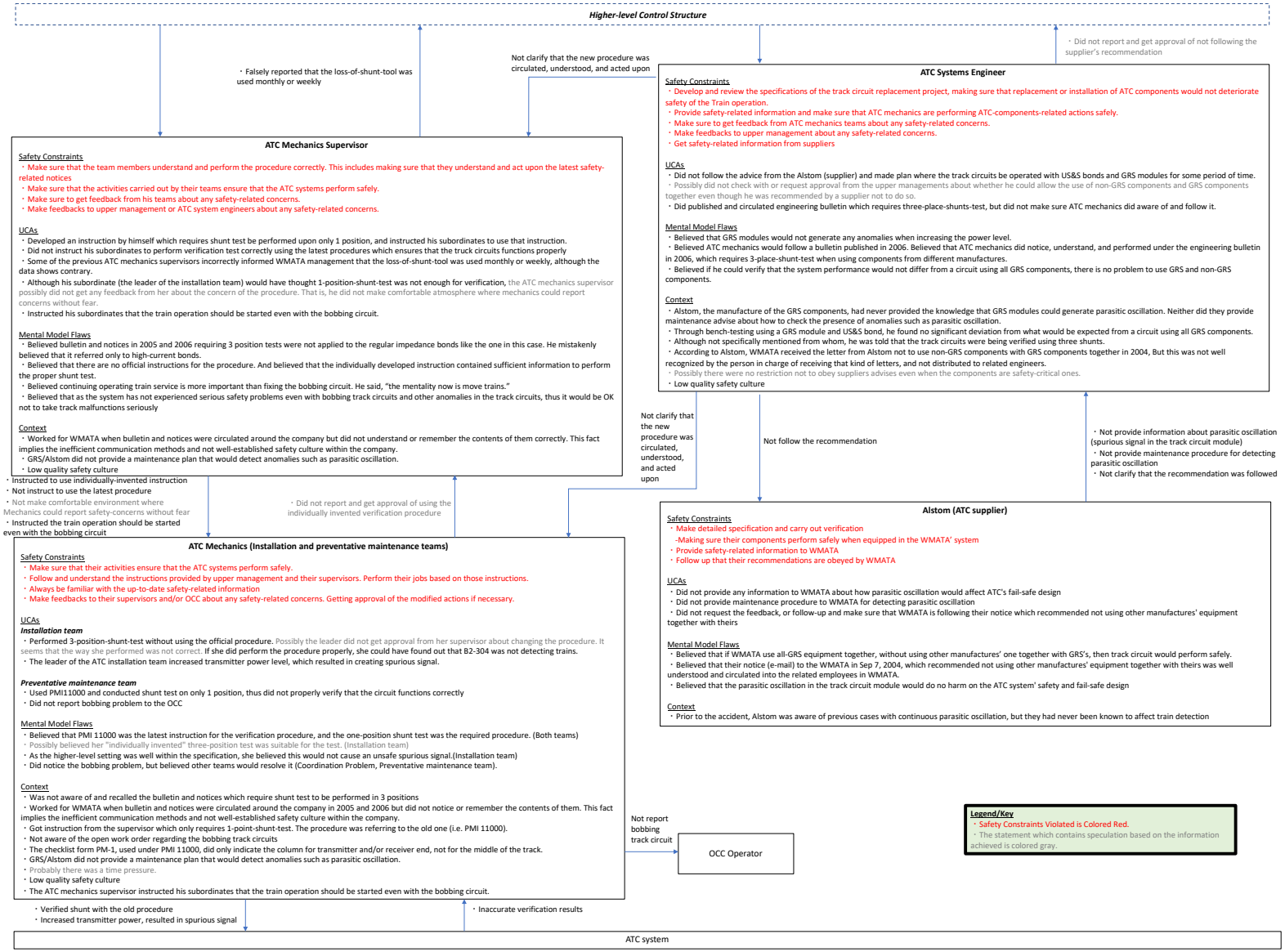


Figure 3- 24 Safety Constraints Violated in the ATC Engineers-Physical System Level of Safety Control Structure.

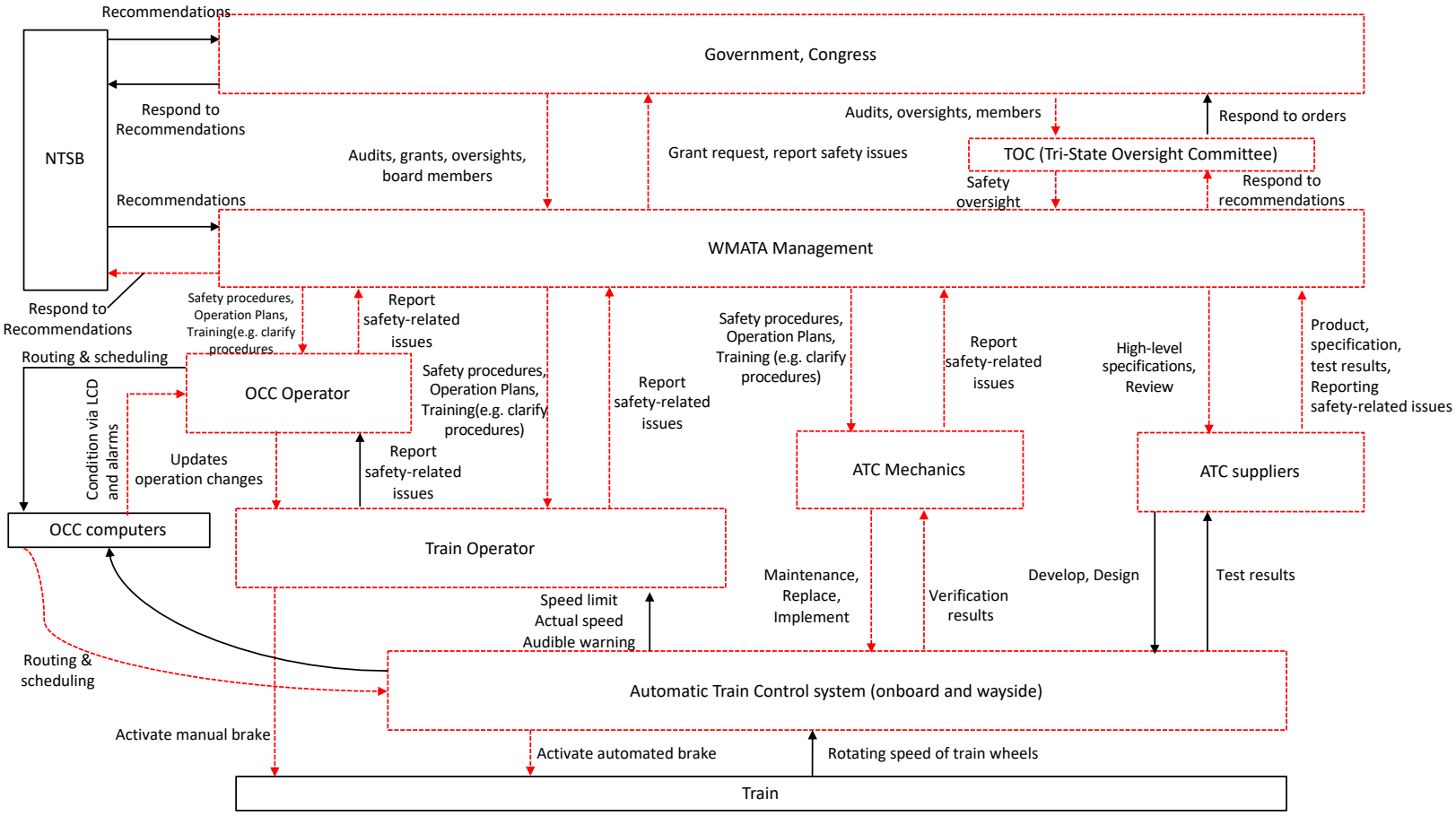


Figure 3- 25 Ineffective Control Actions, Feedback, and Controllers.

3.12 Generating Recommendations

The analysis can be used to propose new recommendations. Some recommendations can be developed by identifying how to eliminate or mitigate the identified factors in the future. As explained in the previous chapter, the goal of the analysis is not to identify a "root cause" but to identify all "causes" and enable more recommendations. Leveson's following argument was helpful to extract the recommendations from the analysis so far [6, p. 56]:

> …a new approach to understanding and preventing accidents rather than assigning blame, the emphasis is on identifying *all* the factors involved in an accident and understanding the relationship among these causal factors in order to provide an explanation of why the accident occurred. That explanation can then be used to generate recommendations for preventing losses in the future. Building safer systems will be more effective when we consider all causal factors, both direct and indirect. … there is no attempt to determine which factors are more "important" than others but rather how they all relate to each other and to the final loss event or near miss.

In addition, in summarizing these recommendations, the author referred to Citichem accident analysis [6, Ch. 11] and SBS Tank 731 Overflow accident analysis [33] for understanding how recommendations are documented by CAST Analysis professionals.

Systems Design

1. Evaluate the best way in which the operation conditions are displayed and alarmed to the OCC operators effectively, changing the interfaces and algorithm if necessary.
    - Consult with human factor professionals about possible design changes
    - If the malfunctions happen in safety-critical equipment such as the ATC system, then the alarms should not be categorized as "minor", and should be acknowledged by the OCC operators.

2. Evaluate the new design of the AIM system algorithm, which will request the OCC operators to take actions (e.g. stop trains) or automatically stop trains if necessary (e.g. if the computer is suspicious about the incapability of track circuits detecting trains).
    - Evaluate the design of the new algorithm of the AIM system, which will distinguish between "ghost trains" and the track circuit anomalies. Ensure the design has the least chance of not detecting trains, considering that the current algorithm at least in some cases does not distinguish between these two types and simply deletes the virtual train from LCD display. That makes it too difficult for the OCC operators to acknowledge the anomalies in the track circuits. The AIM system was already equipped with the capability of monitoring the track circuit function (e.g. bobbing or not detecting trains), thus the new design should be able to utilize the AIM's monitoring capability. That is, Figure 3-15 showed that when the train 214 was on the track B2-312, the AIM system successfully determined that the track circuit B2-312 was "non-reporting block," which suggests that the track should be occupied but not detecting trains. By redesigning algorithm, the malfunctioned track circuit, in this case track circuit B2-304, would also be able to be recognized as having anomalies by, for example, tracking the historical data of the track occupancy by a train (i.e. in this accident, the train 214). By doing so, the new algorithm would recognize that train 214 had disappeared suddenly, and could conclude that the track circuit B2-304 has some anomalies and is not detecting trains.
    - Evaluate the operational strategy of sending a stop signal (i.e. zero ATP speed signal) to the following trains when the track circuit is classified as "incapable of detecting trains" (i.e. when the algorithm determines that the track circuit is not (just) bobbing, but not detecting trains). The stop signal should be sent either automatically by the OCC computer or by the OCC operators' input.

Find and evaluate a way for the ATP speed to be manipulated and overridden by a human operator and/or OCC computer if necessary. For example, evaluate a design change of the OCC computer so that it can directly send ATP speed to the trains between stations, and also provide OCC operators with capability of manipulate ATP speed via OCC computers.

WMATA Management

1. Ensure that malfunctioned track circuits' components are replaced properly and promptly.
2. Ensure that the procedure for the verification of track circuits is followed properly.
3. Improve the methods used to identify hazards and the mitigation plans. Management should not wait until accidents happen to remove hazards and risks.
    - Consult with system safety professionals
    - Research the best practices in the industry
4. Ensure that manufactures are carrying out extensive Hazard analysis and identify all of them as far as possible using the best practices
5. Even when the systems are brand new and the frequency of malfunctions is very low, ensure that every malfunction is properly resolved in a timely fashion.
    - Even more so when malfunctions happen within the safety-critical systems such as ATC system
6. Allocate adequate amount of time and manpower for everyday maintenance activities.
    - Without adequate time for the maintenance, midnight operation should be avoided.
7. Allocate and invest in safety-related activities.
    - Management should keep in mind that the first priority is repairing or replacing the aged track circuits in a very timely manner.
    - It may be appropriate to campaign for adequate grants from governmental agencies.
8. Ensure that the safety-related budget is sufficient to maintain safe operation.
    - Avoid deciding upon non-safety-related capital investment (e.g. capacity expansion projects) when these investments adversely impact the safety-related budget
    - Evaluate current financial policy (i.e. amount of the money received from higher-level controllers, the amount of the money allocated to non-safety-related and safety-related activities), asking outside independent specialists for help with the process. Chang the policy if necessary.
    - Campaign appropriately for increasing budget or grants from governmental authorities, presenting effectively to them how severely degraded the systems are and the urgent need for the extra funding.

9. Make effective official communication channels, making sure any safety-related updates are well circulated around the company, well understood, and acted upon. Management should provide an explicit procedure for this process.
    - Create an environment where employees can comfortably report any safety-related issues without fear
    - Do not rely solely on the informal feedback from lower-level controllers.
    - Always check the validity of information through official communication channels
    - Consult professionals about possible communication systems. Also research and/or ask for best practices in the transportation industry. It would be useful to consult with specialists in the aviation industry where the safety culture seems to be more mature.
10. Require that all changes to the safety-related procedures are approved by upper-level controllers.
    - If the higher-level controller is not the same person who made the official procedure, then he/she must ask that person for approval. The management should provide an explicit procedure for this process.
11. Require that the manufacturers' recommendations are followed
    - If a need arises to deviate from manufacturers' recommendations, then the reasons and the design alternatives should be evaluated and approved by higher-level controllers. Management should provide an explicit procedure for this process.
12. Evaluate the operation strategy to stop every train when there is any malfunction in safety-critical equipment (e.g. track circuits)
    - Considering the current situation where the track circuits malfunction are too prevalent, the best timing would be after the most of the malfunctions are cleared
    - This specific operation strategy is only an example. Other best strategies should also be evaluated simultaneously.
13. Make and carry out the training programs to make sure the recommendations provided above are properly followed and maintained throughout the WMATA.
14. Follow properly the safety recommendations provided by NTSB and other audit authorities in a very timely manner.
    - This includes recommendations provided before this accident.

15. Create a clear procedure that identifies specific actions needed for the OCC operators when they recognize the alarms.
16. Create a clear procedure specifying what the train operators must do when they recognize that the ATP speed signal changes suddenly from non-zero to zero, then back to non-zero, which is the indication of the malfunction of the ATC system. The WMATA management should provide training that enables the train operators to learn this procedure, and then clarify their understanding through, for example, paper tests, or a simulator training.

Congress and Governments

1. Make the audit authorities independent from WMATA management
2. Provide audit authorities with the statutory power to compel a transit authority like WMATA to follow safety-related recommendations
3. Evaluate the amount of money required for improving WMATA's rail operation safety, then create a strategy to allocate sufficient money to WMATA

3.13 Conclusion

In this chapter, the WMATA Metrorail accident in 2009 was analyzed using the CAST framework. The causal factors that contributed to the accident were at every level of hierarchy in the safety control structure. This result supports the idea that there is no "root cause," but many causes. The causes at each level of the structure together contributed to the loss event.

Although there is no single root cause, the causes or causal factors can be classified into some categories, such as Organization Structure, Managerial Decision, System Design, Safety Culture, and many others.

For organization structure, one of the issues was that FTA and TOC, the audit authorities, did not have statutory power to force Amtrak to follow the recommendations, and Amtrak has not been willing to and did not follow their recommendations. In addition, WMATA's management did decide upon expanding capacity, however they did not allocate enough towards safety investment. Furthermore, there were several system design issues. One thing is that the alarm, which notifies

dispatchers that there is likely a malfunction component, was set to be cancelled out 30 seconds after it starts to ring. The extremely high number of alarms (8,000 times / week) were generated due to the malfunctioning infrastructure and made it nearly impossible for a dispatcher to identify that ATC component, a highly-safety-critical system, was not functioning safely. Other design issues include the lack of means for the train dispatcher to modify the speed signal for the trains between stations, which was only locally generated and did not allow human intervention. An effective safety culture was not embedded in WMATA. The on-site engineers did not follow the required procedures and they were even not familiar with the latest verification procedures. Additionally, their supervisor invented his own maintenance procedure without getting approval from upper-level controllers. In addition to these factors, there were issues which can be categorized as Human Factor Issues or Coordination problems.

Most importantly, these causes should be eliminated or at least reduced by implementing the recommendations summarized in the section 3.12.

In the next chapter, another CAST analysis is discussed and documented. Then the recommendations in chapter 3 and 4 are translated into common patterns and lessons learned which can be used to improve future system designs and operations throughout this industry.

(This page intentionally left blank)

Chapter 4 CAST Analysis 2 – Amtrak Derailment in 2015

> *"Having said that, we have also investigated accidents that demonstrated that introducing automation into a complex human-centric situation can present many challenges. Those challenges can be exacerbated when, as here, the automation is partial instead of complete. In this instance, the curve where the derailment occurred had automatic speed protection in one direction, but there was no speed protection for trains going in the direction of Amtrak 188. … Experience has shown, however, that partial automation can be more dangerous than no automation at all."*
>
> --- Christopher A. Hart (NTSB Chairman in 2016) [34]

In this chapter, CAST is applied to analyze the Amtrak derailment in 2015. The accident involved a lack of a speed-reduction system in front of the steep curve, and the train operator handling another emergent situation just before the accident. According to the NTSB's accident report, the train operator's loss of situational awareness is the probable cause leading to the accident. However, in spite of his violation of speed limit, his action seems somewhat reasonable considering the environment he was confronting, that is, less visual outside cues due to darkness, a similar curve after the derailment site contributed to confusion in recognizing the location without any visual aids, and other factors.

In this accident, no components failed, and every component at the physical system and operator level (lowest level of the Safety Control Structure) acted as they were designed. However, the system had been in an unsafe condition as a result of a sequence of unsafe control actions (lack of necessary design constraints) on every level in the Safety Control Structure. This case study would be beneficial for understanding (1) the importance of considering human factors (limitation of human capabilities) in designing automation systems, and (2) how governmental and managerial decisions could degrade an integrity and safety of the system.

Most of the information below is from the official report [34] and internet-available resources such as news articles and the Amtrak homepage.

4.1 Summary of the accident

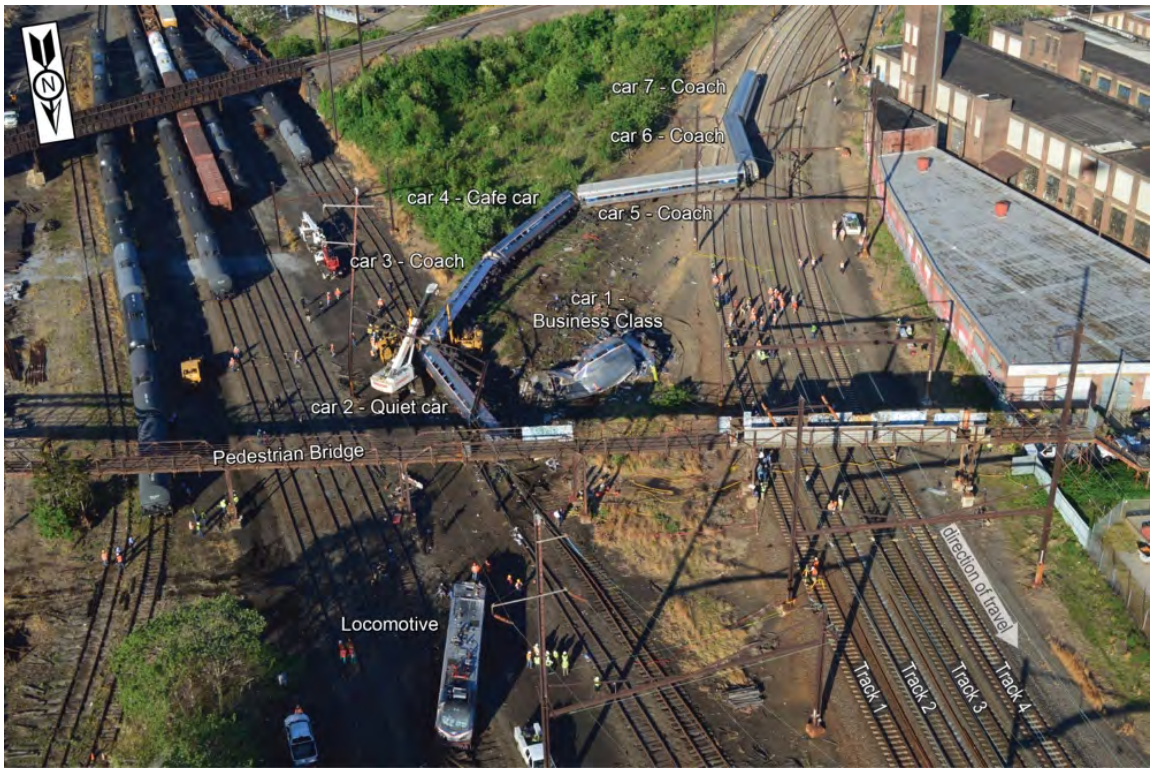


Figure 4- 1 Amtrak Train 188 derailed in Philadelphia on Northeast Corridor.

(Adapted from NTSB report [34] **)**

On May 12, 2015, eastbound Amtrak (National Railroad Passenger corporation) passenger train 188 derailed in Philadelphia, Pennsylvania on Northeast Corridor (NEC). The accident scene is shown in Figure 4-1 above. The train 188 did not decelerate enough and entered the Frankford Junction curve at 106mph, while the speed limit of the curve was 50mph. The accident location was dark at night about 9:21 p.m. The visibility was 10 miles.

There were 245 passengers, 5 on-duty and 3 off-duty Amtrak employees on board. Eight passengers were killed, 46 passengers were seriously injured, and 113 passengers were minorly injured. Amtrak estimated that the total damages to be more than 30.84 million US dollars. An adjacent Consolidated Rail Corporation (Conrail) track sustained about 330 thousand US dollars in damages. The route overview of North East Corridor and derailment point is shown in following

Figure 4-2. The detailed view of the accident route is shown in Figure 4-3.



Figure 4- 2 Amtrak Northeast Corridor Route Overview.

(Adapted from NTSB report [34])

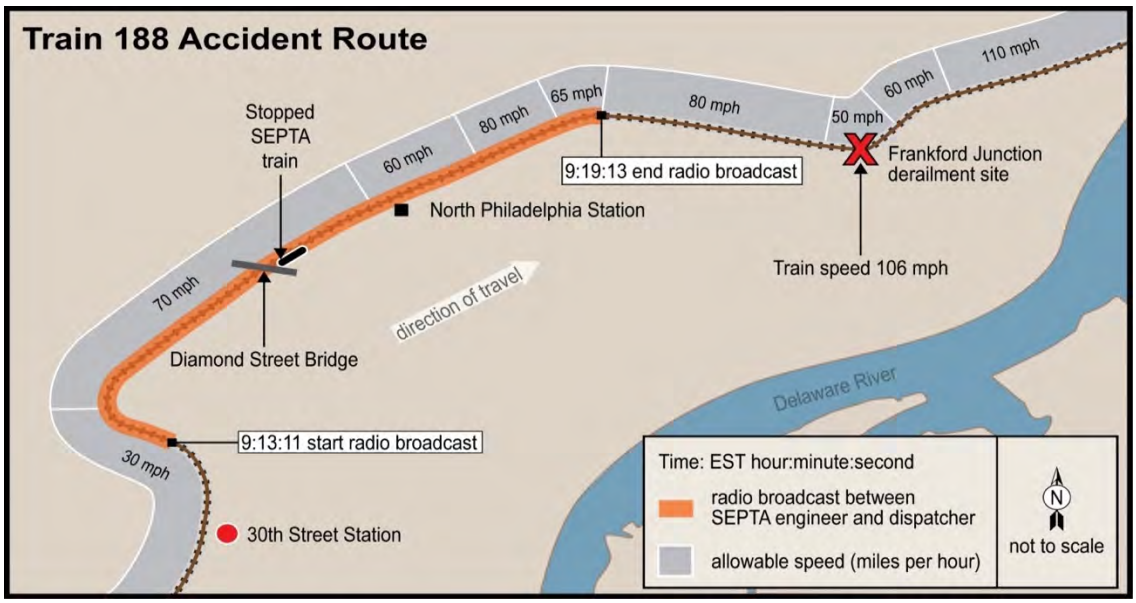


Figure 4- 3 Train 188's Route Through Philadelphia.

(Adapted from NTSB report [34])

According to the NTSB report, the probable cause of the accident was that the "engineer's

acceleration to 106 mph as he entered a curve with a 50 mph speed restriction, due to his loss of situational awareness likely because his attention was diverted to an emergency situation with another train." The contributing factor was "the lack of positive train control system." The contributing to the severity of the injuries were "the inadequate requirements for occupant protection in the event of a train overturning." [34]

4.2 The National Railroad Passenger Corporation (Amtrak)

4.2.1 History and its Mission

Passenger train service was the mainstream for long-haul travel in the US until 1950s when jet airplanes and the Interstate Highway System gained momentum and there had been a rapid modal shift away from rail service to these competing transportation modes. This led to the further deterioration of passenger service profits for the major rail operations and the level of service became worse across the country. It was getting increasingly apparent that the passenger train would be extinct.

At this time period, some of the supporters, like National Association of Railroad Passengers, lobbied members of Congress, having argued against service cuts. With the bankruptcy of the Penn Central Railroad, Congress passed the Rail Passenger Service Act in 1970. This law created Amtrak and assigned it the responsibility of operating the national intercity passenger rail system. As directed by the law, DOT (Department of Transportation) determined which existing routes would be operated, and stipulated that the company would be a for-profit organization. The law also provided for the inauguration of routes outside the existing system with financial support from state authorities. The designated network was about half of the passenger rail services that existed at the start of 1971. Most of these routes still remain today [35]. After Amtrak started its operation on May 1, 1971, it acquired its Northeast Corridor property through the Conrail consolidation process. [36]

Amtrak's mission is "to deliver intercity transportation that helps move people, the economy and the nation forward. Amtrak is advancing its goal of being Americans' preferred mode of travel by running an efficient and effective business; modernizing the customer experience; and

investing in infrastructure, the locomotive and car fleets, and stations and facilities" [36].

4.2.2 Financing System and Board Members

Amtrak is a federally chartered corporation, with the federal government holding majority of company's stock [36]. Historically, Amtrak has been receiving financial supports from government and it would not be able to continue its business without this funding:

> The Company has a history of recurring operating losses and is dependent on subsidies from the Federal Government to operate the national passenger rail system and maintain the underlying infrastructure. These subsidies are usually received through annual appropriations. Appropriated funds for Amtrak are generally provided to the DOT, which through its agency the Federal Railroad Administration (the FRA) provides those funds to Amtrak pursuant to annual grant agreements. Amtrak's ability to continue operating in its current form is dependent upon the continued receipt of subsidies from the Federal Government. The DOT, formerly through the FRA, and now through the National Surface Transportation and Innovative Finance Bureau of the Federal Government (also referred to as the Build America Bureau), also provides financing to Amtrak through the Railroad Rehabilitation and Infrastructure Financing (RRIF) Program [37].
>
> Without the receipt of Federal Government funding, Amtrak will not be able to continue in its current form and significant operating changes, restructurings, or bankruptcy might occur [38].

Seven of nine board members are appointed by the US President and confirmed by the US Senate, and they are removable by the President without cause. The remaining members include the Secretary of Transportation. The 9th member is chosen by the other eight, and also serves as Amtrak's president. Justice Kennedy on the Supreme Court argued that the political branches "exercise substantial, statutorily mandated supervision over Amtrak's priorities and operations." The rationale

behind this statement was that Amtrak must submit detailed annual operation reports, and attend frequent congressional oversight hearings, and so on. He also maintained that “rather than advancing its own private economic interests, Amtrak is required to pursue numerous, additional goals defined by statute.” “Amtrak was created by the Government, is controlled by the Government, and operates for the Government’s benefit” [39]. It is also argued by *the Hill* that:

> However, Amtrak has been on a life support budget for almost all of its existence and an easy target for cuts under the guise of “saving money.” … Nobody wants or will pay the true cost to ride out of their own pocket. Consequently, government has a “say” in whatever it helps fund. Amtrak is no different. … Therefore, unlike a private corporation, Amtrak is much more susceptible to political interference in train routing choices, selection of managers, etc. Such government political interference burdens Amtrak financially and operationally [40] .

To sum up, due to its origin and corporate structure, Amtrak is prone to political interference, and one can safely argue that the Amtrak’s managerial decisions would be influenced by governmental pressures to some extent.

4.2.3 Current Operation Information

Amtrak operates a nation-wide rail service network. It serves more than 500 destinations in 46 states, the District of Columbia, and three Canadian provinces on more than 21,400 miles of routes in total. Amtrak is the US’s only high-speed intercity passenger provider, operating at maximum 150mph (241kph). Almost half of its trains run at top speeds of 100mph (160kph) or faster. The number of employees is over 20,000.

Seventy-two percent of the miles traveled by Amtrak trains are on the tracks owned by other railroad organizations. They are known as “host railroads”. Amtrak pays utilization fees to these host railroads for the use of their track and other resources needed to operate Amtrak’s trains.

There are four types of operation services served by Amtrak. These include NEC, State-

supported, Long-distance, and Contract Commuter services (See Figure 4-4 below for how these services are located in the US, the commuter services are not specified though) [36].

Among first three services (i.e. NEC, State-supported, and Long-distance), only NEC service has been making profit. Sixty-seven percent of state-supported and 100% of Long-distance are generating negative earnings in FY2017 [41].

Although Amtrak has been slightly increasing its ridership recent years, it has been continuously making Loss and getting grants from Federal and Local governments (See Table 4-1).



Figure 4- 4 Amtrak National Network in FY 2017.

(Adapted from Amtrak Company Profile FY2017 [3])

Table 4- 1 Amtrak's Financial and Ridership Data

	(Units: million US dollars)			
	2018	**2017**	**2016**	**2015**
Federal Grant	**$1,924.90**	**$1,480.50**	**$1,381.50**	**$1,379.30**
Total Revenues	**$3,386.73**	**$3,305.71**	**$3,240.56**	**$3,211.00**
State supported Revenues (Included in Total revenues)	**$233.80**	**$224.00**	**$227.00**	**$222.90**
Total Expenses	$4,238.95	$4,210.40	$4,261.27	$4,332.60
Loss before other (income) and expenses	$852.22	$904.69	$1,020.71	$1,121.60
Net Profit	**$-817.21**	**$-968.71**	**$-1,080.49**	**$-1,232.70**
NEC Ticket revenue	Not available	$1,238.30	$1,209.20	$1,198.70
Toal Ticket revenue	$2,207.20	$2,180.80	$2,192.20	$2,185.50
NEC Ticket revenue %	**-**	**57%**	**55%**	**55%**
	(Units: million)			
NEC Ridership	12.1	12	11.9	11.7
Total Ridership	31.7	31.7	31.3	30.9
NEC Ridership %	**38%**	**38%**	**38%**	**38%**

(Data Source: Amtrak[30])

Northeast Corridor Services

NEC is providing "premium and regular intercity rail passenger service along the NEC while seeking to maximize operating surplus. Its customers are intercity travelers on the NEC." [41]

When compared with and included among US airlines, Amtrak ranks No. 5 in domestic passengers carried. In the NEC, Amtrak carried over three times more passengers between Washington, D.C., and New York City, and more passengers between New York City and Boston than all of the airlines combined [36].

The key NEC's operation metrics are summarized in Figure 4-5. The NEC's ridership has been increasing over two decades (See Figure 4-6). Accordingly, the ticket revenue increased (See

[30] The data was gathered from Annual Reports and Consolidated Financial Statements (FY15-18), Grand and Legislative Requests (FY16-19), FY19-23 Five Year Service Line Plans, and Sep 2017 Year-End Reports [42], and the article on Amtrak HP [43]. The years indicated in the Table represent the company's fiscal years ended September 30, 2018, 2017, 2016, and 2015.

Figure 4-7), and so did market share (See Figure 4-8).

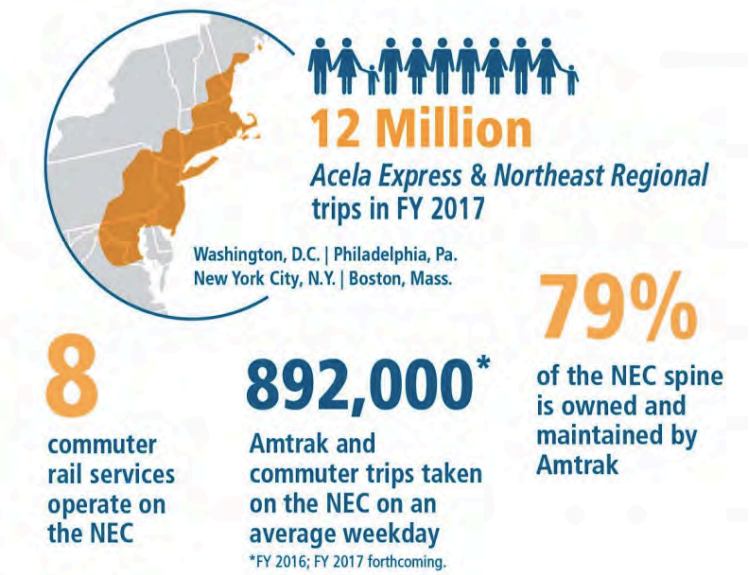


Figure 4- 5 NEC Key Operation Metrics.

(Adapted from Amtrak [36])

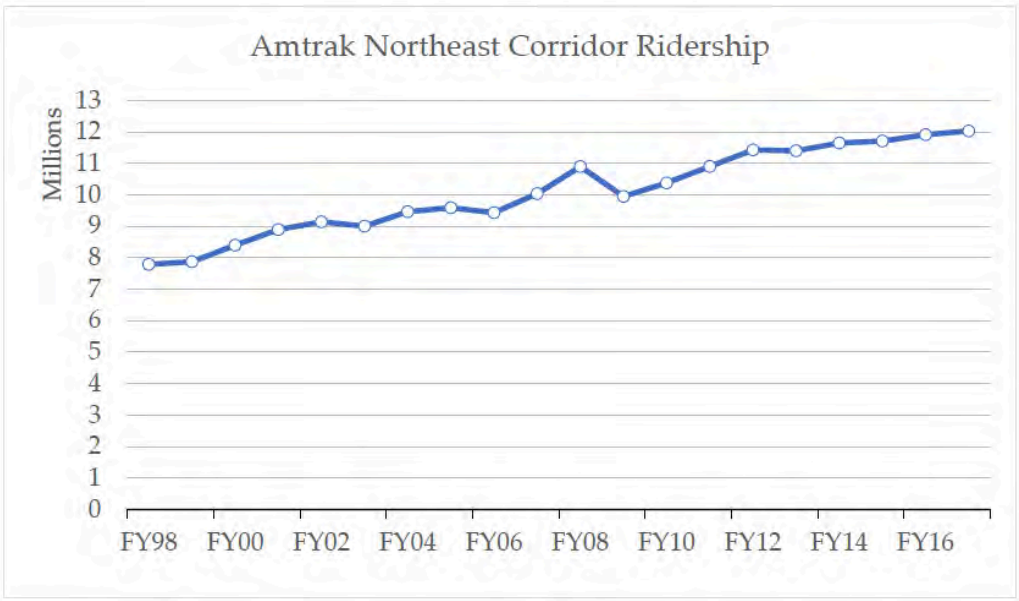


Figure 4- 6 NEC Ridership growth, FY 1998 – FY 2017.

(Adapted from Amtrak [8])

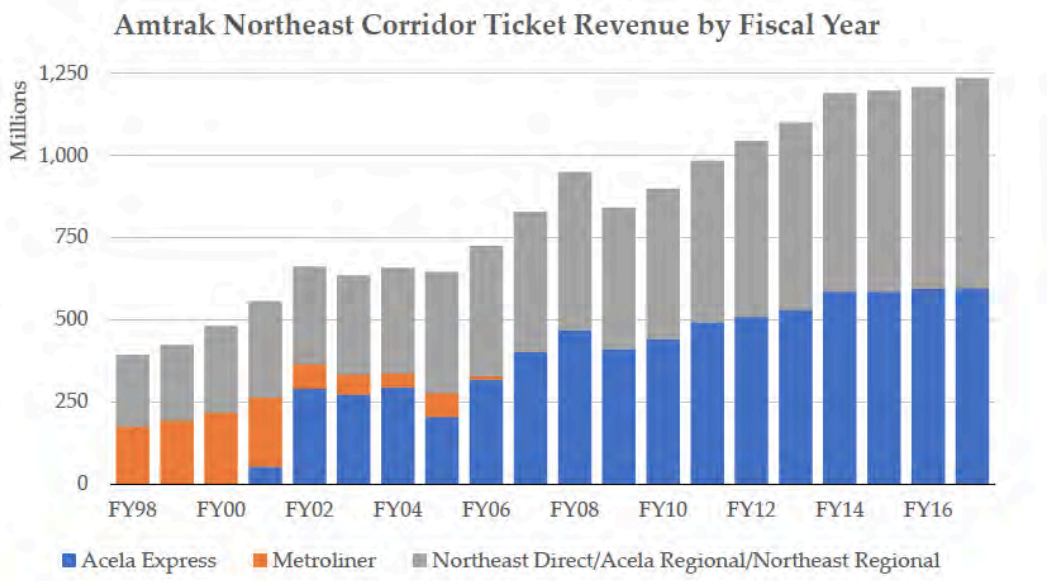


Figure 4- 7 NEC Ticket Revenue growth, FY 1998 – FY 2017.

(Adapted from Amtrak [8])

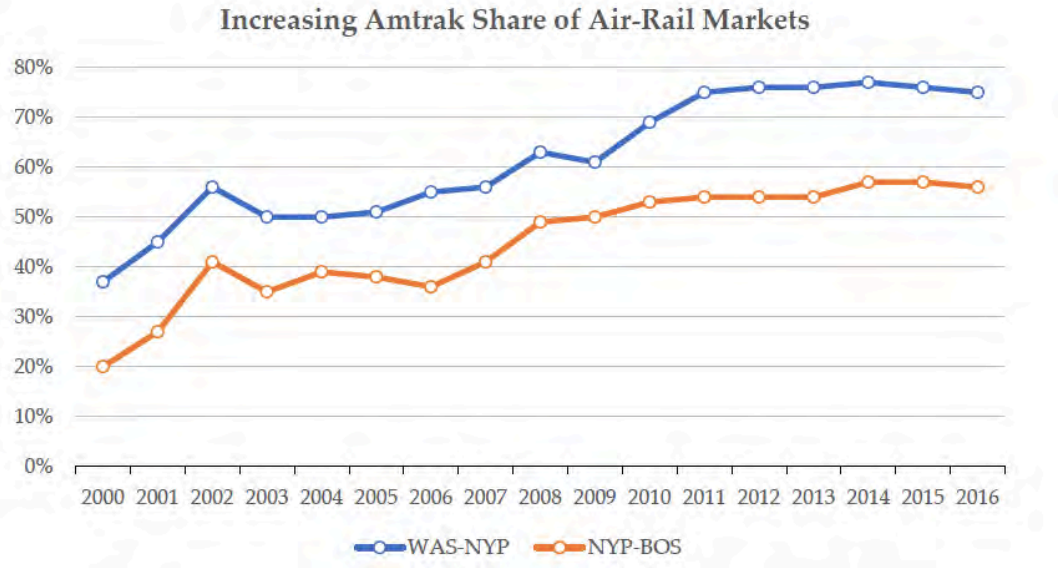


Figure 4- 8 NEC Market Share growth, FY 2000 – FY 2017.

(Adapted from Amtrak [8])

Although NEC is profitable and competitive compared to other services provided by Amtrak, they insist that the NEC is facing near-full capacity and key assets need major repairs in its FY19 grant request report. They argue that some bridges and tunnels are over a century old and some of electrical and signal systems were implemented back in the 1930s, meaning that there are aging assets which are prone to unexpected failures that could disrupt service and create operation delays. They maintain that those infrastructures remain in service due to scarce funding. They also assert that the investment in the NEC has lagged and its infrastructure has gradually deteriorated. They estimate that the backlog has reached 38 billion US dollars. They insist that the condition will be worsen if an adequate amount of investment is not made, impairing the reliability of operations [41].

State-Supported Service

State-supported service is providing "intercity rail passenger service and supporting services under contract to States on corridor routes of not more than 750 miles. Its primary customers are State Departments of Transportation and authorities, and intercity travelers" [41]. The key State-supported service's operation metrics are summarized in Figure 4-9.



Figure 4- 9 State-Supported Service Key Operation Metrics.

(Adapted from Amtrak [36])

Long-Distance Service

Long-distance service is providing "intercity rail passenger service on routes of more than 750 miles. Its primary customers are travelers and communities across the National Network and the federal government" [41]. The key Long-distance service's operation metrics are summarized in Figure 4-10.

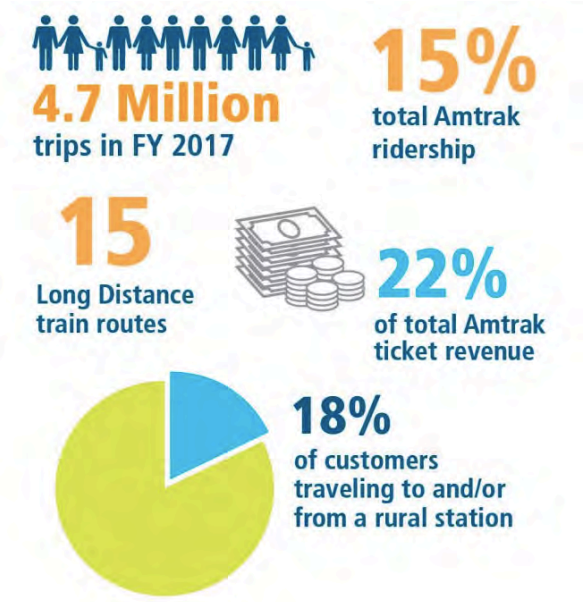


Figure 4- 10 State-Supported Service Key Operation Metrics.

(Adapted from Amtrak [36])

4.3 Train Control Systems on the Northeast Corridor (NEC)

4.3.1 Train Control System Overview

Modern signal systems can be thought of as a pyramid, consisting of Automatic Block Signal System, Cab Signals, Automatic Train Control (ATC), and Positive Train Control (PTC) on the top [44]. See Figure 4-11 below for the hierarchy of the pyramid.

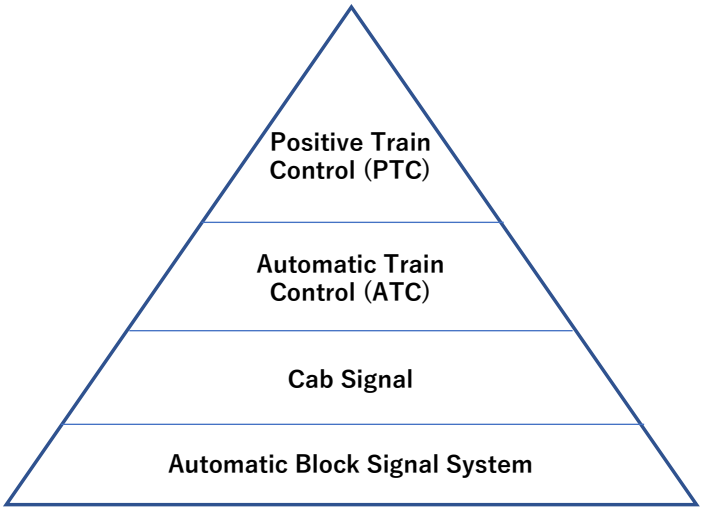


Figure 4- 11 Pyramid of Modern Signal Systems.

Automatic Block Signal System

The base of the pyramid is Automatic Block Signal, which indicate the colored lights, and informing the train operator that (s)he needs to activate brake and decrease speed in order to avoid collisions. However, this system does not override engineers if they do not take proper actions. See Figure 4-12 for an overview.

As Figure 4-12 illustrates, the tracks are divided into "section" or "block," and the Automatic Block System prevents the following train (Train #2) to enter the same block with the previous train (Train #1). Although actual signal algorithm would be different from systems to systems, one example is that the system indicates the "red signal (distant signal)" at the beginning of the block occupied by the previous train, and the "yellow signal" at the beginning of the block which is one block ahead of the occupied track.

As it takes a long distance and time to fully stop the train with full speed, the system needs to consider the "Stopping distance," which is decided by the current speed of the train. As the signals are not visible from that far away, the yellow signal is needed to warn train operators the need of the braking. As the current speed affects the stopping distance, sometimes yellow signal can be indicated at the beginning of the track which is two blocks ahead of the occupied track.

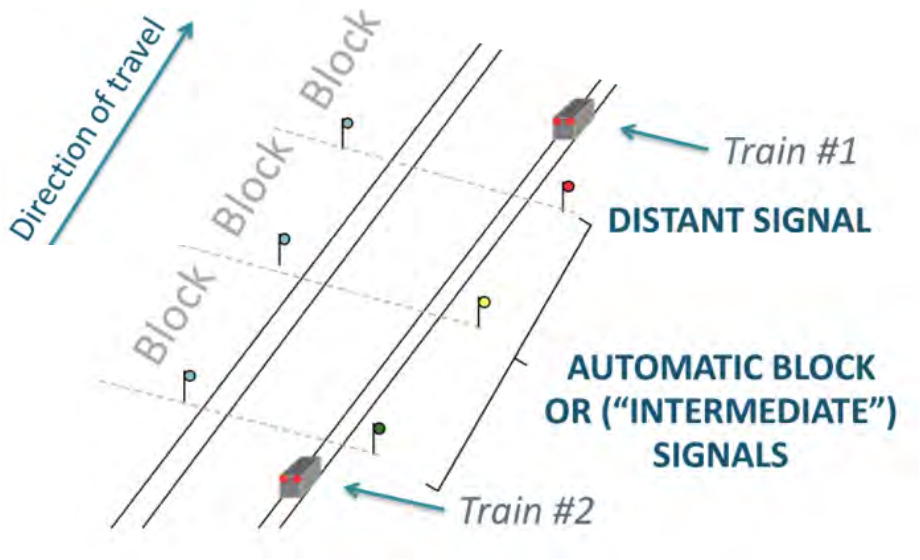


Figure 4- 12 Overview of Automatic Block Signal System.

(Adapted from Amtrak [45])

Cab Signals

The next (upper) level sits Cab Signals, which basically duplicates the indications of the wayside signals created by Automatic Block Signal System. Cab Signals are very helpful and important in bad weather or when train runs at a high speed, and wayside signals are difficult to see from the cabin. Like the wayside signals, Cab Signals do not have overriding ability when the train operator does not appropriately slow the train. For the Cab Signals implemented in the area of the accident, see Table 4-2 below.

Table 4- 2 Cab Signal Indications on the Accident Site

NORAC Rule	Name	Indication	Speed Enforced
280	Clear	Proceed not exceeding Normal Speed (Normal Speed is Maximum Authorized Speed by Timetable)	Limited only by speed governor on locomotive
282	Approach Medium	Proceed approaching the next signal at Medium Speed	45 mph
285	Approach	Proceed prepared to stop at the next signal. Trains exceeding Medium Speed must begin reduction to Medium Speed.	30 mph
290	Restricting	Proceed at Restricted Speed	20 mph

(Adapted from NTSB report [34]**)**

Automatic Train Control (ATC)

ATC is able to automatically slow or stop a train if a train operator does not comply with the speed limit set by the cab signal. While ATC can enforce speed reductions to either 20, 30, or 45 mph[31], it is **not capable of** enforcing a speed restriction on a curve[32] or stopping a train at a Stop Signal if the train operator does not reduce the train speed [44].

The ATC system relies primarily on hard-wired control points, called "**cab signal change point[33]**," installed in the track and do not protect against overspeed conditions if this equipment is not implemented. If a train operator does not reduce the speed before the steep curve in which this equipment is implemented, then the cab signal would drop from clear to Approach medium, enforcing the speed restriction. However, **if it is not implemented, the ATC system basically does nothing even if the train operator does not apply brake. The most important thing noted about ATC system in this accident analysis is that the cab signal change point was not equipped in the**

[31] From the information acquired through the references, it is likely that the speed reductions are based both on the proximity to other trains and the current location of the train. For a latter case, however, only a selected curve had speed-restriction capability only if the curve was equipped with a cab signal change point. There is no clear explanation about the straight track.

[32] It is not clearly explained in the reference [44], whether there are some straight track which is not capable of enforcing speed restrictions.

[33] The author could not find clear explanation about how long the speed restriction last after a train encounters a cab signal change point. This is only a guess though, it is likely that the speed restriction will expire if the train pass the "block" which is controlled by this cab signal change point.

accident site, and it did not enforce speed reduction even if the train exceeded the civil speed limit.

The following are some of the Amtrak ATC's functions (Does) and limitations (Does not) which are important to fully understand the accident analysis provided later [34]:

- Does enforce speed reductions down to 20, 30, or 45 mph if the train operator does not slow the train speed and the cab signal change point is installed in the track.
- Does **not** automatically stop a train even if the train operator does not slow and stop the train at a stop signal[34].
- Does **not** automatically apply brake if a cab signal change point is absent, even if the train driver does not reduce the train speed below the restricted speed.
- Does **not** show the location of the train
- Does **not** allow dispatcher to enforce the temporal speed restriction. (There is no means to directly send modified speed signal from dispatcher to the train. This is the same design policy with the ATC system of WMATA discussed before)

To sum up, the ATC system used in Amtrak is not a perfect speed-control system. Due to its design, "ATC is only activated[35] on specific stretches of rail deemed risky by railroad managers" [47], as cab signal points are selectively implemented.

Positive Train Control (PTC)

The top of the pyramid sits the Positive Train Control (PTC). At the time of the accident,

[34] From the information gathered, the author could not figure out why Amtrak operates trains with this design. That is, if the train cannot automatically stop on the stop sign, then it would lead to the train-to-train collision if the train operator does not activate brake and stop the train. However, this policy is contradicting with Table 4-3, which says that the ATC's functions meet the requirement of PTC's train-to-train collision protection. If the ATC had not been capable of stopping the train automatically, the chances are fatal collision accident will happen. The protection against train-to-train collision is very important function recently as some other accidents happened due to train operators' losing consciousness during his/her duties. See [46], for example.

[35] This means that ATC's civil speed restriction can be activated only if the cab signal change point is implemented on the track.

it was implemented and operated on 206 of the 401 miles of track that Amtrak was responsible for on the NEC. But not on the accident site.

As explained in detail later, Amtrak's PTC would be accomplished by combining functions of ATC and ACSES (Advanced Civil Speed Enforcement System) or I-ETMS (Vital Electronic Train Management System, a.k.a. ITS System). ACSES or I-ETMS would supplement the functions which current ATC system are not equipped with. These functions include automatically stop a train ahead of a red signal (only at home signal location[36]), or slowing trains ahead of steep curves[37] [45].

4.3.2 Positive Train Control Legislation - Railroad Safety Improvement Act

After several "PTC-preventable" accidents [45], Congress passed the Railroad Safety Improvement Act of 2008 (RSIA08; P.L. 110-432), that mandates Positive Train Control (PTC) on many railroads of both passenger and freight by Dec 31, 2015. The RSIA08 does not describe PTC system in technical terms, but it defines that PTC is "a risk mitigation system that could prevent train incidents by automatically stopping trains when a collision or derailment is imminent." The deadline for implementation was later prolonged by Congress to Dec 31, 2018, due to the cost and technical concerns raised by railroads.

Although PTC would improve safety of the train operation, it needs substantial costs and entails a variety of policy-related issues. These include "the access to sufficient radio spectrum to support PTC, the possibility that PTC could be a barrier to market entry, and the suitability of PTC to passenger terminal environments" [48].

[36] Home signal is the signal which protects the trains enter the interlockings. See the Figure B-1 in Appendix B, and find "home signal" in the figure.

[37] This could be accomplished by ATC system if the cab signal change point is implemented. However, Amtrak did not equip cab signal change point on every steep curve and waited until the PTC was fully operational. When accident happened, the accident site was not equipped with cab signal change point nor the PTC was operational. After the accident, Amtrak quickly implemented cab signal change point onto the steep curve which was not equipped with that, including the accident site.

4.3.3 Overview of Positive Control System Requirements set by RSIA08

PTC systems that meet the standards set by regulations are required to reliably and functionally prevent [45]:

- Train-to-train collisions
- Over speed derailments
- Incursion into an established work zone
- Movement through a main line switch in the improper position
- Other functions are applicable within the requirements as specific conditions warrant

4.3.4 PTC on the NEC

Frankly speaking, the official report documented by NTSB and most of internet-available resources including newspaper articles and even Amtrak's official website [44] were not good at explaining the relationship between Automatic Train Control (ATC) system and Positive Train Control (PTC) system. They explain PTC as if it is totally separate from the ATC system, when in fact the ACSES (Advanced Civil Speed Enforcement System) or I-ETMS (Vital Electronic Train Management System, a.k.a. ITS System) is supplementing the ATC system with the functions which are required for PTC legislation (i.e. RSIA08), but which ATC itself is not equipped with [35]. Although this "supplementing" is the way Amtrak decided to observe the legislation, there might be other approaches to meet the requirements posed by the RSIA08. See Figure 4-13 for the overview of ACSES and I-ETMS on NEC.

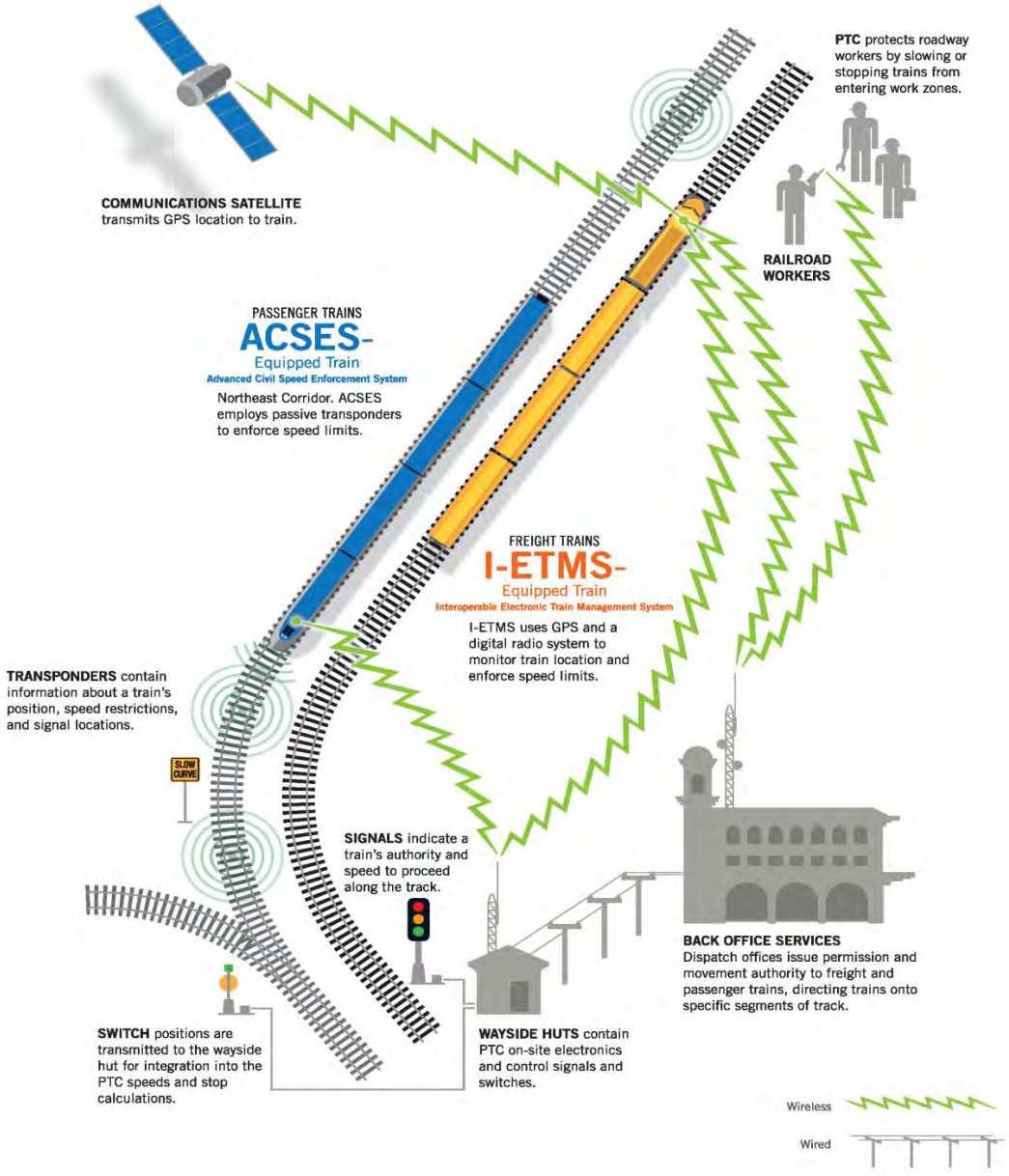


Figure 4- 13 ACSES and I-ETMS on NEC.

(Adapted from Amtrak Office of Inspector General [49])

ACSES Overview

ACSES is a vital overlay transponder-based system that combined with Automatic Train Control provides PTC functionality (See Table 4-3).

The primary functions of ACSES are providing civil and temporary speed, and positive stop enforcement (**at blocks prior to interlockings only**[38]) [35].

If this is true, that is, the ACSES is not capable of stopping trains automatically when there is a train ahead, this system cannot fully supplement ATC's shortcoming. The author believes this system can not ensure that train-to-train collision would be protected if the human operator does not apply brake properly.

The NTSB explained the following in their special investigation report analyzing two train accidents caused by Human Operators' sleep disorder in New Jersey in 2016, and in New York in 2017:

> From a safety perspective, the NTSB has recognized the importance of using technology to mitigate human errors and hazards created by single point failures[39]. The NTSB has advocated for the implementation of PTC systems to prevent collisions and overspeed events for more than 45 years. PTC has appeared on the NTSB's Most Wanted List of Transportation Safety Improvements for 23 of the 27 years that the list has been in existence [46].

The author sincerely agrees with NTSB's argument of "importance of using technology to mitigate human errors and hazards created by single point failures." **However, the PTC system that appears to be implemented does not eliminate single point failure.** That is, if the train operator does not apply brake, then a train-to-train collision could result.

Therefore, one can maintain that the government, media, and even NTSB's campaigning for implementing PTC were not perfect and they should have carefully analyzed hazards in the resulting system which actually would be implemented by railroads operators.

---

[38] See the Figure B-1 in Appendix B, and find "interlocking (cross over)" in the figure.

[39] A single point failure is part of a system that, if it fails, will stop the entire system from working.

Table 4- 3 How ATC and ACSES Satisfies the PTC Functional Requirements

PTC Functional Requirements	CSS/ATC	ACSES	Comments
Train-to-train collision protection	X	X	ACSES provided Positive Stop at Home Signals
Overspeed protection	X	X	
MAS		X	
Permanent civil speed restrictions		X	
Temporary speed restrictions		X	
Crossover speed restrictions	X	X	ACSES provides with ATC failure
Work zone intrusion protection		X	Vital blocking will be utilized for out of service track
Protection of mainline switches	X		
Highway crossing failure enforcement		X	Will enforce positive stop to a failed crossing.

(Adapted from Amtrak [35])

I-ETMS Overview

I-ETMS, which is a communication based vital overlay system that uses GPS for positioning, would supplement the function of ATC and the wayside signal system on the NEC in the areas where freight or commuter trains will fund the installation and be equipped with I-ETMS but not ACSES (See Table 4-4) [35].

I-ETMS would enforce a positive stop at interlocking home signals. However, from the information gathered, there is no explanation about a positive stop aside from interlocking home signals. If home signal is the only place where positive stop is enforced, then it is clear that I-ETMS is also incapable of eliminating train-to-train collision hazards.

Table 4- 4 How ATC and I-ETMS Satisfies the PTC Functional Requirements

PTC Functional Requirements	CTC/ABS Outside NEC	CSS/ATC On NEC	I-ETMS®	Comments
Train-to-train collision protection	X	X	X	I-ETMS® provides Positive stop at home signals
Overspeed protection		X	X	
MAS			X	
Permanent civil speed restrictions			X	
Temporary speed restrictions			X	
Crossover speed restrictions		X	X	
Work zone intrusion protection			X	Vital blocking will be utilized for out of service track on NEC
Protection of mainline switches	X	X		
Highway crossing failure enforcement			X	

(Adapted from Amtrak [35])

4.4 System Definition & Hazards

As a first step of CAST analysis, the System Definition, Accident Definition, and Hazards related to these accidents are described in following Table 4-5.

Table 4- 5 System Definition, Accidents, and Hazards (Amtrak)

System Definition
・In this analysis, the human components and non-human physical components such as Trains or Train control systems are all considered as part of the broader system. ・Both Amtrak components and higher-ranked components, such as legislative authorities or audit authorities, are considered part of the system. ・Operation, Maintenance, Implementation, Design, and Development are all considered in an analysis. ・Evacuation activities are not the focus of this analysis, thus those are considered as outside of the system.
Accidents
A1: Death and injuries of the people A2: Loss of the fortune (e.g. Money, Property/Facility)
Hazards
H1: Trains do not maintain safe distance from each other (i.e. Train collision) →Combined with H3 would lead to A1 and A2. H2: Train does not run on the track (i.e. Train derailment) →Combined with H3 would lead to A1 and A2. H3: Train seriously injures or ejects passengers during a crash H4: Train does not allow passengers to safely egress after a crash.

4.5 Safety Constraints and System Requirements Associated with Hazards

Next, Safety Constraints are identified which needs to be enforced so as to avoid the Hazards (See Table 4-6). Note that SC3 and SC4 are competing requirements which needs to be somehow resolved by appropriate design.

Table 4- 6 System-Level Safety Constraints and System Requirements (Amtrak)

Safety Constraints and System Requirements
SC1. Train must maintain safe distance from other trains→ H1
SC2. Train must not violate speed limit → H1, 2
SC3. Train must adequately protect occupants in the event of a crash. →H3
SC4. Train must allow passengers to safely egress after a crash →H4

4.6 Safety Control Structure

The high-level safety control structure is depicted in Figure 4-14. As with the WMATA case, some of the components, controls, or feedback are simplified and abstracted in the high-level control structure. A more detailed safety control structure is shown in Figure 4-15. In each figure, the human components are colored gray.

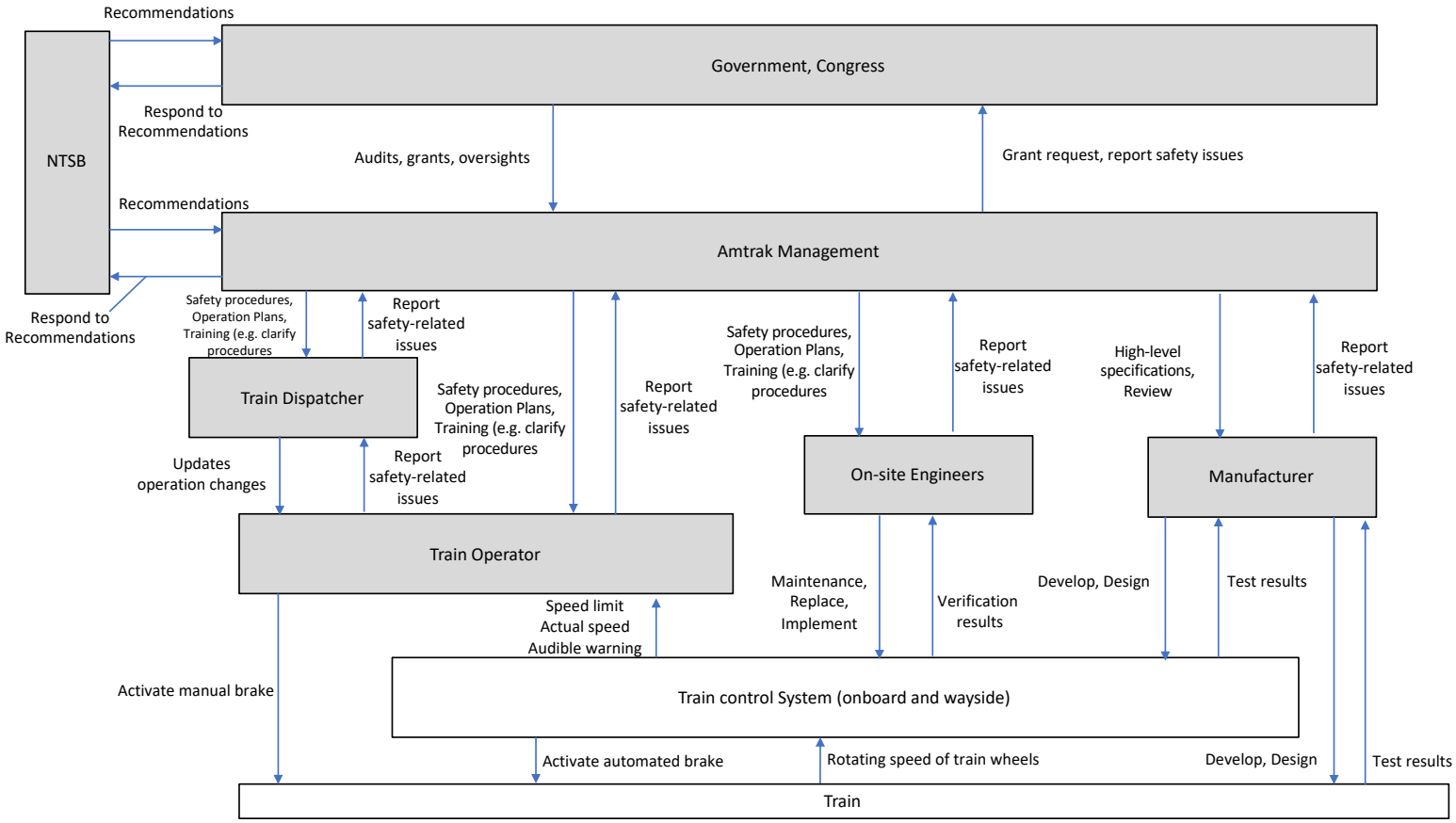


Figure 4- 14 Level 1 High-Level Safety Control Structure (Amtrak).

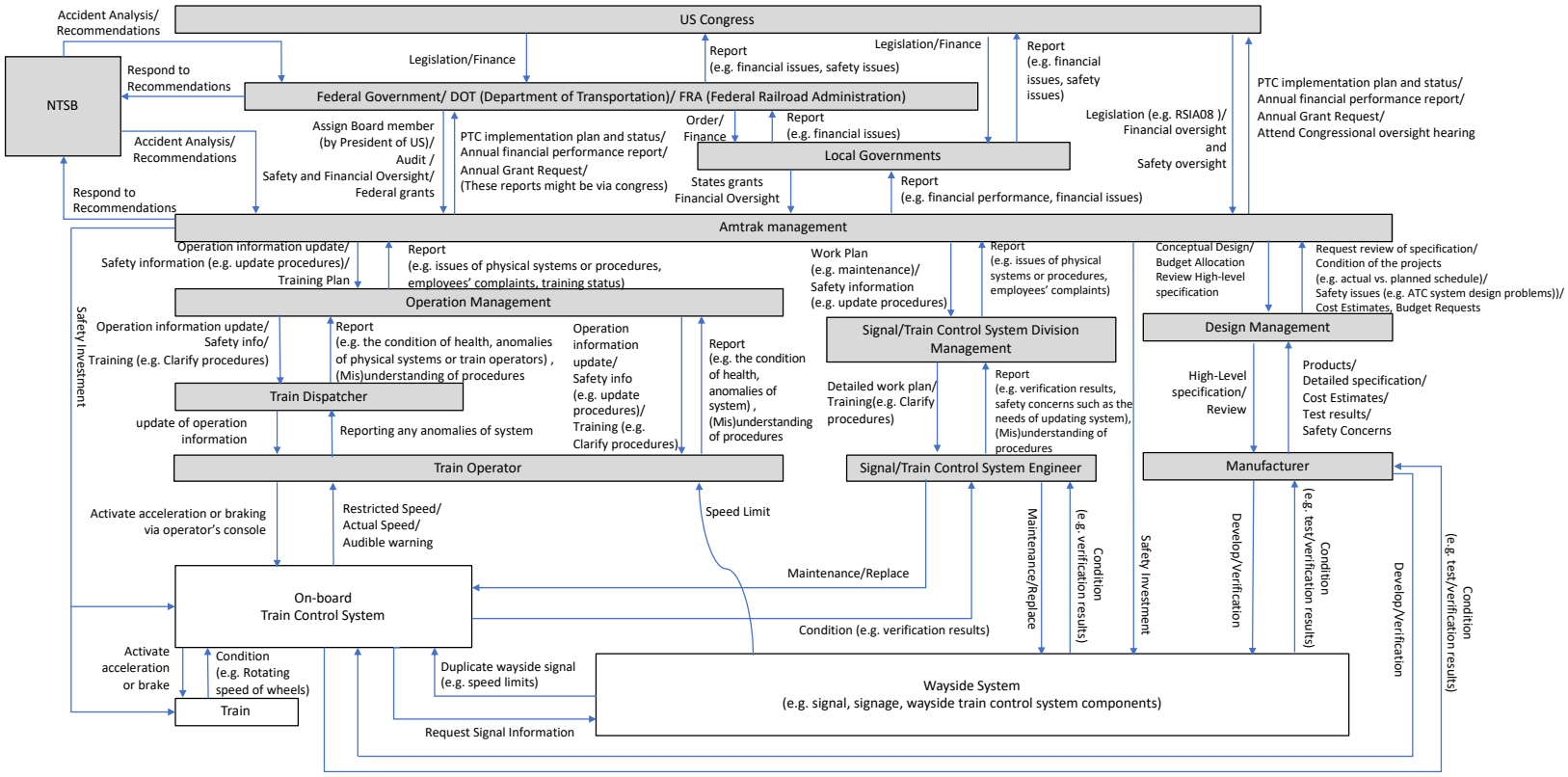


Figure 4- 15 Level 2 detailed Safety Control Structure (Amtrak).

Next, the safety-related roles and responsibilities of major components (controllers) relevant to the analysis are provided in Table 4-7.

Table 4- 7 Safety-Related Roles and Responsibilities (Amtrak)

US Congress
・Decide the budget allocation to Amtrak through DOT and FRA, ensuring the amount is adequate to ensure safe operation. ・Review federal grants requests and financial performance reports from Amtrak. ・Make sure the current law structure ensures safety of the transit operation. ・Monitor governmental and audit agencies and determine whether operators are following safety recommendations or safety-related regulations.
NTSB
Mission: "Making transportation safer by conducting independent accident investigations, advocating safety improvements, and deciding pilots' and mariners' certification appeals" [50]. ・Independently investigate significant accidents in a railroad, determining the probable cause and issuing safety recommendations so as to prevent future accidents [50].
Governmental Agencies
・Provide financial oversight and decide and secure budget allocation to Amtrak, ensuring the amount is adequate to ensure safe operation. - Review federal grants requests and financial performance reports - Inform congress by explaining the need for and the safety-related impact of grants (budget). ・Federal government must ensure FRA is carrying out its oversight responsibility and enforcing safe operations ・FRA must provide safety oversight to Amtrak and ensure safe operations by; - Conducting audits, providing recommendations, and requiring actions regarding inadequacies in Amtrak's current and planned system design and operation. - Make sure Amtrak is following recommendations and legislation.

- Review system implementation plans and make sure Amtrak's planned system would improve or maintain safety, and meet the legislative requirements.

・President of United States shall assign board members and make sure that they would improve or maintain safety and financial performance.

・FRA must receive and monitor recommendations by NTSB, and implement when necessary to ensure safe operations

Amtrak management

Ensure that rail operations are performed safely by achieving following requirements and constrains;

・Ensure that the budgets and investments for maintaining and improving safety of the system are adequate and appropriately distributed

- Make grants requests in order to receive necessary funding from government/congress.
- Ensure grants requests contain sufficient budget for maintaining safe operations.
- Improve financial performance so that the company can operate the system safely with the available budget
- Make a short-term and long-term investment plan so as to maintain and improve safety

・Follow and respond to safety-related regulations and recommendations from governmental agencies and NTSB.

・Make a company-wide safety policy and effective safety culture, characterized by an informed, reporting, and just culture.

- Collect feedback from employees about any safety-related problems, and provide feedback to upper-level controllers about safety-related issues.
- Provide safe procedures, operation plans, and incident reports
- Update operation changes and safety procedures as needed
- Ensure that the safety-related information (e.g. new procedures, incident reports) is circulated, understood, and acted upon effectively and properly.

- Create a safety training program and clarify understanding of each element including procedures. Periodically check the progress of training and effectiveness by getting feedback from front-line workers and their management.

・Make and retain good relationship with unions so that the front-line workers perform their duties in a safe manner.

・Make high-level work plans (e.g. maintenance, replacement, or installment), operation plans of trains, and conceptual design specifications for physical systems.

- Perform effective risk/hazard analysis
- Address and prevent hazards that will lead to accidents, including single point failures and other causes
- Redesign physical systems and organization if needed to ensure safety

・Coordinate all PTC implementation, including collaboration across interdisciplinary teams from all departments to meet the PTC legislation of 2008.

- Make sure that PTC will address appropriate hazards thorough risk/hazard analysis, interviewing front-line mechanics or its supervisors, manufactures, and any other effective methods

Design Management

Please note that this thesis assumes that this component is responsible for oversight of signaling, ATC, PTC, and locomotive design and development.

・Develop and review the detailed specifications using the expertise of manufactures, making sure that replacement or installation would improve or retain safety of the Train operation.

・Provide feedback to upper management about any safety-related concerns.

・Collect safety-related information from suppliers**.**

Signal and Train Control System Division Management

Please note that this thesis assumes both ATC-related and PTC (ACSES)-related planning and installing are their responsibilities.

- *It is also assumed that the more detailed design (specification) was carried out by manufacture under the oversight of Design Management.*

- *It is also assumed that this controller would make a blue print of PTC implementation plan, and it would be reviewed by Amtrak Management. After reviewed and acknowledged, the detailed design would be carried out by Design Management component.* ・Provide training sessions to make sure the engineers would perform their duties safely ・Collect safety-related concerns from engineers, and report those issues to upper-level management ・Provide safety-related information to engineers ・Provide planning and oversight of maintenance, installation, or replacement of ATC/PTC components to ensure safe operation. ・Get approval of Planning of maintenance, installation, or replacement of ATC/PTC components from upper-level management to ensure safe operation. ・Make provisional PTC implementation plan before the congressionally mandated deadline while making sure that the PTC system meets the legislative requirements
Operation Management
・Provide training sessions to make sure the human operators can perform their duties safely. ・Collect any safety-related concerns from lower-level operators, and report those concerns to upper-level management. ・Provide safety-related information, such as new operation procedures, to lower-level operators.
Manufacturer
Please note that this thesis assumes that this component contains manufactures of signaling, ATC, PTC, and locomotive. ・Make detailed specification and carry out verification -Ensure components can perform safely when equipped in Amtrak's system ・Provide safety-related information, such as maintenance procedures, to Amtrak
Signal and Train Control System's Engineer

・Plan and perform activities to ensure that the ATC and signal systems perform safely. These activities include installation, replacement, and maintenance of ATC and signal systems. ・Follow and understand the instructions provided by upper management and their supervisors. ・Collect and review up-to-date safety-related information ・Report any safety-related concerns to supervisors
Train Dispatcher
・Update the operation information, such as the needs of temporal speed restriction in certain area, to train operators via radio communication system ・Supervise train operators via radio communication system when they require operational decisions such as how to deal with emergency situations ・Provide feedback to the operation management if there are issues in the system
Train Operator
・Maintain distance from other trains by appropriately activating brake ・Monitor the conditions of the train (e.g. train speed, location), and react by activating manual brake so that the speed does not exceed the speed limit for a given area ・Monitor the radio broadcasting for operation-related information (e.g. emergency of other trains) ・Report any safety-related issues, such as the difficulties of safe operation due to system design issues, to upper-level managements
Wayside Signal and Signage
・Inform a train operator of a restricted speed so that the train does not violate the speed limit
ATC System
・Prevent a train from exceeding speed limits and train-to-train collisions by automatically activating brake at the proper timing and strength, if the train operator does not appropriately activate brake ・Notify a train operator of restricted speed limit and actual speed. ・Inform a train operator of current location and brake pattern to ensure that the train

would slow down appropriately by an operator's input.
ACSES(PTC) System
・Prevent a train from incursions into established zone limits (e.g. where temporary work is being execute.) ・Prevent a train from moving into a interlocking (switch) in the wrong position. *In addition to these two requirements, ACSES has same safety requirements and constraints of ATC System explained earlier.*

4.7 Proximal Event Chain Leading to the Loss

The proximal events are shown in following Table 4-8.

Table 4- 8 Proximal Event Chain (Amtrak)

Timeline (All May 12, 2015)	Events
1:20 p.m.	The Amtrak engineer, conductor, and an assistant conductor went on duty at New York's Pennsylvania Station
5:19 p.m.	They worked on a train, and arrived in Washington, DC
	(They went off duty for dinner)
6:30 p.m.	They went back on duty, and another assistant conductor, who had worked on an earlier train from New York, was added to train 188's crew.
7:15 p.m.	Train 188 departed Washington for New York
9:06 p.m.	Train 188 arrived at Philadelphia's 30th Street Station. The engineer inspected the locomotive pantograph, as required by Amtrak.
9:10 p.m.	The train left the 30th Street Station on time on main track 1
	The engineer, who was alone in the cab, maintained the train speed near the required 30 mph for the next few miles.
9:13 p.m.	Radio Broadcast between SEPTA train operator and the dispatcher started[40]. The Amtrak train operator was monitoring the radio, as this was the place he was approaching.

[40] During the 6-minute conversation, the SEPTA engineer said his windshield was shattered near the Diamond Street Bridge—an area where people were known to throw rocks and other objects at passing trains. The SEPTA engineer said he had glass in his face and had used the emergency brake to stop his train on main track 1. He requested medical attention.

	As the Amtrak engineer approached the Diamond Street Bridge, he crossed from main track 1 to main track 2 in preparation for passing the SEPTA train.
	He accelerated to 67 mph in compliance with the authorized speed and sounded the horn as he approached the SEPTA train, which was stopped to his right at MP 86.
	The Amtrak engineer broadcasted on the radio that he was about to pass the SEPTA train; he sounded the horn again as he passed in case the SEPTA crewmembers were on the ground inspecting the train for damage as required by operating rules.
	The Amtrak engineer continued to comply with authorized speeds, slowing to transit a right-hand curve that had a maximum speed of 65 mph.
9:19 p.m.	Radio Broadcast between SEPTA train operator and the dispatcher ended. At the time, the Amtrak train was at MP83.4, and the authorized speed increased to 80 mph; the Amtrak engineer moved the throttle to full power, and the train accelerated.
	The throttle stayed at full power for about 25 seconds. It had reached the 80 mph speed limit near MP 82.3, which was 1.2 miles from the point of derailment. At that point, the Amtrak engineer momentarily reduced the throttle, then returned to full throttle before reducing power about 20 seconds later.
	The train speed reached 106 mph as it entered the left-hand curve at Frankford Junction.
9:20 p.m.	The engineer began activating emergency brake
	Three seconds later, the train had slowed to 102 mph, and the event recorder and forward-facing video stopped recording.
About 9:21 p.m.	**The train derailed to the outside of the left-hand curve at MP 81.62.**

4.8 Analyzing the Physical Process

Next, the physical processes are analyzed. The main physical systems in this accident are a train, train control system, and some wayside system components. Their Safety responsibilities, Physical Controls, Failures and Inadequate Controls, and Contextual Factors are summarized in following Table 4-9.

Table 4- 9 Analysis of the Physical Process (Amtrak)

Safety responsibilities (what must it do)
SR1. Train must maintain safe distance from other trains **SR2.** (Violated) Train must not exceed the speed limits for a given area **SR3.** (Violated) Train must adequately protect occupants in the event of a crash **SR4.** (Violated) Train must allow passengers to safely egress after a crash
Physical Controls: Partial List (what design features were meant to fulfill the safety responsibilities)
PC1. Onboard train control system → SR1,2 - Cab signals - ATC system - PTC (ACSES) system (not operational in the accident area) PC2. **Cab signal change point (not implemented on the eastbound direction)** → SR2 PC3. Propulsion system PC4. Braking system → SR1,2 PC5. Radio Communicating system with dispatcher → SR1,2 PC6. Wayside signal, signage → SR1,2 PC7. Car Windows → SR3,4 PC8. Compartmentalization[41] →SR3

[41] This is explained in the NTSB accident report as follows: “Compartmentalization, although not required, has been one strategy to protect occupants in railroad accidents by restricting their movement and preventing them from being thrown from their seats in the car. In the preamble to its final rule promulgating the

Failures and inadequate controls (what went wrong)
Component Failures ・There was no component failures ***Inadequate Controls*** **IC1.** Train ran beyond the restricted speed at the steep curve. → PC4 **IC2.** Train Control System did not automatically activate brake ahead of the steep curve, allowed train to run beyond the restricted speed. → PC1 **IC3.** Some passengers were thrown out from the window (if passengers were secured within the train, some of them might not have been severely or fatally injured.) → PC7,8
Contextual Factors (why did those things go wrong)
C1. Cab signal change point, which enforces a certain speed cap, was not implemented in the eastbound trains at the curve. →IC1, 2 **C2.** PTC (ACSES) system was not operational yet →IC1, 2 **C3.** Train Operator did not activate manual brake ahead of the steep curve so as to maintain the train speed within the speed limit. →IC1 **C4.** Windows had two competing performances to be considered; containment capabilities (may inhibit passenger egress), and emergency egression (allow passengers to egress in crash) →IC3

Passenger Equipment Safety Standards currently codified at 49 CFR Part 238, the FRA noted that based on previous research, interior passenger protection requirements for Tier I and II passenger cars rely on compartmentalization as a passenger protection strategy" [34].

4.9 Analyzing the Higher Levels of the Safety Control Structure

In this section, components in the higher levels are analyzed in terms of: 1) Safety Requirements and Constraints; 2) Unsafe Control Actions (UCAs); 3) Mental Model Flaws; and 4) Context in which Decisions Made.

4.9.1 Signal and Train Control System Level

4.9.1.1 Analysis of Signal and Train Control System Level

Firstly, the components in Signal and Train Control System Level are examined. In the Safety Control Structure, these components are located at the bottom of the Structure as colored red in Figure 4-16 below.

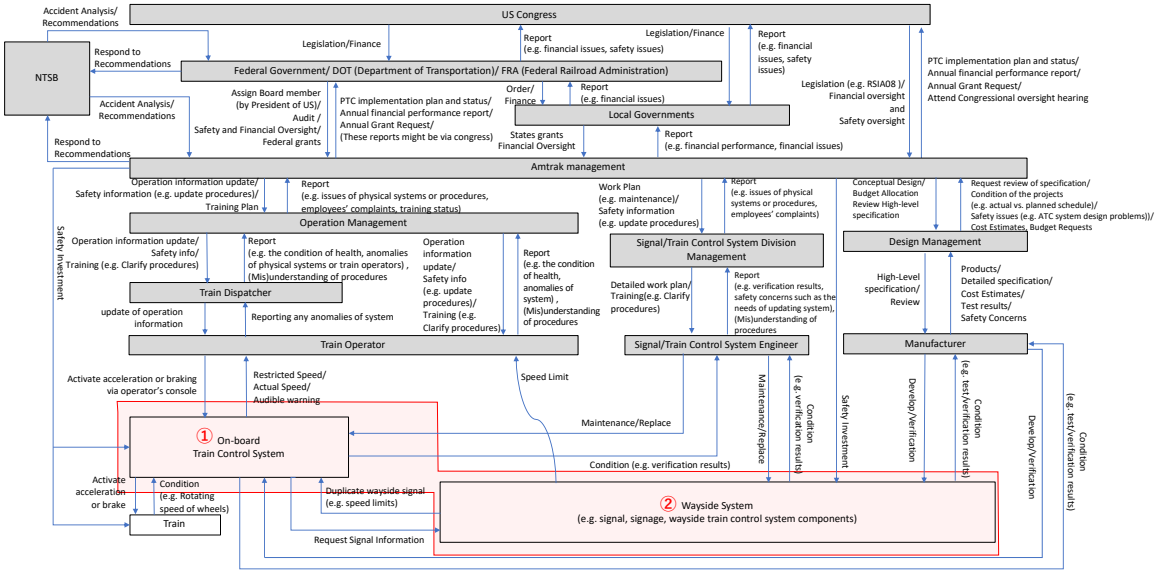


Figure 4- 16 Signal and Train Control System Level Safety Control Structure.

(2) Train Control Systems

First, Train control systems were examined. The analysis result is shown in Table 4-10 and Table 4-11.

First, take a look at Table 4-10. At the time of the accident, PTC system was still not activated yet, thus ATC system was supposed to be in charge of preventing overspeed situation. However, ATC did not accomplish its safety requirement of "automatically activating brake if human does not act properly (SR1)" and "notifying human operator of the need of braking (SR2)".

Why did ATC not do that? The reason is that the equipment, called cab signal change point, which activates ATC's automated braking function, was not implemented in the accident site. Therefore, the ATC acted as it designed, but it could not meet its safety requirements.

Then, why was the equipment not in place? The locations upon which cab signal change point was implemented were decided based on risk assessment of Amtrak, and Amtrak believed that this site did not have an overspeed risk and that the ATC-protection was not needed. The rationale for this decision-making was that the speed limit of the straight track ahead of the Frankfort junction curve was 80 mph, which is slower than the overturn speed of 98 mph, thus the management believed that the train would not enter the curve beyond this overturn speed. In the hindsight, this seems very unsafe decision, but why they decided this way? This will be further analyzed in the upper-controller level.

Table 4- 10 Analysis of ATC System

Safety Requirements and Constraints (What goals they should achieve)
SR1. (Violated but not designed to achieve this requirement) Prevent a train from exceeding speed limits and train-to-train collisions by automatically activating brake at the proper timing and strength, if the train operator does not appropriately activate brake **SR2.** (Violated but not designed to achieve this requirement) Notify a train operator of restricted speed limit and actual speed.

SR3. (Violated but not designed to achieve this requirement)
Inform a train operator of current location and brake pattern to ensure that the train would slow down appropriately by an operator's input.

Unsafe Decisions and Control Actions (What they did that was unsafe)

UCA1. ATC system did not prevent the train from exceeding the speed limit of 50mph before entering the curve by activating brake at appropriate timing and strength. →SR1
UCA2. ATC system did not notify a train operator that he needs to activate brake and the train would overspeed otherwise. → SR2
UCA3. ATC system did not present the current location, current and future speed limits, and required brake patterns to the train operator through train operator console. →SR3

Process Model Flaws (What did they believe about the system that explains their actions)

PMF1. Believed that the speed limitation was not 50 mph.

- Believed that it does not need to inform an eastbound train's operator of the need of braking →UCA2
- Believed that it does not need to override a human operator and automatically activate brake ahead of the steep curve for the eastbound trains. →UCA1

Context in which Decisions Made (What other factors - pressures, incentives, history, etc. - explain their actions)

C1. (Unsafe Managerial Decision)
A signal change point, a hardware which activates the speed restriction function, was not installed in the northbound track on the accident site, due to the managerial decision of "the trains would not violate the speed limit". According to the *fortune*, the hardware would have cost about only $40,000 [47]. There are no wayside signal and "signal change point," thus ATC system was not designed to enforce a speed limit on the curve. →MMF1

C2. (Unsafe Design)

From the information provided in an accident report, it is likely that there was no on-board display which tells a train operator the location of his/her train, and current and future speed limits, and brake pattern. → UCA3

C3. ACSES was not activated yet. →MMF1, UCA1,2,3

C4. The speed limit of the straight track ahead of the Frankfort junction curve was 80 mph, which is slower than the overturn speed of 98 mph, thus the management believed the train would not enter the curve beyond this overturn speed. This led the management to decide the risk of the overturn in the accident site was very low →C1

Another violated safety requirement was "informing the place of the train to train a train operator (SR3)." One member of the NTSB investigation team commented that:

> It is very disturbing that so much rests on the ability of an engineer, working alone for extended periods of time, to determine his or her location based not on clear visual markers, but on memory. The engineer must do this in many instances **without the assistance of GPS driven, two-dimensional map display and guidance** [34].

Why was this Safety Requirement not achieved? The reason is that Amtrak believed that kind of situational information is not needed. One question here is, why did Amtrak believe it is not necessary? This will be further analyzed in the upper-controller level.

Lastly, if PTC was implemented, SR1 and SR2 might be accomplished. Although the Amtrak's slow implementation of PTC was largely picked up as the contributing factor to the accident, it was understandable when considering Amtrak's situation. They had received no federal financial support when the legislation mandated railway operators to implement PTC by 2015 [51], [52], although one can assume it required substantial initial cost. Plus, there were other obstacles as well,

such as low readiness level of PTC technology [52], the need of interoperability [48], and difficulty in getting right for using wireless spectrum in 220 MHz range [53].

Table 4-11 examines the PTC system. PTC has the same responsibilities from SR1 to SR3, as well as SR4 and SR5. Many newspapers argued that the slow implementation of PTC was the main reason of the accident, as did the NTSB report.

Table 4- 11 Analysis of ACSES(PTC) System

Safety Requirements and Constraints
SR1. Prevent a train from exceeding speed limits and train-to-train collisions by automatically activating brake at the proper timing and strength, if the train operator does not appropriately activate brake **SR2.** Notify a train operator of restricted speed limit and actual speed. **SR3.** Inform a train operator of current location and brake pattern to ensure that the train would slow down appropriately by an operator's input. **SR4.** Prevent trains from incursions into established zone limits (e.g. where temporary work is being execute.) **SR5.** Prevent trains from moving into an interlocking (switch) from the wrong direction.
Unsafe Control Actions
(PTC was not operational at the time of the accident)
Mental Model Flaws
(PTC was not operational at the time of the accident)
Context in which Decisions Made
C1. PTC (ACSES) was not implemented yet when accident happened. It is reported that the biggest obstacles were cost [51] (no federal funds for PTC at least when it was first mandated in 2008 [52]), low readiness level of technology [52], need of interoperability [48], and difficulty in getting right for using wireless spectrum in 220 MHz range [53]. **C2.** PTC was only months away from being activated. **C3.** In the past and even after this accident, there were several cases where a train derailed or crashed as a result of overspeed in the place where PTC was not installed and

no other measures to slow down trains if it runs too fast. This includes 2017 Amtrak train Derailment at Dupont [54], 2008 Union Pacific Train crash at LA [55], and many others.

(3) Wayside System (Wayside Signal and Signage)

Second, wayside systems were examined. The analysis result is shown in Table 4-12. Compared to Train Controls Systems, not as much information was gathered. One can argue that there was no clear signage (i.e. speed-limit post) ahead of the curve. This is clearly stated in the accident report as "determine his or her location based not on clear visual markers[42]" [34]**.** Even if there was signage, it may not have been apparent at night. Thus, one can maintain that the train driver could not get information from outside speed-limit information. Why was there no such signage at the Frankfort Junction? This will be analyzed in the upper-controller level.

Table 4- 12 Analysis of the Wayside Signal and Signage

Safety Requirements and Constraints
SR1. (Violated but not designed to achieve this requirement) Inform a train operator of a restricted speed so that the train does not violate the speed limit
Unsafe Decisions
UD1. Wayside signal and signage did not communicate speed limit to train operator.
Process Model Flaws
N/A
Context in which Decisions Made
C1. From the information provided in the accident report, one can infer that there was no signage or no clear/effective signage which shows speed limit ahead of the curve. →UCA1 **C2.** Dark at night, difficult to see signs **C3.** No speed limit indication onboard, no persistent indication.

[42] This quotation is retrieved from the comments by one of the NTSB investigation members.

4.9.1.2 Unanswered Questions at Signal and Train Control System Level

At this level, following questions (UQ: Unanswered Question) were not fully answered (See Table 4-13), and these are analyzed in the higher controller level in later sections.

Table 4- 13 Unanswered Questions at Signal and Train Control System Level

UQ1. Why did Amtrak Management believe that it was reasonable not to fully eliminate single point failure hazard? (They believed that the train would not overspeed beyond the overturn speed at Frankford Junction curve.)
UQ2. Why didn't Amtrak equip the operator console with a visual aid which would assist a train operator to locate his/her train?
UQ3. Why there was no clear speed-limit signage at Frankford Junction curve?

4.9.2 Front-Line Human Controller Level

"We were able to determine that no track or train malfunction caused the accident. … however, it is impossible to say with certainty what happened inside that locomotive or what, in fact, caused the engineer to lose awareness to the extent that he failed to reduce the train's speed in time for the curve. It is very disturbing that so much rests on the ability of an engineer, working alone for extended periods of time, to determine his or her location based not on clear visual markers, but on memory. The engineer must do this in many instances without the assistance of GPS driven, two-dimensional map display and guidance. While memory training may prove to be of some benefit when studied in the future, the reality is that intervening events are likely. … The reality is that exactly what happened that night will never be known. What is obvious, however, is that something did cause the engineer to fail to properly control the speed of the train. There is no doubt that an alert, well trained, healthy operator is the most important safeguard in any mode of transportation, but humans are inherently fallible. Even with the best training, medical

screening, and hours of service prohibitions, anything from an undiagnosed medical condition to a poor night's sleep to some external stress can result in a temporary, partial or complete loss of awareness or even consciousness."

--- Earl F. Weener (NTSB investigation member) [34]

4.9.2.1 Analysis of Front-Line Controller Level

Next, the analysis was carried out on the human controller level. In the Safety Control Structure, these components are located at the upper level of physical systems, as colored red in Figure 4-17 below.

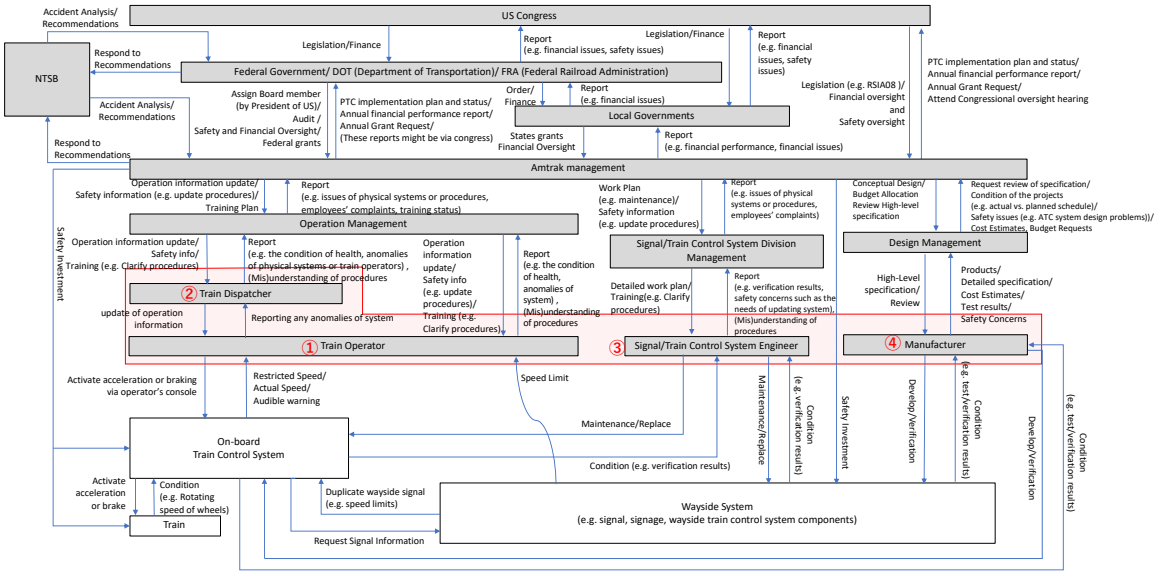


Figure 4- 17 Front-Line Controller Level Safety Control Structure.

(1) Train Operator

First, the train operator is examined. The analysis result is shown in Table 4-14.

The NTSB report argues the train operator directly caused a derailment due to his

inappropriate timing of braking. However, the rationale for his action is not fully understood even from NTSB official report[43]. The probable scenarios which might explain why he did not slow the train down should be discussed so that one can learn from his actions and why humans might not always act perfectly to operate these systems safely.

Why he did not slow down the train speed below 50 mph (UCA1)? This was a violation of SR4. This may be because: 1) he did not recognize where he was, and that the speed limitation was 50 mph (MMF3); or 2) he was on "autopilot" and performed his duty automatically without his attention.

For the first scenario, the competing information about the emergency situation involving other train is a compelling explanation (C2, C4). Few visible external cues were available about where he was and what the speed-limit was due to the darkness (C1), and the fact that there was similar curve which is followed by 110 mph straight track (C3) might have contributed to MMF3.

To some extent, it is understandable that he did not perform his task properly considering the competing information and the lack of safety aids to assist him in operating the train safely. One can conclude from this analysis that his Unsafe Control Actions are just symptoms of the unsafe control structure of Amtrak, as there were known options to supplement the human's memory limitations.

The other Unsafe Control Action which was identified is that none (or few) of the train operators who engaged in the eastbound train at the accident site possibly had not been reporting the safety-related problems, that is, no clear speed-limit signs and no active ATC protection (UCA2), or at least they were not able to persuade upper management to do so.

As was explained in the WMATA case, an organization with an effective safety culture has a reporting culture, and the UCA2 implies that Amtrak may have lacked this culture. The lack of Safety Culture within Amtrak is pointed out in the NTSB accident report for the other accident caused by Amtrak in 2016 [56], thus the argument that ineffective safety culture in which Amtrak prioritized other issues than safety contributed to the operator's UCAs seems reasonable. For the lack of safety culture in Amtrak, see the appendix B for detail.

[43] NTSB acknowledges the fact that "it is impossible to say with certainty what happened inside that locomotive or what, in fact, caused the engineer to lose awareness to the extent that he failed to reduce the train's speed in time for the curve.[34]" Thus, some of the scenarios in the NTSB report especially about the train operator are containing speculations to some extent.

Another question in the analysis is why Amtrak did not create an effective safety culture, which is supported by the fact that (1) it did not set up a visual aid to support engineers to locate themselves, (2) no clear speed-limit signage especially in the night, (3) no convincing actionable reporting of the unsafe condition, and (4) no activated Train Control System.

Table 4- 14 Analysis of the Train Operator

Safety Requirements and Constraints
SR1. Maintain distance from other trains by appropriately activating brake **SR2.** (Violated) Monitor conditions of the train (e.g. train speed, location). **SR3.** Communicate with the dispatcher if necessary to maintain safe operation **SR4.** (Violated) Recognize the speed limits and appropriately activate brake so that the train does not run over the speed limit. **SR5.** Listen to the radio broadcasting about operation-related information (e.g. emergency of other trains) **SR6.** (possibly violated) Report any safety-related issues to upper-level management
Unsafe Decisions and Control Actions
UCA1. The train operator did not slow down the train below 50 mph before entering the curve. →SR4 **UCA2.** (This is speculation due to lack of evidence) The previous train operators who engaged in this area (not only the person who operated the derailed train) possibly had not reported the safety-related issues, such as needs of clear indication of speed limit or active ATC protection. →SR6

Mental Model Flaws
Likely Scenario (Determined by NTSB)
MMF1. He believed that it was appropriate to increase train speed to 110 mph after transitioning the first curve → MMF3
MMF2. He believed that his train was on the 110 mph straight track, instead of 80 mph one (See Figure 4-3) → MMF1
MMF3. Believed that the speed limitation was not 50mph in the coming curve →UCA1, SR2,4 - Possibly did not know where his train was. → SR2
Another scenario (Not involving MMF)
Another1. He may have been operating on "autopilot" due to the nature of his task, with his behavior processed almost automatically without deliberate intention (skill-based behavior[44]). →UCA1
Context in which Decisions Made
C1. Operated at night, with fewer visible external cues, such as a bridge which served as a cue to start braking. One can infer that the outside speed sign may not be clearly visible to the train operator at night. →MMF2
C2. The curve before the approaching straight track (65 mph) was very similar to the curve after the derailment site (60mph) (See Figure 4-3). The first curve is followed by 80 mph straight, whereas the second one is followed by 110 mph straight track. →MMF2
C3. His attention was likely drawn to the emergency situation of other train, which was being broadcast via the radio communication system. This would have been competing

[44] "The skill-based behavior represents sensory-motor performance during acts or activities which, following a statement of an intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior" (Adapted from Rasmussen [57])

information. This may have caused him to forget about the impeding operation (i.e. slowing down the train) **C4.** "Studies have shown people are vulnerable to forgetting to resume interrupted tasks in a timely manner. When they do resume the interrupted task, they may struggle to mentally reconstruct the point at which they were interrupted, and they are vulnerable to increased errors" (NTSB 2016) → C3 **C5.** Lax safety culture with no clear reporting system. (See Appendix B for detail) →UCA2 **C6.** No evidence of fatigue, severe medical conditions, alcohol use or drugs. **C7.** Experienced, certified, and qualified to perform his duties. Had 5 years of experience in operating train.

(2) Train Dispatcher

Second, the train dispatcher was examined. The analysis result is shown in Table 4-15. No adequate information about the train dispatcher was provided, thus no UCAs were generated.

Table 4- 15 Analysis of the Train Dispatcher

Safety Requirements and Constraints
SR1. Update the operation information to train operators via radio communication system **SR2.** Supervise train operators via radio communication system when they require operational decisions such as how to deal with emergency situations

SR3. Report to the operation management if there are issues in the system
Unsafe Control Actions
Inadequate information to determine
Mental Model Flaws
Inadequate information to determine
Context in which Decisions Made
Inadequate information to determine

(3) Signal and Train Control System's Engineer

Third, the signal and train control system's engineer was examined. The analysis result is shown in Table 4-16.

Due to a lack of information, it can only be inferred that this controller may not have reported the system's issue, that is, the incapability of the ATC system to protect the overspeed situation at the curve to their supervisors (UCA1). This is based on the assumption that they were in charge of maintenance or other activities in which they had opportunities to look into the ATC components' implementation status. One can infer that as they are experts of the ATC components, they may have noticed the single point hazards, which could be eliminated by implementing $40,000-worth cab signal change point (C3).

Why would they not report this situation? It is possibly due to ineffective Safety Culture (C1) and Restricted Budget (C2). Why would their budget be restricted? Amtrak had been consistently operating at a loss as was discussed before (See Table 4-1). So, more precisely, the remaining question here is why Amtrak did not get enough budget so that front-line workers could properly evaluate and implement necessary safety features.

Table 4- 16 Analysis of the Signal and Train Control System's Engineer

Safety Requirements and Constraints
SR1. Implement, replace, and maintain ATC and signal systems, making sure these activities

ensure that the ATC and signal systems perform safely. **SR2.** Follow and understand the instructions and safety procedures provided by upper management and their supervisors. **SR3.** Monitor and understand new safety-related information as it becomes available **SR4.** (Possibly violated) Report to supervisors any safety-related concerns.
Unsafe Decisions and Control Actions
UCA1. (This is speculation due to lack of information) Possibly signal and train control system's engineer did not report ATC limitation that would allow trains run beyond restricted speed. →SR4 **UCA2**. Did not install PTC on train to prevent this type of accident →SR1
Mental Model Flaws
There is no adequate information
Context in which Decisions Made
C1. Lax safety culture with no clear reporting system (See Appendix B for detail). →UCA1 **C2.** Restricted budget →UCA1 **C3.** A signal change point was not installed in the northbound track on the accident site due to the risk analysis of Amtrak management. The hardware would have cost about only $40,000 [47]. Without this hardware, ATC system was not designed to enforce a speed limit on the curve. →UCA1 C4. The engineers were not directed to install PTC on the train, and Amtrak management had not approved PTC installation before this accident →UCA2

(4) Manufacturer

The analysis of the manufacturer is shown in Table 4-17. The manufacturer is responsible for creating a design that protects passengers in a crash, minimizing the possibility of passengers thrown out from the window, and allowing safe egress in event of an accident. However, there are competing goals to be considered, like assuring containment capabilities (may inhibit passenger egress after an accident), and emergency egression (allow passengers to egress after accident). Due to the limited information available, this thesis did not dive into detailed analysis concerning this aspect.

Table 4- 17 Analysis of the Manufacturer

Safety Requirements and Constraints
Please note that this thesis assumes that this component contains manufacturers of signaling, ATC, PTC, and locomotive. **SR1.** Provide detailed specification and carry out verification -Ensure their components can perform safely when equipped in the Amtrak's system **SR2.** Provide safety-related maintenance procedures to Amtrak **SR3.** Create a design that protects passengers in a crash, minimizing the possibility of passengers thrown out from the window, and allowing safe egress in event of an accident
Unsafe Control Actions
UCA1. Manufacturer designed the train with car windows that allowed passengers to be thrown out through the windows, and may not allow egress in a collision. → SR3
Mental Model Flaws
There is no adequate information
Context in which Decisions Made
C1. Windows had two competing performances to be considered; containment capabilities

(may inhibit passenger egress after an accident), and emergency egression (allow passengers to egress after accident) →UCA1

4.9.2.2 Unanswered Questions at Signal and Train Control System Level

At this level, following questions (UQ: Unanswered Question) were not fully answered (See Table 4-18), and these are analyzed in the higher controller level in later sections.

The questions UQ1,2, and 3 seem to be contributed by the Amtrak's weak safety culture to some extent, but these remain to be classified as "Unanswered" until the whole analysis would be finished at every level of safety control structure.

Table 4- 18 Unanswered Questions at Signal and Train Control System Level

UQ1. Why would Amtrak Management believe that it was reasonable not to fully eliminate single point hazards? (They believed that the train would not overspeed beyond the overturn speed at Frankford Junction curve.) →At least partially due to ineffective safety culture.
UQ2. Why did Amtrak not equip the operator console with a visual aid which would assist a train operator to locate his/her train?
UQ3. Why there was no clear speed-limit signage at Frankford Junction curve? →At least partially due to ineffective safety culture.
UQ4. Why Amtrak did not make an effective safety culture?
UQ5. Why did Amtrak not get enough budget so that front-line workers did not need to compromise on critical safety issues? →At least partially due to ineffective safety culture.

4.9.3 Amtrak Management Level

4.9.3.1 Analysis of Amtrak Management Level

Next, the analysis was carried out on the Amtrak management level. In the Safety Control Structure, these components are located at the middle of the hierarchy, as colored red in following Figure 4-18.

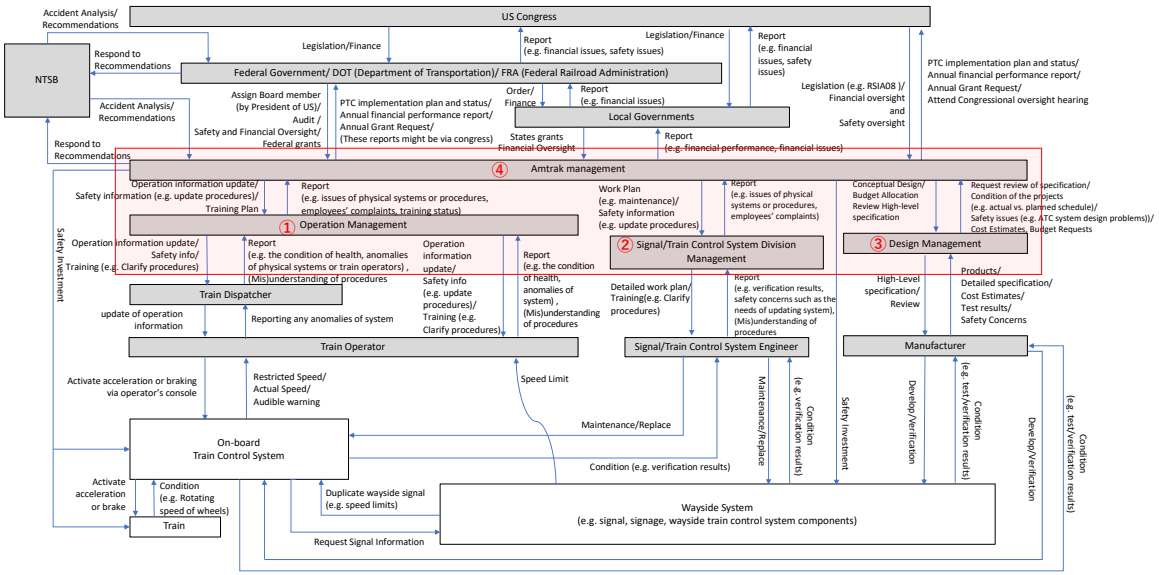


Figure 4- 18 Amtrak Management Level Safety Control Structure.

(1) Operation Management

The analysis of operation management is shown in Table 4-19.

Operation Managers may not have collected adequate feedback from their subordinates about safety-related concerns, but this is speculation due to lack of available information (UCA1). In order to assure safety, they need to not only educate, but also constantly update their mental models about what their subordinates think and find challenging by getting feedback about any safety-related

concerns. The lack of this reporting system seems to be the indicative of lax safety culture (C1).

Workers may also have been unwilling to report this information to their upper-management because of the restricted budget, which might have left Operation Managers with incomplete information and made it more difficult to convince Amtrak management to pay for redesigning. However, this is also speculation due to lack of available information.

Table 4- 19 Analysis of the Operation Management

Safety Requirements and Constraints
SR1. Provide training sessions to make sure human operators can perform their duties safely **SR2.** (Perhaps violated) Make sure to collect safety-related concerns from lower-level operators, and report those concerns to upper-level management - Create comfortable environment where their subordinates document and report safety concerns with no fear. **SR3.** Provide safety-related information to lower-level operators, such as new operation procedures.
Unsafe Control Actions
UCA1. (This is a speculation due to lack of available information) Possibly the operation management may not have created a comfortable environment for dispatchers and train operators where they can document and report safety-related issues without fear, so as to document and collect important safety concerns from their subordinates. In this case, the need for a clear indication of speed limit and current location, or active ATC protection, may not have been reported. →SR2
Mental Model Flaws
There is no adequate information
Context in which Decisions Made

C1. Lax safety culture with no clear reporting system. (See Appendix B for detail) →UCA1 **C2.** Restricted budget (See Table 4-1 for detail). →UCA1

(2) Signal and Train Control System Division Management

The signal and train control system division management is analyzed in Table 4-20. This group is in charge of supervising ATC/PTC maintenance and installation engineers. The reasons why they did not get safety-concerns about no ATC protected track (UCA1) would be at least partially due to ineffective safety culture (C1) and budget restriction (C2). Due to ineffective reporting culture, probably no convincing feedback was made and the management did not believe that the signal change point was needed on the accident site, or/and managers were just unwilling to implement the signal change point for some reasons. Also due to insufficient budget, one can infer that there could have been a mentality which would have made them believe that their claims would be ignored due to inadequate budget for installing the equipment.

Although not directly contributing to this accident, it is notable that the planned PTC implementation is not fully capable of eliminating train-to-train collision, as explained earlier [35]. That is, aside from ahead of interlockings (switches), PTC would not automatically stop trains at the stop signal. Therefore, one can argue that this controller did not eliminate single point hazards, and this could be treated as a UCA (UCA3). In a similar fashion with UCA1, UCA3 was applied at least partially due to ineffective safety culture and budget restriction.

Table 4- 20 Analysis of the Signal and Train Control System Division Management

Safety Requirements and Constraints
Please note that this thesis assumes both ATC-related and PTC (ACSES)-related planning and installing are within scope for this controller. Designing ATC and PTC are not their responsibilities, but Design Management's. - *It is also assumed that the more detailed design (specification) was carried out by manufacture through "Design Management" component.*

- *It is also assumed that this controller would make a blue print of PTC implementation plan, and it would be reviewed by Amtrak Management. After reviewed and acknowledged, the detailed design would be carried out by Design Management component.*

SR1. Provide training sessions to make sure the engineers can perform their duties safely

SR2. (perhaps violated)
Make sure to get any safety-related concerns from engineers, and report those issues to upper-level management

- Create comfortable environment where subordinates can report safety concerns with no fear.

SR3. Provide safety-related information to engineers, such as new maintenance procedures.

SR4. (Violated)
Plan necessary maintenance, installation, or replacement of ATC/PTC components to ensure safe operation. Oversee maintenance, installation, and replacement of ATC/PTC components

SR5. (Violated)
Request, and get approval of Planning of maintenance, installing, or replacement of ATC/PTC components from upper-level management to ensure safe operation of the system.

SR6. Make provisional PTC implementation plan before the congressionally mandated deadline while making sure that the PTC system meets the legislative requirements

Unsafe Decisions and Control Actions

UCA1. (This is speculation due to lack of available information)
The signal and train control system division management may not have created a comfortable environment in which mechanics who were engaged in this area could report

safety issues with no fear, such as the limitations of the system that can allow trains to run beyond restricted speed. →SR2 **UCA2.** The signal and train control system division management did not plan to implement and activate ACSES before accident happened. →SR4 **UCA3.** The signal and train control system division management did not create PTC implementation plan which would address single point hazards. That is, the resulting PTC system would not stop trains automatically even if it were installed before this accident [35].→SR4
Mental Model Flaws
There is no adequate information
Context in which Decisions Made
C1. Lax safety culture with no clear reporting system. (See Appendix B for detail) →UCA1,2,4, C3 **C2.** Restricted budget (See Table 4-1 for detail). →UCA1, 3 **C3.** Whether a signal change point was implemented was based on risk analysis, but the risk analysis did not portray a clear need of ATC protection in the region of the accident. **C4.** There were many obstacles to implement PTC, including cost (no federal funds for PTC at least when it was first mandated in 2008), low readiness level of technology, need of interoperability, and difficulty in getting right for wireless spectrum in 220 MHz range. →UCA2

(3) Design Management

The analysis of Design Management is shown in Table 4-21. This thesis assumes that the

design managers are in charge of making high-level design for the physical systems, and the oversight of manufactures' detailed designs and verifications[45].

One can argue that they did not redesign the system to be capable of operating safely. That is, (1) they did not change the human-machine interface (i.e. locomotive's operator console) to be equipped with the visual aids (UCA2), (2) they did not (re)design the ATC system such that it automatically activates brake when a train exceeds the speed limits (UCA3), and (3) they did not design PTC capable of automatically stopping trains ahead of all stop signals (UCA4). They could do these either in their first design, or after the system's operation started. In the latter case, after operation starts, they could directly interview the users and constantly update their mental model about design improvement potentials. In order to assure safety, it is important to periodically check and learn from the current system's performance and fed that information into the next design cycles. From information gathered, the design processes used are unknown. If they did include this iterative design policy, it would boost the efficiency of the design process and maintain the safety of the operation.

Table 4- 21 Analysis of the Design Management

Safety Requirements and Constraints
Please note that this thesis assumes that this component is responsible for oversight of signaling, ATC, PTC, and locomotive design and development.
SR1. Oversee and review the detailed specifications using the expertise of manufacturers, making sure that replacement or installation would improve or retain safety of the Train operation.
SR2. (Violated)

[45] It is assumed that the PTC implementation plan was (1) first, planned by Signal and Train Control System Division Management, (2) then, reviewed and approved by Amtrak management, (3) then, Design Management would make high-level specifications for the PTC system, and (4) passed to and designed in detail by Manufactures, which would then be reviewed and approved by Amtrak. This whole iterative process was led by "Senior Manager PTC [35]," who is assumed to be contained in Amtrak Management component in this thesis. This thesis assumes other system's implementation would also be processed in a similar way.

Report any safety-related problems to upper management **SR3.** Ensure suppliers provide necessary safety-related information, including hazard analysis results, proper maintenance procedures, etc. Provide comfortable environment where the suppliers can report safety concerns with no fear.
Unsafe Decisions and Control Actions
UCA1. The design management approved a design that provided insufficient protection to allow passenger egress after an accident and to prevent passengers from being thrown out of windows in an accident. **UCA2.** The design management did not report and re-design the train operator's console to be equipped with the visual aids which notify an operator of important information such as current location, current and future speed limits, and brake pattern. →SR1, 2 **UCA3.** Did not redesign the ATC system such that it is capable of automatically braking when train runs beyond the speed limit. One possible solution was to implement the cab signal change point, for example **UCA4.** The design management did not recognize or report to company management that PTC should be designed in a way that would eliminate critical collision hazards like stopping trains ahead of stop signals (except ahead of the interlockings). →SR2 They did not equip PTC with that feature. →SR1
Mental Model Flaws
There is no adequate information
Context in which Decisions Made
C1. Windows had two competing performances to be considered; containment capabilities (may inhibit passenger egress), and emergency egression (allow passengers to egress)

→UCA1

C2. Lax safety culture with no clear reporting system. (See Appendix B for detail) →UCA2

C3. Restricted budget (See Table 4-1 for detail). →UCA2

(4) Amtrak Management

The analysis of Amtrak Management is shown in Table 4-22.

Amtrak was prone to political influence because its board members are assigned by the president of the United States, and it has been receiving federal grants. Possibly because of this, Amtrak has not been securing enough budget for maintenance and safety investment. In fact, Amtrak argues that "investments in the NEC has lagged, resulting in a gradual deterioration in the condition of the infrastructure. Today, the NEC Commission estimates that this backlog has reached $38 billion" [41]. The investment in safety should be prioritized as a train-operating authority, but Amtrak had not been able to get strong monetary support from government.

Also, Amtrak had been operating non-profit-generating routes, and its revenue per assets was only a half of Japan Railway companies' average (See Table 4-23). The difference between two railway authorities is the degree of governmental interference. Amtrak needs the substantial financial and managerial inputs from government, thus it can not decide upon strategies on their own. For example, it would be very difficult to eliminate non-profit-generating routes due to strong governmental interference.

The other remarkable information provided in Table 4-23 is that the number of derailments was 7 times more than Japanese Railway companies. Even considering the difference in the total track length in which Amtrak has 1.7 times longer track distance[46], this indicates the severity of Amtrak's safety degradation.

[46] Amtrak has 34,000km[58], whereas Japan Railway has 21,000km[59]

Table 4- 22 Analysis of the Amtrak Management

Safety Requirements and Constraints
Making sure that the rail operations are performed safely by achieving following requirements and constrains: **SR1.** (Violated)   Make sure that the budgets and investments for maintaining and improving safety of the system are enough and appropriately distributed   - Make grants requests in order to get enough funds from government/congress.   - Make sure grants requests contain sufficient budget for maintaining safe operations.   - Manage financial performance so that the company can operate the system safely even without governmental supports   - Maintain a short-term and long-term investment plan so as to maintain and improve safety   **SR2.** Follow safety-related regulations and recommendations from governmental agencies and NTSB.   **SR3.** (Violated)   Create a company-wide safety policy and effective safety culture, which may include components like an informed, reporting, and just culture.   - Collect feedback from employees about any safety-related problems, and provide feedback to upper-level controllers about safety-related issues.   - Provide safety procedures, incident reports, or operation plans.   - Update operation changes and safety procedures.   - Make sure that the safety-related information (e.g. new procedures, incident reports) are circulated, understood, and acted upon effectively and properly.   - Make a safety training program and ensure that procedures are understood. Periodically check the progress of training and effectiveness by collecting feedback from front-line workers and their management.

SR4. (Violated)

Cultivate and retain good relationship with unions so that the front-line workers can perform their duties in a safe manner.

SR5. (Violated)

Make high-level work plans (e.g. maintenance, replacement, or installation), operation plans of trains, conceptual design specifications for physical systems.

- Performing effective risk/hazard analysis
- Ensure that critical hazards that will lead to accidents are addressed
- Ensure there are no single point hazards within the system
- Redesign physical system and organization as needed to ensure safety

SR6. (Violated)

(Senior Manager PTC was) responsible for coordination of all PTC implementation, including collaboration across interdisciplinary teams from all departments, to meet the PTC legislation of 2008.

Ensure that PTC will eliminate critical hazards thorough risk/hazard analysis, interviewing front-line mechanics or its supervisors, manufactures, and any other effective methods

Unsafe Control Actions

UCA1. Amtrak management did not improve its financial condition, securing enough budget for improving and retaining safety. →SR1

- Some potential options include: closing the lines which are not used by many passengers, or increasing fares. These business decisions are essential for maintaining enough budget for safety expenses. Except for NEC, both state-supported and Long-distance are not profitable. 67% of state-supported and 100% of Long-distance are generating negative earnings in FY2017 [60].

UCA2. Amtrak management did not create an effective Safety Culture (See Appendix B for detail) →SR3

UCA3. Amtrak management did not maintain good relationship with unions so as to make sure that work is performed safely (See Appendix B for detail). →SR4

UCA4. Amtrak management did not make sure that all hazards of single point failures were eliminated even before PTC was fully implemented. That is, the accident site was not equipped with a cab signal change point, which would activate ATC function of automatically activating brake. →SR5

- May not have collected feedback about unsafe conditions from front-line workers through their management →SR3

UCA5. Amtrak management did not ensure the design has sufficient protection against passengers being thrown out of windows in an accident, and did not ensure the design allows passengers to egress after an accident. →SR5

UCA6. Amtrak management did not implement and activate fully-functioned PTC in time to prevent this accident.

UCA7. Amtrak management did not decide to re-design the train operator's console to be equipped with the visual aids which notify an operator of important information such as current location, speed limits, or brake pattern. →SR5

Mental Models

MMF1. Believed that the accident site was low-risk of overspeed. → UCA4

- They may have believed that the safety-assuring equipment (i.e. cab signal change point) is not worth the cost
- The cost for the equipment is reportedly only $ 40,000.

MMF2. May have believed that implementing PTC is a more pressing matter and therefore the existing ATC system does not need to be analyzed to ensure safe operation until PTC is fully operated. → UCA4

MMF3. May have believed that the train operators had enough visual cues outside at night, and the train operator's console needs not to be equipped with the visual aids which notify an operator of important information such as current location, speed limits, or brake pattern. →UCA6, 7

Context in which Decisions Made

C1. They had been experiencing continuous financial losses and difficulty getting governmental grants →C2, UCA1,2,7

- One can infer that it would be very difficult to increase the federal funds. In fact, the federal funds have been relatively constant and have very little variability (See Table 4-1).

C2. Affected by politics and governmental decisions (See section "4.2.2 Financing System and Board Members"). →MMF2, UCA1,2

C3. Ineffective or inadequate safety culture (See Appendix B for detail).
→MMF1,2, UCA1,2,3,4,7

C4. There were many obstacles to implement PTC, including cost (no federal funds for PTC at least when it was first mandated in 2008), low readiness level of technology, need of interoperability, and difficulty in getting right for wireless spectrum in 220 MHz range. →UCA6

- Some part of infrastructure is owned or operated by other organizations. This forces Amtrak to put extra effort into collaborations in order to ensure the interoperability of systems, such as train control system.

C5. The train windows had two competing performances to be considered; containment capabilities (may inhibit passenger egress), and emergency egression (allow passengers to egress)→UCA5

Table 4- 23 Comparison of Maintenance Expenditure and Capital Investment between Amtrak and Japan Railway in FY2017[47] (Data sources: [61], [62], [63], [64]).

(Units: million) *(Exchange rate: 110.87Japanese yen/$@ Feb 20th, 2019)*	**Amtrak FY2017**	**Japan Railway FY2017**
1. Railroad Assets	$13,349	$98,879
2. Passenger related revenues	$2,544	$43,094
3. Total capital investment on railroad assets	$1,586	$9,481
4. Maintenance and Repair Expenses	$453	$5,840
5. =3+4	$2,039	$15,321
2/1 Revenue/Assets	19%	44%
3/1 Investment/Assets	12%	10%
3/2 Investment/Revenue	62%	22%
4/1 Maintenance/Assets	3%	6%
5/1	15%	15%
# of derailment /year	22.00	3.00
- High Speed Rail derailment / year	No info	0.00

4.9.3.2 Unanswered Questions at Amtrak Management Level

At this level, previously Unanswered Questions were answered from the information and analysis provided so far (See Table 4-24). In the next section, these questions are again tested and verified through the analysis in the higher controller level.

[47] Railroad Assets→Amtrak: "Total property and equipment, net"/ JR: "Tetsudo-Jigyou Kotei Shisan", Total capital investment on railroad assets→Amtrak: "Purchases and refurbishments of property and equipment"/JR:"Tetsudo-Jigyou Setsubi Toushi", Maintenance and Repair Expenses→Amtrak: "Expenses: Train operations" + "Expense: Materials"/JR: "Shisetsu, Sharyou no syuzenhi (Maintenance expenditure for Facilities and Vehicles)"

Table 4- 24 Unanswered Questions at Signal and Train Control System Level

UQ1. Why Amtrak Management believed that it was reasonable not to fully eliminate single point hazards? (They believed that the train would never overspeed beyond the overturn speed at Frankford Junction curve.) →At least partially due to ineffective safety culture. →At least partially due to insufficient budget. Increasing the budget was tough because of the prone-to-politics nature of the company. One can infer that it would be a difficult decision for congress/government to change the budget accordingly, with the Amtrak's request, as it would mean the other sectors' budget would be affected and decreased.
UQ2. Why did Amtrak not equip the operator console with a visual aid which would assist a train operator to locate his/her train? →At least partially due to ineffective safety culture. Possibly no official reporting system for the design problems. →At least partially due to insufficient budget.
UQ3. Why was there no clear speed-limit signage at Frankford Junction curve? →At least partially due to ineffective safety culture. Possibly no official reporting system for the design problems.
UQ4. Why did Amtrak not make an effective safety culture? →At least partially because the absence of political initiative. The author believes that without effective government or other initiatives with enough funding, it will be difficult to cultivate effective safety culture. Maintaining safety requires adequate amount of money, and without it, the difficult compromises will be inevitable. This can lead to a spiral of deterioration of safety and safety culture over time.
UQ5. Why did Amtrak not get enough budget so that front-line workers did not need to compromise safety? →At least partially due to ineffective safety culture.

4.9.4 Governmental and Audit Organizations Level

4.9.4.1 Analysis of Governmental and Audit Organizations Level

Next, the analysis was carried out on the governmental and audit organizations' level. In the Safety Control Structure, these components are located at the top of the hierarchy, as colored red in following Figure 4-19.

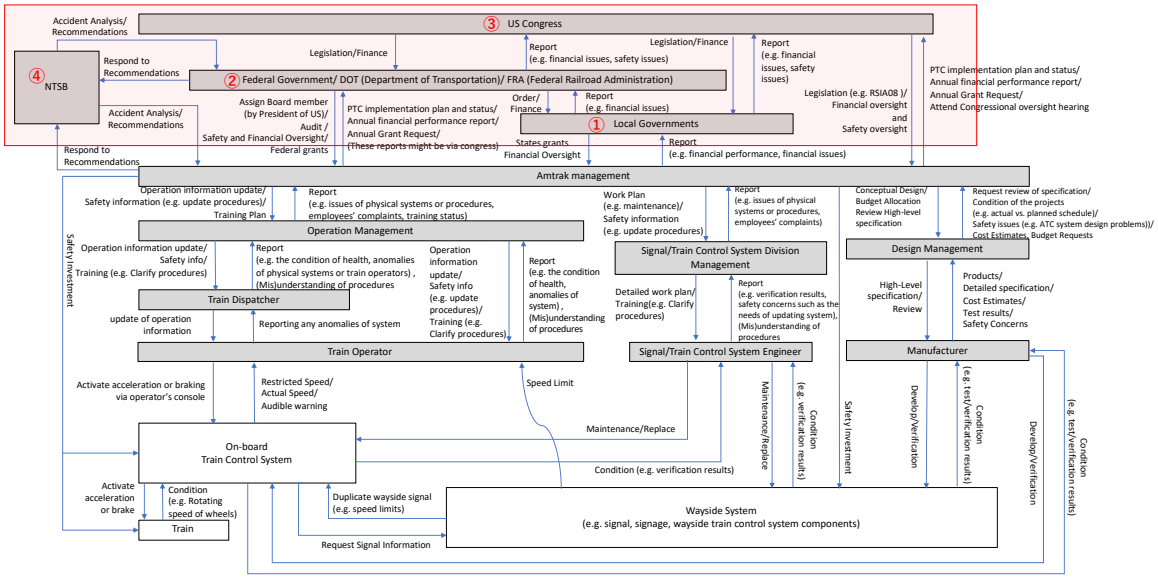


Figure 4- 19 Governmental and Audit Organizations Level Safety Control Structure.

(1) Local Governments

Firstly, the local governments were examined. The analysis results are shown in Table 4-25. There is no adequate information about how Local Governments are involved with NEC operation and how they were related to this accident, thus no UCAs were generated.

Table 4- 25 Analysis of the Local Governments

Safety Requirements and Constraints
SR1. Provide state grants to Amtrak and get financial performance reporting.
Unsafe Control Actions
There is no adequate information
Mental Model Flaws
There is no adequate information
Context in which Decisions Made
There is no adequate information

(2) Federal Governments, DOT, and FRA

Secondly, the Federal governments (including DOT and FRA) were examined. The analysis results are shown in Table 4-26.

An important point to be noted here is the question of "was PTC the best and only answer?" There were several sources that argued that if PTC was implemented, the overspeed could have been avoided. However, one could maintain that there were also other measures to avoid that situation.

In Amtrak's case, it could implement a cab signal point, which would have activated the ATC speed protection capability. If the government's initiative and emphasis was broader than simply enabling PTC, like enabling more "solution-neutral" legislation and requiring railroad companies to carry out hazard analysis and eliminating single point hazards, then the accident might not have occurred.

Table 4- 26 Analysis of Federal Government/DOT/FRA

Safety Requirements and Constraints
SR1. (Violated) Provide financial oversight, deciding upon and securing budget allocation to Amtrak, with sufficient allocations so as to ensure safe operation. - Review federal grants requests and financial performance reports

- May need to persuade congress by providing compelling reasons for the amount of grants (budget).

SR2. Federal government shall make sure FRA is carrying out its oversight responsibility of ensuring a safe operation

SR3. (Violated)
FRA shall provide safety oversight to Amtrak and ensure safe operation by;
- Conducting audits and provide feedback and recommendation regarding any concerns about Amtrak's current and planned system design and operation.
- Ensuring Amtrak is following recommendations and legislations.
- Reviewing system implementation plans and make sure Amtrak's planned system will improve or maintain safety and meet the legislative requirements.

SR4. President of United States shall assign board members and make sure that they would improve or maintain safety and financial performance.

SR5. FRA would need to follow recommendations by NTSB.

Unsafe Control Actions

UCA1. Federal government did not secure enough budget for Amtrak →SR1

UCA2. FRA did not make sure that Amtrak's risk analysis was reasonable and would eliminate hazards of single point failures. →SR3

UCA3. FRA may have put too much pressure on PTC implementation, without adequate oversight over Amtrak's risk analysis concerning present system design. →SR3

Mental Models

MMF1. Possibly believed there are more important matters which need to be addressed other than railway system →UCA1

MMF2. Possibly believed that PTC is the best and fastest way to assure safe operation →UCA2, 3
Context in which Decisions Made
C1. Prone to politics, and having many different stakeholders (e.g. Lobby group) →MMF1

(3) Congress

The analysis results for Congress are shown in Table 4-27. Their safety requirements and UCAs are similar to those of other government entities.

Table 4- 27 Analysis of Congress

Safety Requirements and Constraints
SR1. (Violated) Decide upon budget allocation to Amtrak through DOT and FRA, the amount of which is enough to ensure the safe operation. - Reviewing federal grants requests and financial performance reports **SR2.** (Possibly Violated) Make sure the current law structure would ensure the safety of the transit operation. **SR3.** Get feedback from governmental and audit agencies and being familiar with whether operators are following safety recommendations or safety-related regulations.
Unsafe Control Actions
UCA1. Congress did not pass the bills to increase budget for Amtrak →SR1 **UCA2.** Congress may have put too much pressure on PTC implementation →SR2
Mental Models
MMF1. Possibly believed there are more important matters which they need to take care of than railway system →UCA1

MMF2. Possibly believed that PTC is the best and fastest way to assure the safe operation →UCA2
Context in which Decisions Made
C1. Prone to politics, and having lots of stakeholders (e.g. Lobby group) →MMF1

(4) NTSB

The analysis results for NTSB are shown in Table 4-28. As was discussed in (2), one can argue that PTC was advertised too much. NTSB has been recommending and advocating PTC implementation for over 40 years in order to "prevent collisions and overspeed events."

As their recommendations are not only on the operators, but also on regulators (i.e. FRA), their technical recommendations have strong impact on governmental decisions.

Table 4- 28 Analysis of NTSB

Safety Requirements and Constraints
Mission: "Making transportation safer by conducting independent accident investigations, advocating safety improvements, and deciding pilots' and mariners' certification appeals." [50] **SR1.** Independently investigate significant accidents in transportation (including railroads), determine the probable cause, and issue safety recommendations so as to prevent future accidents [50].
Unsafe Control Actions
UCA1. NTSB may have pushed too much for implementing PTC. They did not recommend Amtrak to eliminate single point failures in previous accident recommendations, for example.
Mental Model Flaws

MMF1. They possibly believed that PTC was the best and only way to assure safe operation.
Context in which Decisions Made
There is no adequate information

4.9.4.2 Unanswered Questions below Governmental and Audit Organizations Level

At this level, previously Unanswered Questions were all answered from the information and analysis provided so far (See Table 4-29).

Table 4- 29 Unanswered Questions at Signal and Train Control System Level

UQ1. Why Amtrak Management believed that it was reasonable not to fully eliminate single point hazards? (They believed that the train would never overspeed beyond the overturn speed at Frankford Junction curve.) →At least partially due to ineffective safety culture. →At least partially due to insufficient budget. Increasing the budget was tough because of the prone-to-politics nature of the company. One can infer that it would be a difficult decision for congress/government to change the budget accordingly, with the Amtrak's request, as it would mean the other sectors' budget would be affected and decreased. →At least partially due to audit and governmental authorities' solution-central recommendations
UQ2. Why did Amtrak not equip the operator console with a visual aid which would assist a train operator to locate his/her train? →At least partially due to ineffective safety culture. Possibly no official reporting system for the design problems. →At least partially due to insufficient budget. →At least partially due to audit and governmental authorities' solution-central

recommendations
UQ3. Why was there no clear speed-limit signage at Frankford Junction curve? →At least partially due to ineffective safety culture. Possibly no official reporting system for the design problems. →At least partially due to audit and governmental authorities' solution-central recommendations
UQ4. Why did Amtrak not make an effective safety culture? →At least partially because the absence of political initiative. - The author believes that without effective government or other initiatives with enough funding, it will be difficult to cultivate effective safety culture. Maintaining safety requires adequate amount of money, and without it, the difficult compromises will be inevitable. This can lead to a spiral of deterioration of safety and safety culture over time. →At least partially due to audit and governmental authorities' solution-central recommendations
UQ5. Why did Amtrak not get enough budget so that front-line workers did not need to compromise safety? →At least partially due to ineffective safety culture. →At least partially because budget was dependent upon political decisions

4.10 Examining how Coordination and communication contributed the Loss

As was the case with the WMATA, the Amtrak also may have lacked an effective reporting culture with the official reporting system about safety issues such as problematic system designs.

The train control system was only partially automatic, that is, there were some places where ATC was not activated. This means that the train operators are required to remember the model of the ATC system, that is, in which curve it is activated or not. This has the potential for confusion about computer's mode. The operator might have been dependent on the computer, as the computer would brake automatically even when the human operator does nothing. But this could not have

applied to every location because it was only applied partially. Thus, human operators might have been used to doing nothing as they believed computers would aid them, and this may have been true most of the time. This mental model is “unsafe” for the partially automated system.

4.11 Dynamics and Migration to a High-Risk State

In this section, the dynamics and migration of the System’s State over time into an unsafe condition is discussed.

4.11.1 Declining public utilization of railroad and government interest

Figure 4-20 shows the transition of commuting modal shares from 1970 to 2016 in the US. This graph shows the share of the railroad transit has decreased especially until 1990, due to the increase of the automobile commuters’ share.

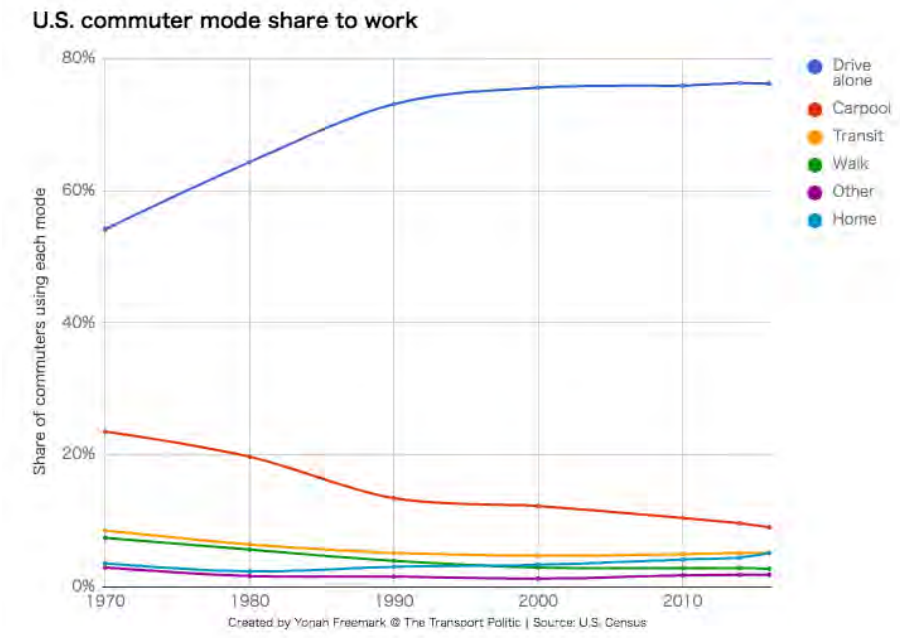


Figure 4- 20 US commuter modes’ transition from 1970 to 2016.

(Adapted from The Transport Politic [65])

Figure 4-21 shows the comparison of passenger modal share in US (left) and in Japan (right). Note that this includes not only commuters, thus the percentage does not consistent with Figure 4-20. This indicates that the people in the US are not using passenger rail services much (below 1%) compared to Japanese people, where railway system is well-recognized as "safe" system and many people use it both in commute and leisure.

As US is the democratic country, one can infer that the priority of railroad investment by government would be not so high compared to that of highways. The less people use railroad, the less attention it would get by the government.

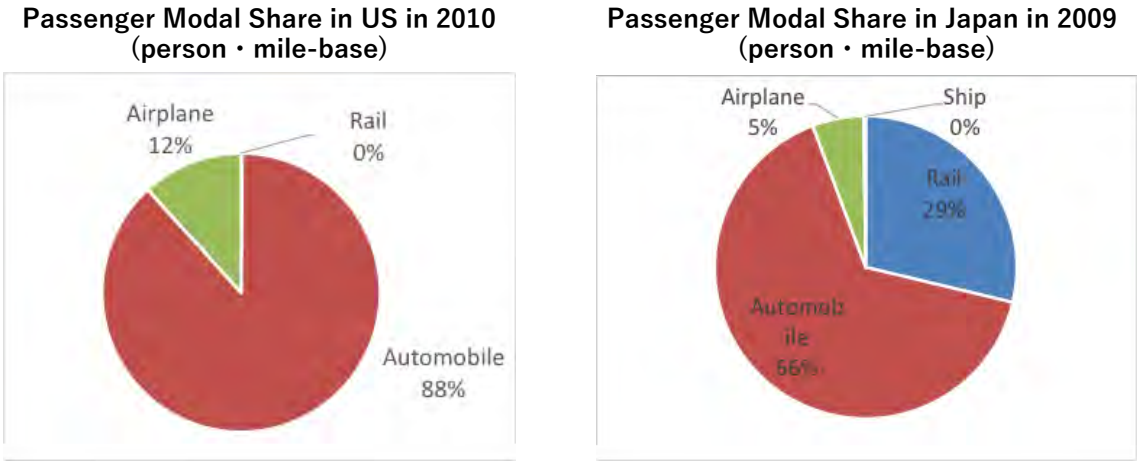


Figure 4- 21 Comparison of Passenger Modal Share between US and Japan.

(Figures are made by the author. Data Source: MLIT Japan [66])

Plus, the government interest on its infrastructure has declined, as is represented in Figure 4-22. This figure shows the "combined money that federal, state and local governments spend on construction," "relative to the size of the economy, in the last five years. And only part of the decline stems from the end of the stimulus program, which temporarily lifted infrastructure spending." And it argues that "such spending now represents about 1.5 percent of total economic activity, down from about 1.8 percent on average from 1993 through 2008. It's at its lowest level in at least 22 years."

One can infer that governmental interest on infrastructure has dropped, thus railroad

investment would not be the most important issue the government cares about.

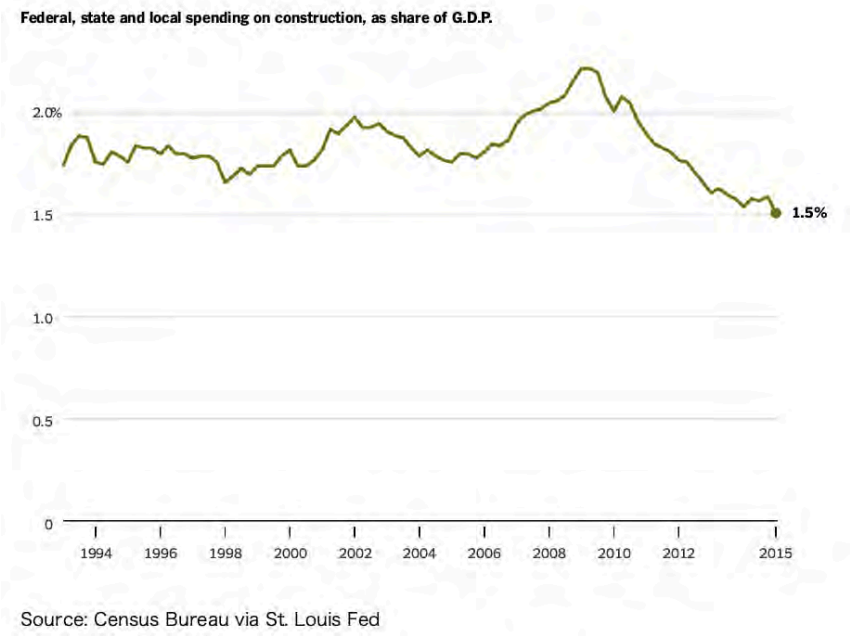


Figure 4- 22 Transition of US's Federal Investment on Construction as Share of GDP.

(Adapted from The New York Times [67])

This argument can be underpinned by the fact that the government was trying to decrease its federal financial support on Amtrak for the Fiscal Year ended Sep 30th, 2018 [68]. Their main point was that States should pay more budget on Long-distance trains. Their other rationales included that Amtrak could improve its efficiency and cut operation cost. They also argued that Amtrak could eliminate redundant routes. One can see that these are political discussions, and are not completely driven by Amtrak's aged infrastructure and degraded safety. It seems some of the Long-distance trains could be eliminated, but it would not be possible without the federal government's initiative.

However, the government did eventually increase its funding amount [69]. But the attempt by the government seems to reflect their low priority on the railroad infrastructure. They were more focused on other issues, such as military or border security [68]. This indicates that the Amtrak's

financial stream is very prone to political decisions.

Even worse, the U.S. Congress voted to decrease funding immediately after the second derailment happened in 2015:

> The House Appropriations Committee voted to cut funding to the public-sector rail company by 18% – less than 24 hours after its Northeast Reginal train 188 came off the tracks at more than 100 mph, killing seven. The Republican-controlled committee rejected Democratic attempts to boost spending on Amtrak by more than $1 billion, including $556 million for the busiest north-east corridor that links Washington, Philadelphia, New York and Boston [70].

Therefore, one can maintain that the underlying issue is broader than Amtrak or government. That is, if people do not care or use the system, then the government does not have any reason for prioritizing the system's improvement.

4.11.2 Aging Infrastructure

The result is the old railroad infrastructure (See Figure 4-23). This figure shows the transition of average age of Amtrak's vehicles from 1972 to 2015. It is estimated that Amtrak's infrastructure backlog has reached 38 billion US dollars [41]. This is at least partially due to insufficient governmental supports over time.

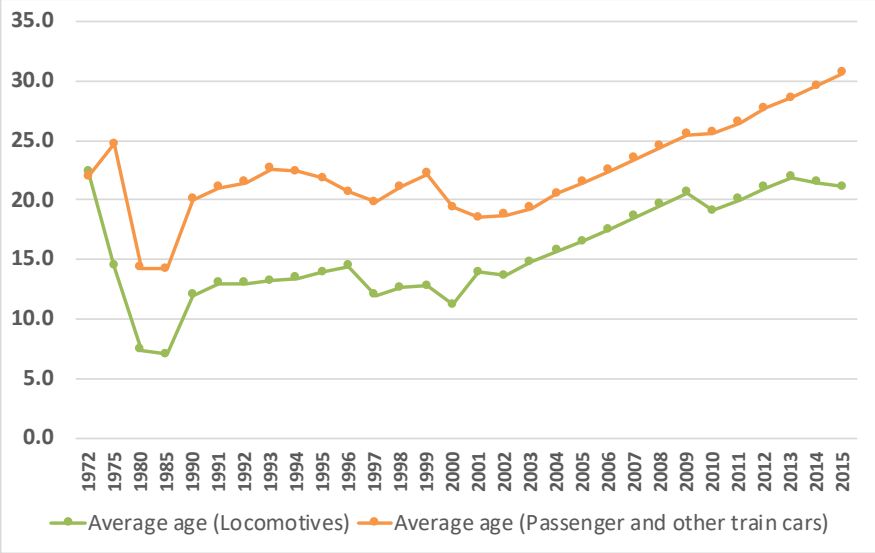


Figure 4- 23 Aged Vehicles of Amtrak.

(Figures are made by the author. Data Source: USDOT [71])

4.11.3 Others

The issues mentioned in the WMATA section, including “Degradation of Safety Culture” and “Degradation of Safety” are also applied to the Amtrak case. For details, see the CAST Analysis for WMATA crash.

4.12 Reviewing and Revealing the Weakness of Safety Control Structure

In this section, the analysis results are summarized in the safety control structure, which explain each controllers’ safety constraints, UCAs, Mental Model Flaws, and Context.

Figure 4-24, 4-25, and 4-26 show Safety Constraints Violated in the Highest-Level of Safety Control Structure, that of Middle-Level, and Lowest-Level, respectively. From these figures, one can see how many UCAs and violated safety constraints are found in the different levels. This means that there is no “root cause,” but there are many “causes” or “factors.” These causes should be guarded by more appropriate safety constraints at each level. As these revealed causes should be

documented and passed on to the future system design, in the next section these are translated into the form of recommendations.

Figure 4-27 shows the simplified and consolidated version of Figure 4-24 ~ 4-26. The dotted red line indicates what was ineffective and contributed to the accident, whether control actions, feedback, or controllers. As is revealed so far, every controller contributed accident, and there are many ineffective control actions and feedback.

Although there seems to be no “root cause,” this thesis concludes that there are underling weaknesses in this safety control structure. At each level, (1) Ineffective Safety Culture and (2) Insufficient Budget seem to have enabled many UCAs to occur. This underlining weakness is very similar to that of WMATA, thus the discussions about these causes are provided in the next Chapter to summarize the lessons learned from two CAST analyses.

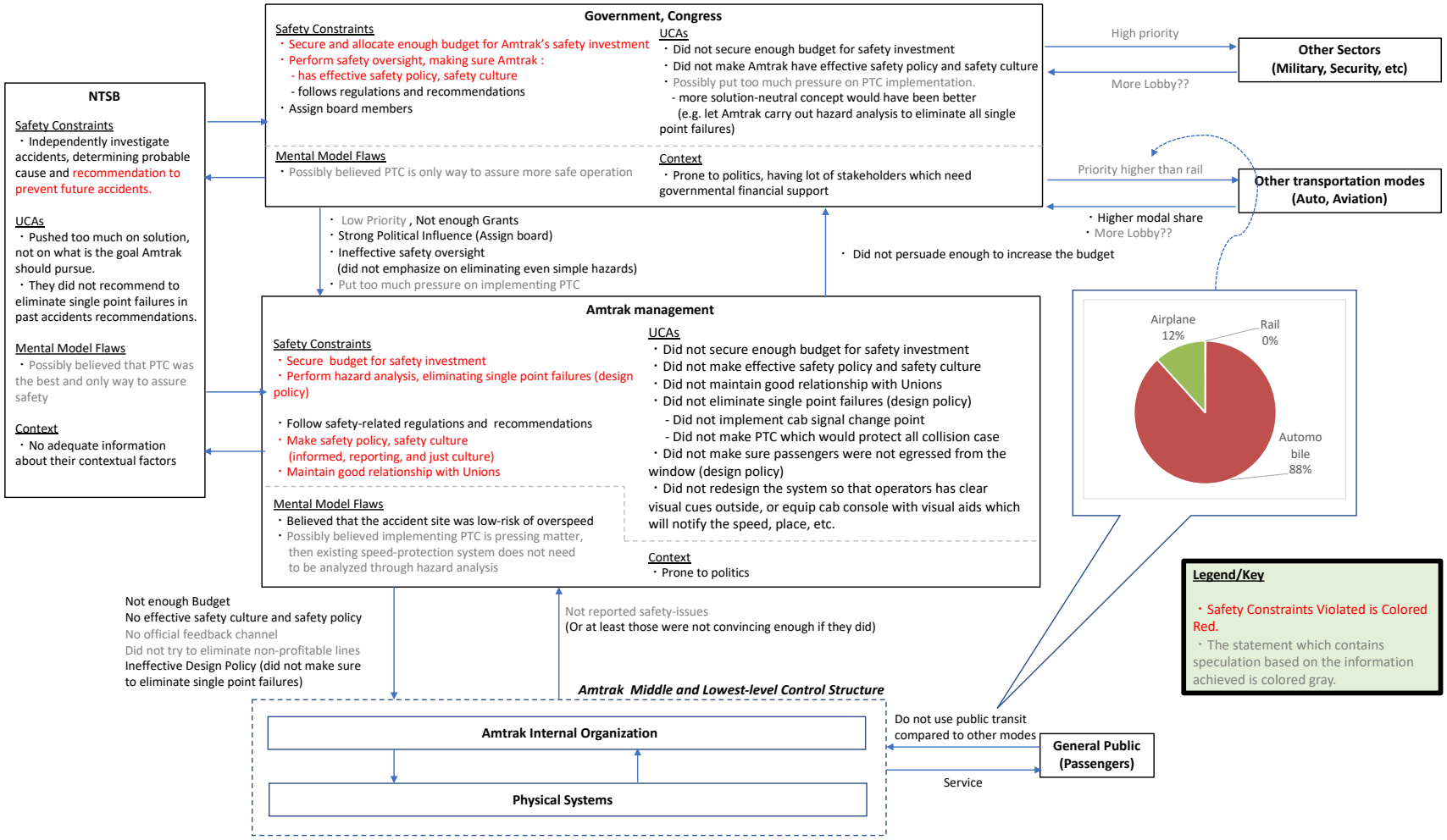


Figure 4- 24 Safety Constraints Violated in the Highest-Level of Safety Control Structure.

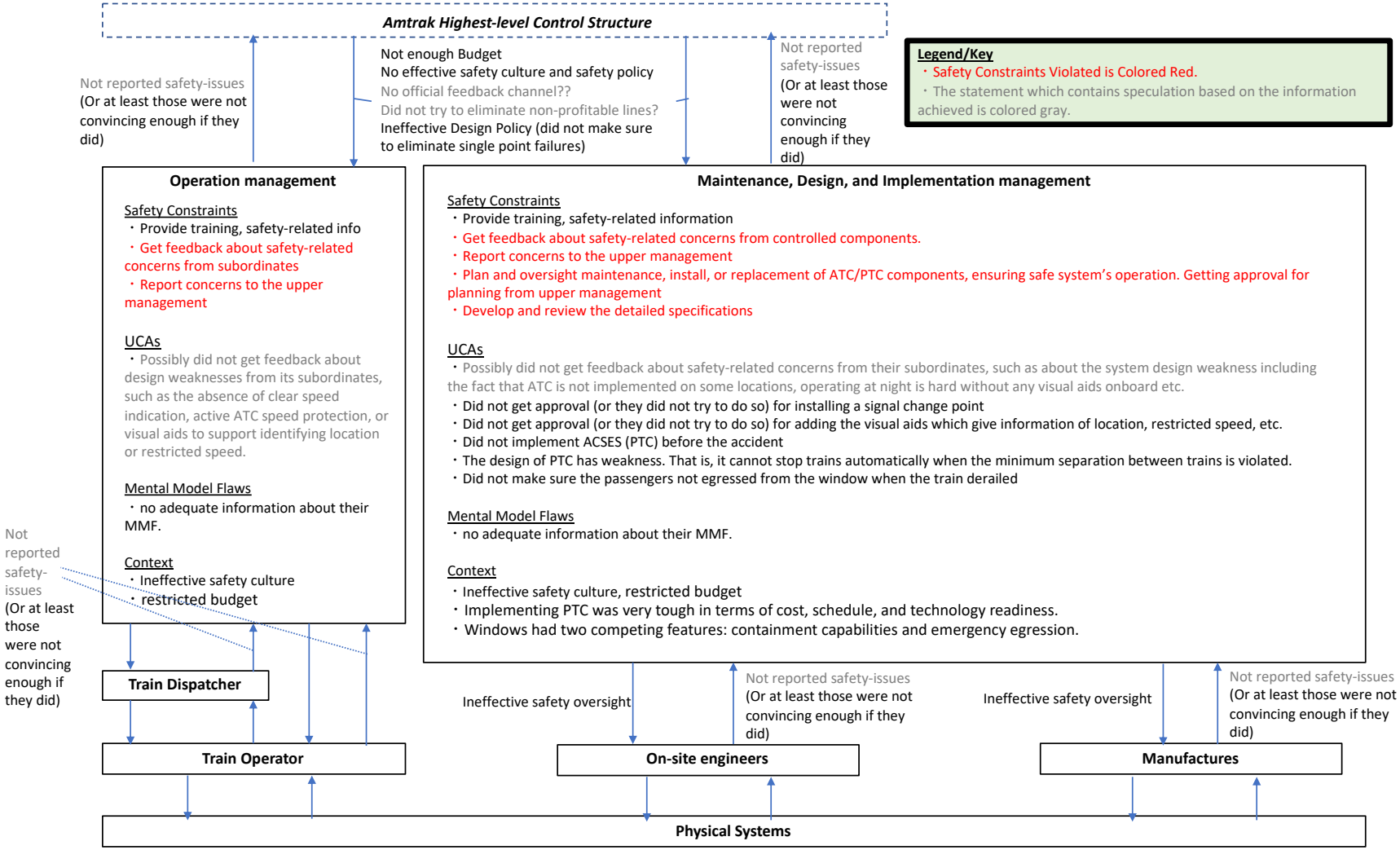


Figure 4- 25 Safety Constraints Violated in the Middle-Level of Safety Control Structure.

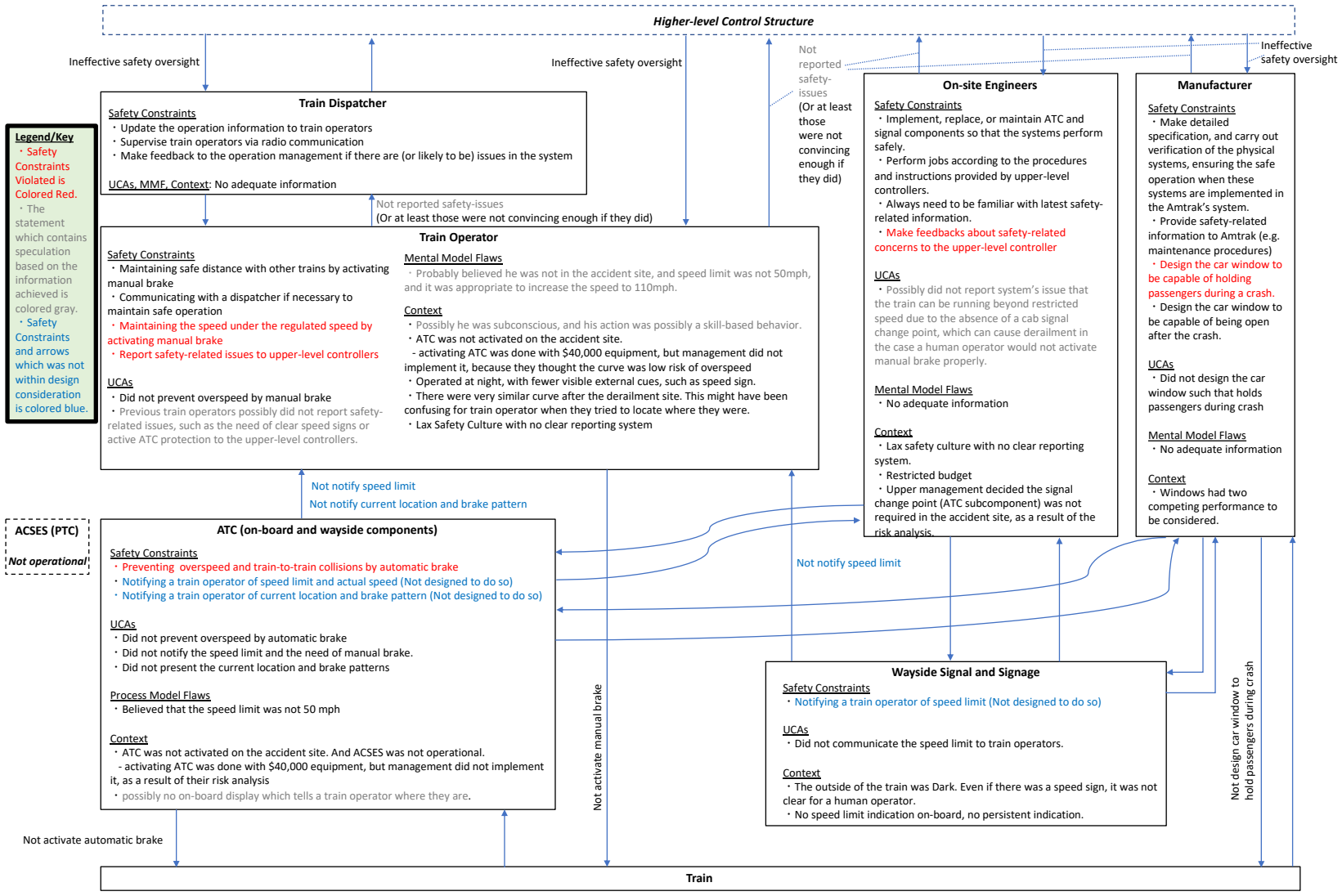


Figure 4- 26 Safety Constraints Violated in the Lowest-Level of Safety Control Structure.

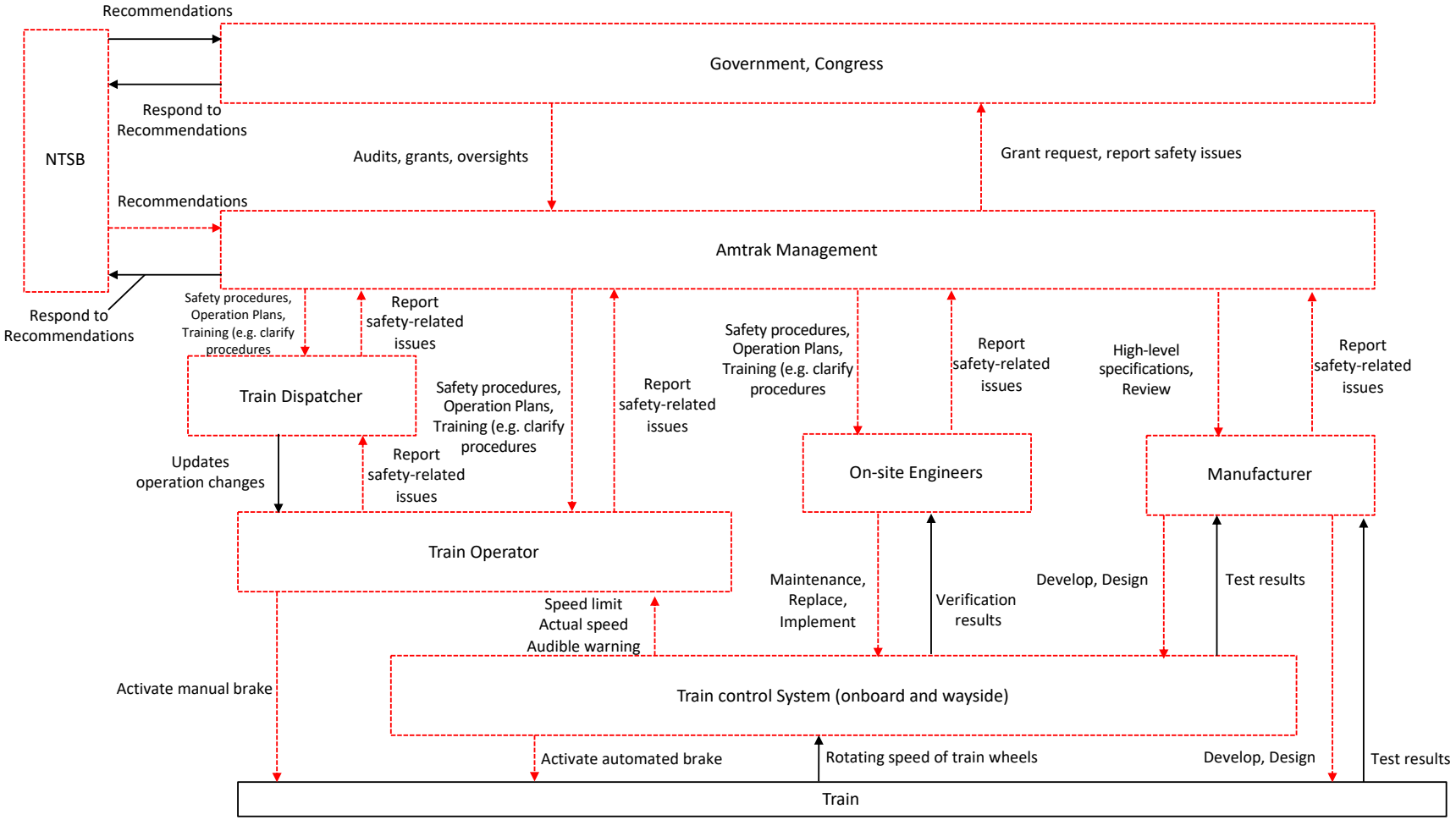


Figure 4- 27 Ineffective Control Actions, Feedback, and Controllers.

4.13 Questions Unanswered in the NTSB Accident Report

Through the CAST analysis, it was revealed that some information was not gathered in the NTSB accident report. These areas are labeled as “no adequate information” in the analysis (See Figure 4-24, 4-25, and 4-26 for instance). If CAST framework was used in the accident analysis process, this information would be gathered or at least requested and investigated. This missing information is important to understand the underling systematic causes.

4.14 Generating Recommendations

Through the analysis provided so far, some recommendations have been proposed. A more complete list of the recommendations resulting from the CAST analysis are as follows.

Systems Design

1. Review and improve the design processes to assure high-level safety.
    - Implement iterative design processes that periodically check and learn from the current system’s performance to drive the next design cycles.
    - In the process, interview current users and operators about the design issues and possible improvements.
2. Improve the way in which the operation conditions are provided and displayed to the train operators, changing the interfaces and algorithm if necessary.
    - Evaluate and equip an on-board display which provides a train operator the current location, current and future speed limits, and brake patterns
    - Consult with human factor professionals about possible design changes
    - Consult with other country’s professionals, such as Japan, about possible design changes
3. Implement the way-side speed signs ahead of every speed-change point. Make sure those signs are visible from the cabin even in the night and poor weather.

4. Explore and evaluate the best design policy of train vehicles' windows, which would optimize the two competing performances of the train windows. Both performances should be assured at the same time.
    - The current design of the train windows had two competing performances to be considered; containment capabilities (may inhibit passenger egress), and emergency egression (allow passengers to egress).
5. Make sure the Train Control system can eliminate all the hazards of single-point-failures.
    - Evaluate the redesign of ATC system such that it will automatically activate brake if a train speed exceeds a speed limit or brake patterns. One possible solution is to implement signal change point ahead of every speed-change point.
    - Current PTC design does not seem to address this hazard. Ensure that PTC is equipped with capability to eliminate it.

Amtrak Management

1. Create Organizational Policy, Rules Values, and Practices to ensure the effective safety culture is embedded in the organization.
    - It may be useful to consult with specialists in aviation industry where the safety culture seems to be more mature.
2. "Establish organizational and management structures to ensure that safety-related technical decision making is independent from programmatic considerations, including cost and schedule." (Adapted from Leveson [6, p. 437])
3. Evaluate the System Safety Control Structure, and redesign it if necessary.
4. Evaluate the System Safety Programs.
    - Learning best practices in the railway company
    - Exploring and learning best practices in other industries, such as aviation industry.
5. Improve the methods used to identify hazards and the mitigation plans
    - Consult with system safety professionals
    - Researching the best practices in the industry
6. Ensure that manufactures are carrying out effective hazard analyses, including single point hazards, non-failures, and human factors interactions

- Evaluate the best design strategy of ensuring egress after a collision and protecting passengers during a collision through effectively coordinating with manufactures and research entities.

7. Ensure that the safety-related budget is sufficient to maintain safe operation.
    - Evaluate current financial policy (i.e. amount of the money received from upper controllers, amount of the money allocated to non-safety-related and safety-related activities), including outside specialists.
    - Campaign appropriately for increasing budget or grants from the governmental authorities, present how severely degraded the current systems are, and the urgent need for the extra funding.
8. Create effective official communication channels, making sure any safety-related information or concerns are well circulated around the company, well understood, and acted upon. This is not only top-down, but also bottom-up reporting and horizontal communication.
    - Create an environment where employees can comfortably report any safety-related issues without fear
    - Do not rely solely on the informal feedback from the lower-level controllers. Always check the validity of the information through official communication channels
    - Identify means to improve the current communication system.
9. Make and maintain good relationships with Unions, and ensure employees can maintain safe operation and reports of safety concerns are acted on.
10. Create and carry out training programs to make sure the recommendations provided above are properly followed and maintained throughout Amtrak.
11. Follow the safety recommendations provided by NTSB and other audit authorities in a very timely manner.
    - This includes recommendations provided before this accident.

Congress and Governments

1. Evaluate current routes that are not profitable, identify how to make them more efficient or eliminate them from Amtrak's operation by coordinating with Amtrak, States, and other stakeholders. This would require initiative from the federal government.

2. Should not think the Amtrak's budget as "floating". Amtrak is very relying on Federal grants, thus it would be impossible for Amtrak to continue operation without it. It should try to leave some amount of annual budget for Amtrak, so that Amtrak can plan long-term investment plan more easily, for example.
3. Evaluate the funding required to improve Amtrak's rail operation safety, then make a strategy to ensure the safety-related funding needs are met.
4. Evaluate current financing methods to Amtrak.
    - Evaluate the possibility of assuring long-term grants, so that Amtrak can plan long-term safety improvement plans.
5. Evaluate current safety oversight methods to Amtrak.
    - Review and ensure Amtrak has effective safety policy and safety culture.
6. Evaluate the best way to propose recommendations to Amtrak.
    - Consider how emphasis on specific solutions may overlook other hazards, like inadequate PTC implementations that meet the letter of the law but would not prevent accidents like this (including Amtrak's current PTC implementation plan)
    - Consider solution-neutral recommendations if needed

NTSB

1. Include broader recommendations about quality of hazard analysis and risk assessment methods.
2. Include recommendations about eliminating hazard involving single point failures.
3. NTSB should remember that pushing a specific "solution" too hard can make operators not think deeply about what is actually needed to maintain safe operation.
    - Activating ATC was relatively easier and quicker for Amtrak than implementing PTC. Both implementations would require upgrading to prevent this type of accident, but recommendations focused on implementing the technology rather than ensuring the type of implementation would be effective

4.15 Conclusion

In this chapter, the accident analysis was carried out for the Amtrak derailment in 2015 using the CAST framework. The train ran at 106 mph on a steep curve where the restricted speed was only 50 mph, causing derailment and 8 people were killed. Although the accident report pointed out the human error of the train operator, his action was somewhat understandable considering the situation he was facing. First of all, he was probably not alert at the time of the accident because he was focusing on other emergency situation near the accident site. Plus, there was no clear indicators about where he was and what is the speed limit.

Because human operator is not perfect, the limitation of human capabilities should be considered in the system design process. In this specific case, the speed-protection-system such as ATC, which can be a back-up when human cannot act properly, was not in the place. In addition, there was no on-board visual aid to help locate the location of the train, which would be of use especially when the outside information is very limited due to darkness. These designs should be taken into account in the future system designs.

This thesis considered that Amtrak had no requirement to eliminate single point hazards, where the safety of the operation was solely dependent on the human operator. In NEC, there were some places where ATC was not activated by design, and the safety was dependent on the human's alertness. The lack of speed protection was due to Amtrak's managerial decision, that is, they believed that train operator would not exceed the speed limit in these places. This thesis explored possible explanations for their decision such as the lack of safety culture, where the costs and a restricted budget required compromises in safety.

Amtrak has been in a deficit for a long time and they have been receiving governmental financial support. However, that support was not sufficient for investing in safety maintenance and improvement. Actually, the backlog was estimated to be $38 billion. This thesis identified contributing factors like the government's low priority on the railway system, and unprofitable lines which would be difficult to eliminate without political initiative.

In addition, this thesis maintains that the NTSB and FRA were pushing for implementing PTC as a solution, despite the technology was not ready and the cost was tremendous. Instead of this solution-based recommendation style, they might consider recommending solution-neutral criteria.

In this case, the solution-neutral recommendations might involve technical capabilities like automatic controls to decelerate and prevent derailments (rather than specific technology like ATC or PTC, which could both be implemented in either effective or ineffective ways). Recommendations should also consider hazard analysis and safety assessment criteria like eliminating situations where the safe operation are solely dependent on a human operator's alertness or solely dependent on a single-point issue. Pushing a specific solution too much may not always be effective.

Further, as the section 4.12 reveals, there are many systemic causes/factors within the safety control structure which contributed to the loss. Importantly, these were not connected linearly, rather they were interwoven nonlinearly and intricately. Thus, we need to appropriately add safety constraints to each controller. This would be facilitated by implementing recommendations provided in section 4.13 so that the identified causal factors would be eliminated or controlled [6, p. 442].

Lastly and importantly, it was also revealed that NTSB accident report did not provide enough information about several causes, such as Mental Model Flaws of Amtrak middle management controllers, which would explain their unsafe control actions. This missing information could have revealed more systemic causes that contributed to the accident, and should be understood and translated into the recommendations so that one can learn from the accident and design safer systems in the future. If CAST framework was used during the accident investigation, this missing information would be were gathered and more precise picture of the underlying causes would have been revealed.

In chapter 3 and 4, two CAST analysis were carried out and the results were documented so far. Although recommendations were proposed in the end of chapter 3 and 4 respectively, these lessons would be summarized into the list of recommendations for the future system design and operation in the next chapter.

(This page intentionally left blank)

Chapter 5 Lessons Learned from CAST Analysis

The previous two chapters carried out accident analyses for two accidents in the US, and generated several recommendations. Some of these are very specific to the analyzed system, but most of them are applicable and beneficial for future systems and organizational designs as well as for understanding effective decision-making. This chapter translates those recommendations into combined lessons learned for future system design and organizational design of safety-critical rail systems. Although both systems examined are conventional rails, the following lists of lessons may also be beneficial and relevant for other rail systems, that is, HSR and SC-Maglev.

In addition to the two case studies in previous chapters, this thesis further explores other accident analysis results carried out by other researchers. As such, the author found it important to introduce the CAST analysis result of the Fukuchiyama derailment in Japan in 2005 carried out by Ota [72]. The result of his analysis is relevant because: 1) his thesis's motivation was similar to that of this thesis; 2) the Fukuchiyama derailment involved the lack of an operational speed protection system, which is similar to that of the Amtrak derailment in the US; and 3) some of his findings potentially strengthen the lessons learned through this thesis.

5.1 Literature Review – CAST Analysis for the Fukuchiyama Derailment in 2005 in Japan

5.1.1 Overview of the Fukuchiyama Derailment

Around 9:16 a.m., on Monday, April 25th in 2005, train 5418M of the West Japan Railway Company (JR West) departed from Itami station. It passed Inadera station, then passed Tsukaguchi station around 9:18 a.m. When it was following the right-hand curve with a radius of 304 m in the south of the highway that connects Nagoya and Kobe, it was traveling at 116 kph while the speed limit was only 70 kph. The first car derailed around 9:18:54 a.m. to the left, then the second to fifth cars derailed, and finally the 7th (last) car stopped around 9:19:04 a.m. This resulted in a total of 107 fatalities and 562 total injuries [11].

The investigation concluded that the operator of train 5418M violated some of the operation rules on the day the accident happened. The report found that the operator was afraid of being punished for those violations and was trying to make up excuses for his actions, so he might not have been focused enough on his job of operating the train. The report also points out the absence of a speed-protection system at the accident site. One of the reasons for that absence is the slow decision-making process within JR West. It also found that the Japanese government did not mandate the speed-protection system at the time of the accident. See Figures 5-1 and 5-2, which show the location and the aftermath of the derailment.



Figure 5- 1 Fukuchiyama Line and the Location of the Derailment.

(Adapted from JR West [73])



Figure 5- 2 Accident Aftermath of the Fukuchiyama Derailment.

(Adapted from The Sankei News [74])

5.1.2 Key Findings from CAST Analysis and comparison with those in this thesis

Regarding the Fukuchiyama derailment, Ota [72] carried out the CAST analysis and documented some important lessons learned from that analysis. He pointed out the following as valuable lessons:

i. This is not a component failure, but a system accident, with which the reliability engineering approach cannot deal;

ii. This type of accident, a derailment accident, is extremely rare; however, it still has great potential to cause enormous damage;
iii. Risk/hazard analysis is the key to assuring safety in today's complex systems;
iv. The accident deeply involves human factors, which play a major role in current railway systems;
v. It is almost impossible to figure out the probability of this type of accident;
vi. The railway systems are prone to asynchronous evolutions, which could be one of the factors that cause an accident [72].

The author believes that all of the lessons pointed out by Ota are also true for the two accidents analyzed in this thesis so far.

First, Ota insists that the current international standard IEC 62278, which provide the guidelines for hazard analysis for today's railway systems, cannot deal with and prevent system accidents in which no component failure contributed to the accident. He points out that the underlying approach of IEC 62278 is a reliability engineering approach, but a different approach should be utilized for hazard analysis. As the Fukuchiyama derailment did not arise from component failures, the reliability engineering approach was not effective to prevent the accident.

Considering the WMATA and Amtrak accidents, it is unknown whether the operating companies did carry out hazard analysis and what approach was used for the analysis if it was carried out. However, it is true that a reliability engineering approach would not have been effective for preventing these accidents either because they were also not caused by component failures.

Second, Ota acknowledges the fact that the Fukuchiyama derailment was a very rare event, that is, it was the third overturn accident in eighteen years. However, he also insists that there exist potentially serious accidents even with a rare occurrence, thus we should not ignore the risk even if it is very rare. In fact, although the Fukuchiyama derailment was a rare accident, it was "the most serious accident in Japan in forty years" [72]. Because the overturning accident was rare in Japan, Ota claims, Japanese MLIT did not pay enough attention to this type of accident, failing to communicate the risks to railway operation companies.

This point is also applicable to the Amtrak accident. The Amtrak management and/or

lower-level controllers did not decide to implement speed-protection in the curve where the accident happened. PTC was planned to be operated within several months after the accident happened, but there was not any speed-protection system in place. One possible solution would have been implementing a cab signal change point, which reportedly would cost only $40,000 but was not implemented. This is because Amtrak believed that the probability of overspeed was very low.

Third, Ota argues that both JR West's management and their employees did not recognize the risk of overturning accidents due to a poor risk/hazard analysis. For one thing, he points out the fact that the company did not accurately calculate the overturning speed. While the correct calculation result should have been 106 kph, the company incorrectly calculated that it was 133 kph. It was later revealed that the company did not consider vehicle vibrations in the calculation. Thus, the company did not assess the risks of overturning correctly. Company management also believed that it would not result in overturn even if the train speed is 120 kph because there had been no derailment so far with this speed, but this mentality contributed to the inappropriate risk analysis that concluded the train would not derail even if it runs at 120 kph. The management simply did not recognize the overturning risks correctly. In addition, the train operators did not understand the overturn risks correctly, and many of them overestimated the overturning velocity. These findings reinforce the importance of carrying out appropriate risk/hazard analyses to ensure both management and employees understand and recognize the risks.

This point is also true for WMATA and Amtrak. For Amtrak, the risk analysis was poor as explained above. The same was true for WMATA, where both management and lower-level controllers did not understand the risk correctly. For example, management believed that the expansion of capacity was an improvement and would not degrades the safety of the system. However, the increased operation hours and longer track length forced the maintenance teams to finish their work within a smaller amount of time while the total amount of work increased. In addition, some of the maintenance engineers did not follow procedures or seek approval for doing so. These examples demonstrate instances where both management and the front-line workers did not understand the risks involved in the systems they were overseeing.

Fourth, Ota pointed out that JR West did not adequately consider human factors and lacked effective system design which would have prevented errors caused by humans. This was demonstrated by:

1) The safety device assumed operators would be attentive and would initiate braking when needed, and therefore was incapable of automatically activating the brake. In fact, the train operator did activate the manual brake but was too late by 16 seconds, which was not protected by the safety device;
2) Time pressure and mental and physical stresses were felt by the train operators due to the reduced time margin as a result of increased frequency of operation;
3) The punitive training program had negative effects on some train operators, including the one who operated the train 5418M and had been afraid of attending training after his duty that day [72].

Ota concludes that these examples support his idea of the significance of considering human factors in today's railway systems [72].

This point is also applicable to WMATA and Amtrak accidents. For WMATA, one example includes the OCC Display, which generated more than 8,000 alarms every week. This made OCC operators inattentive to alarms, and they were likely unable to find all the causes of all alarms. For Amtrak, examples include the lack of the speed-protection system and the visual aids which would have supported the train operators in understanding the location of the trains and the current speed limits.

Fifth, Ota argues that it is almost impossible to calculate and predict the probability of a system accident because it arises from often unanticipated component interactions rather than component failures. He maintains that the international standard IEC 62278 considers systematic failures as non-quantifiable elements, thus his idea is aligned with the standard in this perspective. He also claims that in human factors it is very difficult to assign a probability, thus the probability of the situation where a train operator does not activate manual brake and prevent overspeed is impossible to calculate accurately. Thus, he concludes that it is impossible to determine the probability of a system accident. He further explains that risk is characterized as the severity and probability of accidents, but focusing on the probability is not appropriate because of its uncertainty. He argues that the focus and emphass should be on severity of accidents instead.

His fifth argument, that is, focusing on severity instead, is applicable to the Amtrak accident and might have prevented it. As was explained earlier, Amtrak believed that the probability

of overspeed was very low, thus the cab signal change point was not needed on the accident site which would have prevented over-speed situation. If Amtrak focused not on probability, which in hindsight was not easy to calculate accurately due to uncertainty, human factors contributions, and other issues, but instead had focused on severity, then they would have likely implemented the cab signal change point before the accident.

Sixth, Ota contends that asynchronous evolution, in which a subsystem changes without appropriate changes in other subsystems, contributed to the accident. He argues that JR West did not improve ground equipment (e.g. ATS-P or ATS-SW) so that it would be capable of detecting or preventing speed violations, but the operation speed limit was increased from 100kph to 120kph and the radius of the curve was reduced from 600 meters to 304 meters. He further maintains that "railway systems are vulnerable to asynchronous evolution" [72], because: 1) railway operations are achieved by several functions and organizational components, and 2) changes are constantly introduced into subcomponents as a result of modernization or degradation. However, he points out, "there is always a possibility of neglect of their consequences for other parts of the systems" [72].

This last point also holds for both WMATA and Amtrak systems. For WMATA, management decided to expand capacity but they did not allocate enough budget and time toward eliminating and repairing the malfunctioned track circuits that had been almost paralyzing OCC due to the unmanageable frequency of alarms. This initiative, aimed at a partial improvement within the system (i.e. capacity), caused further deterioration of other parts critical to safety that were neglected (i.e. an increased number of track circuit malfunctions and inability of OCC to solve those malfunctions). For Amtrak, the train maximum speed was increased continuously but speed-protection systems were only selectively added and the accident site was not on the list. Asynchronous evolution clearly contributed to the both WMATA and Amtrak accidents to some extent and should be noted as one of the lessons learned.

In this section, the lessons learned from CAST analysis carried out previously by the other researcher were introduced and compared to the two accidents that this thesis analyzed. These lessons were found to be applicable to both accidents in another country and almost a decade later (in the case of Amtrak). Therefore, the next section considers these points in deriving lessons learned in the hope that these can be remembered and translated as future railway systems are designed and managed.

5.2 Lessons Learned

In this section, common patterns are extracted from the recommendations provided in chapter 3, chapter 4, and section 5.1, and these are summarized as “lessons learned”. These should be considered and translated into systems design and management requirements for future systems.

General

1. Carry out extensive risk/hazard analysis starting in early concept development and continuing through any design or redesign processes after operation starts. In assessing the risk/hazard, put the emphasis on severity rather than on probability. That is, even if the occurrence of the risk/hazard is assumed to be low probability, if the severity is tremendous then we still should eliminate or minimize that risk/hazard.

2. In developing a subsystem, carry out a risk/hazard analysis that considers how components and subsystems can indirectly affect other subsystems and impact the whole system’s performance. If a new development affects the whole system’s integrity and safety, then other subsystems may need to be updated as well to ensure safety of the overall system.

3. Human factors (i.e. human capability and limitations) must be considered throughout development processes, making sure that the designers consider unsafe human actions that can be caused by design choices like limited or missing feedback for the operator. Do not assume human operators are infallible and will always intervene when necessary.

Management and Operation

1. Set Organizational Policy, Rules, Values, and Practices to ensure an effective safety culture is embedded in the organization.

2. “Establish organizational and management structures to ensure that safety-related technical decision making is independent from programmatic considerations, including cost and schedule.” (Adapted from Leveson [6, p. 437])
3. Evaluate the System Safety Control Structure, and redesign it if necessary.
4. Evaluate the System Safety Programs.
    - Learning best practices in the railway company
    - Exploring and learning best practices in other industries, such as aviation industry.
5. Improve the methods used for identifying hazards, performing hazard analysis, and creating mitigation plans
6. Ensure that malfunctioned track circuits’ components are replaced properly and promptly.
7. Ensure that procedures for verification of equipment (like track circuits) are understood and followed properly.
8. Ensure that manufactures are carrying out appropriate hazard analysis and are not limited to considering a narrow set of causes like component failures (e.g. use systems approaches like STPA)
9. Even when systems are brand new and the frequency of malfunctions is low, make sure every malfunction is properly resolved in a timely fashion.
    - Even more so when malfunctions happen in safety-critical systems like an ATC system
10. Allocate adequate amount of time and manpower for everyday maintenance activities.
    - Without adequate time for maintenance, midnight operations should be avoided.
11. Allocate and invest in safety-related activities.
    - Management should keep in mind that the first priority is repairing or replacing the aged track circuits in a very timely manner.
12. Ensure that the safety-related budget is sufficient to maintain safe operation.
    - Take extra attention when deciding upon non-safety-related capital investment (e.g. capacity expansion projects). These investments should not harm the safety-related budget
    - Evaluate current financial policy (i.e. amount of the money received from upper controllers, amount of the money allocated to non-safety-related and safety-related activities), asking outside independent specialists for help with the process. Change the policy when deficiencies are found.

- Campaign appropriately for increasing budget or grants from governmental authorities, presenting openly and effectively how severely degraded the systems are and the urgent need for the extra funding.

13. Create effective official communication channels, making sure any safety-related updates are well circulated around the company, periodically check that they are well understood, and verify they are acted upon. Management should define the explicit procedure for this process.
    - Create an environment where employees can comfortably report any safety-related issues without fear
    - Do not rely solely on the informal feedback from lower-level controllers. Verify the validity of the information through official communication channels
    - Consult professionals about creating more effective communication systems. Research and ask for best practices in the transportation industry. It would be useful to consult with specialists in the aviation industry where the safety culture seems to be more mature.
14. Require that any improvised procedures are checked and approved by upper-level controllers.
    - If the upper-level controller is not the same person who made the official procedure, then he/she must ask that person for approval. Management should provide the explicit procedure for this process.
15. Require that manufacturers' recommendations for safety-critical equipment be followed
    - If a need arises not to follow manufacturers' recommendations, then the reasons and the design alternatives should be evaluated and approved by upper-level controllers. Management should provide the explicit procedure for this process.
16. Evaluate the operation strategy to stop every train when there is even the least chance of malfunction in a safety-critical equipment (e.g. track circuits)
17. Respond and follow properly to safety recommendations provided by investigative and audit authorities in a very timely manner. Create and carry out training programs to make sure the recommendations are disseminated, properly followed, and maintained throughout the company.
18. Create a clear procedure that shows exactly what actions are needed from the operators in a control center when they recognize alarms.

19. Create a clear procedure specifying what the train operators must do when they recognize equipment malfunctions, like an ATP speed signal that changes suddenly from non-zero to zero, then back to non-zero, indicating a malfunction of the ATC system. Management should provide the training for train operators to learn this procedure, and then clarify their understanding through, for example, paper tests, or simulator training.
20. Create and maintaining a good relationship with Unions and make sure employees are able and empowered to do what is needed to maintain safe operation.

System Design

1. Evaluate how operational conditions are displayed and alarmed to the operators in an operation center to improve their effectiveness.
    - Consult with human factors professionals about possible design changes
    - If the malfunctions happen in safety-critical equipment such as an ATC system, then the alarms must be acknowledged by the human operators and not automatically suppressed.
    - Too many alarms, especially false alarms, will defeat the purpose of having alarms. Consult with human factors to define limits on the number of alarms and false alarms, and take action to improve the quality of alarms or redesign to eliminate the need for alarms whenever the limits are exceeded.
2. Evaluate a redesign of the operator center's system algorithm, such as requesting the human operators to take actions (e.g. stop trains) or automatically stop trains if necessary (e.g. if the computer is suspicious about the incapability of track circuits detecting trains).
    - Design to detect track circuit anomalies that can result in trains not being detected.
    - A malfunctioning track circuit could be recognized by, for example, if the historical track occupancy by a train is traced and available. The system could then recognize, for example, when a valid train disappears suddenly and could conclude that the track circuit has some anomalies and is no longer detecting trains.
    - Evaluate the operation strategy of sending a stop signal (i.e. zero speed signal) to the following trains whenever the track circuit is classified as "incapable of detecting trains".
    - The stop signal should be sent either automatically by the operation center's computer or by the human operators' input. This point is related to the next recommendation.

3. Evaluate the design processes to assure high-level safety.
    - Implement an iterative design processes to periodically check and learn from the current system's performance, using this information to drive further design cycles.
    - In the process, interview current users about design issues and necessary improvements.
4. Evaluate the best way in which the operation conditions are displayed or alarmed to train operators effectively, changing the interfaces and algorithm if necessary.
    - Evaluate and equip the on-board display to provide train operators with the current location, current and future speed limits, and brake patterns (rather than requiring operators to memorize this information)
    - Consult with human factor professionals about possible design changes
    - Also consult with professionals in other countries, such as Japan, about possible design changes
5. Implement way-side speed signs ahead of every speed-change point. Make sure those signs are visible from the cabin even in the dark and in poor weather.
6. Explore and evaluate a design policy for train vehicles' windows to ensure passengers are not ejected during a collision but are able to egress after an accident.
7. Ensure the Train Control system is designed to eliminate all the single-point hazards.
    - Evaluate a (re)design of the ATC system such that it can automatically activate brake if a train speed exceeds a speed limit or brake patterns[48], as in standard in other countries and other industries (e.g. in automotive)

Congress, Government, and safety-recommendation-providing authorities (e.g. NTSB)

1. Create audit authorities that are independent from a railway operation company, including independent board members.
2. Provide the audit authorities with the statutory power to compel a railway operation company to respond and follow safety recommendations
3. Evaluate the budget required for maintaining or improving rail operational safety, then create a strategy to allocate the necessary budget to railway operations.

[48] Brake patterns mean the projected speed limit that the train should not violate. In a common rail speed protection system like ATC, the automated brake would be activated if the train actual speed violates or "touches" this brake pattern.

- If a train company relies heavily on government grants, then evaluate the possibility of assuring long-term grants so that a train company can create long-term safety improvement plans.

4. Evaluate the best way to propose recommendations to a railway company.
    - Create solution-neutral recommendations when appropriate, considering the fact that technologies change and can be implemented in both effective and ineffective ways.
5. Evaluate cost and technology-readiness when making recommendations as far as possible.

5.3 Conclusion

In this chapter, lessons learned from two CAST analysis in chapter 3 and 4, and lessons learned in the literature were summarized as “lessons learned.” These lessons are of course not complete, but intended to be useful for future systems in the passenger rail sector.

In the next chapter, the thesis will be concluded with the answers to questions raised in section 1 and a discussion of potential future work.

(This page intentionally left blank)

Chapter 6 Conclusion and Future Work

In this thesis, the new accident analysis technique called CAST was applied to two US rail accidents. The accident analysis results were then summarized as recommendations, translated into common lessons for future system operations, management, and development in section 5.2.

In this chapter, the answers to the research questions of this thesis that were proposed in section 1.2 will be documented first, then the thesis will be concluded with some final remarks and suggestions for future work.

6.1 Answers to the Proposed Questions

In this section, the answers to the questions proposed in section 1.2 are provided.

6.1.1 Why and How Do Automated Railway Systems Behave in Unsafe Ways

Through two CAST analyses, it was found that many causes contributed to the accidents. It was remarkable that causes existed in almost every level of safety control structure in the form of Unsafe Control Actions (UCAs), Mental/Process Model Flaws, or Contextual Factors. These causes together lead to the accidents. Therefore, one can conclude that there were inadequate or ineffective safety constraints over each controller to regulate their behaviors. Thus, there is no “root cause.” The reason for each accident is not only one cause, but many.

In addition, although a human operator’s unsafe control actions (UCAs) could be one of the causes that contribute to an accident, it is not the purpose of an accident analysis to blame those human operators and engineers involved with accidents, if one wants to maximize the learning opportunity.

Furthermore, as the systems are dynamic, not static, the systems can change over time and migrate towards states of higher risk. For example, when the systems are brand new, then there might not be many accidents even if the maintenance and capital investments for safety improvements are not perfect. However, as time goes on, this may not hold. If the human mental models about risk,

updated procedures, the safety policy, etc. are not updated or drift, their attitude or priority toward safety could degrade over time. These changes can be enabled by, for example, ineffective safety information systems or a reporting culture where employees cannot comfortably report issues without fear of blame. If effective methods are not well established, then safety will degrade over time.

One should note that chronic problems in the system are nearly irreversible in the short span. That is, it often takes more time to improve the system back to an acceptable level than the time it takes to degrade to an unsafe level. Therefore, it is important to maintain systems and combat this degradation before it's too late. In other words, if no such measures are implemented, then a large backlog will accumulate and the system will drift toward unsafe states.

6.1.2 What Kinds of Causal Factors Contribute to Railway Accidents Involving Automated Systems

As was discussed in section 3.11 and 4.12, there are many different kinds of causal factors at each level of the safety control structure. The following summarizes the kinds of causal factors that were revealed through the two accident analyses:

Government, Policy Makers

・Did not secure sufficient budget for safe rail operation.

- They believed that the budget for railway was "floating" and can be reallocated to the other policies. This is possibly because the number of passengers for rail was far less than other transportation modes.

・Pushed too hard for specific (and flawed) solutions, which possibly made rail companies limit their goals of implementing appropriate solutions (e.g. PTC) in more effective ways. This is possibly because they believed that the specific solution was the only way to assure safe operation.

・Did not give audit authority the statutory power, thus the recommendations published by audit authorities could be ignored by the rail company

・Did not perform safety oversight effectively so that the rail company would have effective safety

policy and safety culture.

Audit Authorities (e.g. NTSB, TOC)

・Did not have statutory power to force rail company to follow the safety recommendations.

・Comprised of members who had conflict of interests, and was not a truly independent authority from the rail company.

・Pushed too hard for specific (and flawed) solutions, not more solution-neutral requirements of what must be accomplished regardless of the specific implementation.

・Did not recommend more solution-neutral goals. That is, they could have recommended rail company to “eliminate situations where the only safeguard for safe operation is the human operator.” To be more specific, some curves were not equipped with any speed-protection system so that if the train operator did not manually brake and slow down the train then it could overspeed resulting in catastrophic accidents.

Management, Design Decisions

・Did not secure sufficient budget for safety investment.

・Invested in expanding system capacity first to satisfy certain stakeholders, whereas they did not invest in needed safety improvements or maintenance projects adequately. This mentality caused the degradation of the safety culture, degradation of the infrastructure, and degradation of safe operations over time.

・Did not set effective organization policy, rules, values, and practices to protect safety-related technical decision-making from programmatic considerations, such as cost.

・Did not create an effective safety culture in which employees are informed of and have a knowledge of causal factors affecting safety, they are encouraged to report safety concerns or other safety-related incidents, and

・Did not have effective reporting systems or safety-related information systems whereby safety-information could be passed on to those who needed it, including bottom-up, top-down, or horizontal communication. This also includes the absence of checking or validation systems, which would assure that employees have and understand required safety-related knowledge.

・Did not leverage effective safety oversight

・Did not maintain good relationship with Unions

・Hazard (Risk) analysis was based on the assumed probability not on the impact or severity, which led to the situation where the human operator was a “last bastion” for the safe operation because management believed that the probability of the human’s speed violation would be less likely.

・Did not equip any visual aids in the cab console which would assist the train operator with locating the position of the train or identifying the speed limit, for example.

・Did not equip the system with the capability of allowing inputs from a human operator that would allow them to intervene to prevent collisions. For example, WMATA’s ATP system was generating speed signals only locally, thus human operators in the dispatch center did not have any authority to modify the speed signal even if they realized the train was about to collide with a stopped train in front (See chapter 3 for detail. Please note that ATS speed can only be modified within the stations, thus the human operators in OCC did not have authority to modify speed signal for the trains in between stations).

・Designed critical alarms to be automatically muted after several seconds have passed. In addition, more than eight thousand alarms were generated every week. This made it nearly impossible for human operators to realize the true anomaly in which the ATC system was unable to detect trains.

Human Operators, Engineers

The followings are some of the UCAs from humans, but these are just symptoms of the ineffective safety control structure. The focus should not be on blaming them, because deeper systemic factors will not be revealed with that mindset and important lessons would not be passed on into the future design considerations.

・Did not appropriately activate manual brake to slow down under the speed limit. (But this seems understandable considering the limitations of the system, including the lack of location and speed limit feedback that required operators to memorize this information.)

・Did not follow defined procedures and did not know, understand, utilize the latest procedures. (This is due to the inherent ineffective safety culture and the absence of effective reporting and safety-related information circulation systems.)

6.1.3 What Kinds of Considerations Should be Taken During Both Design and Operation So As To Maintain Safe Operation

The identified causal factors in 6.1.2 should be eliminated to create and operate safer systems (See section 3.11 and 4.12 for more detail). One of the ways to do that is by implementing the recommendations summarized in chapter 5. Importantly, when actually trying to implement these recommendations, they may need to be tailored and aligned with one's own system and environment. The recommendations are intentionally made to be generalized and solution-neutral so that they can be of use for a wide range of passenger rail sectors.

6.2 Conclusion of the Thesis

This thesis was intended to propose some considerations in designing today's safety-critical railway systems, such as HSR or SC-Maglev. As today's transportation systems, including railway, aviation, and automobile, are highly automated, the types of hazards and accidents have changed. Often, the automation is believed to increase the safety of the system, but it is not always true if appropriate considerations are not taken in the design process for both physical system and the organization.

As a way of thinking about the required considerations, this thesis carried out two accident analyses and generated design considerations for safety. This thesis utilized the CAST (Causal Analysis based on STAMP) approach, which can examine the whole hierarchy of a system holistically and thoroughly analyze why and how systems and components acted in unsafe ways.

As a result of the two accident analyses and the analysis results from the literature, 35 lessons (design considerations) were generated as "lessons learned" which the author believes to be useful and required in designing highly-automated safety-critical railway systems and organizations.

6.3 Future Work

In this section, potential future work is suggested, although this is subjective and not intended to be complete.

6.3.1 Specific Solutions for Implementing the Recommendations

In this thesis, several recommendations were proposed. However, these are very high-level (abstracted), and more concrete specific solutions should be examined and implemented in real systems.

Leveson argues:
"Recommendations to eliminate or control these factors must be created along with concrete plans for implementing the recommendations." (Adapted from Leveson [6, p. 442])

For example, both accident analyses showed that safety culture and its financial system (inadequate budget) were impacting many areas of the safety control structure, and many UCAs were somewhat affected by these two causes. This thesis did not dive into specific detailed solutions to these causes. For the former cause, possible solutions include examining successful examples in this or other industries and applying them as part of an overall safety program. For example, Leveson states that SUBSAFE, which is the safety program created for preventing mishaps in nuclear Naval systems, is one of the successful examples. The applicability and detail were not examined in this thesis, but something like this may provide a good opportunity to start thinking about how to design a safe culture.

6.3.2 Database for the Results of Accidents Analyses

Leveson proposes that one responsibility for management includes:

“Establish safety education and training for all employees… The education should include reminders of past accidents and causes and input from lessons learned and trouble reports.” (Adapted from Leveson [6, p. 437])

The management at JR West after the deadliest Fukuchiyama derailment in 2005 in Japan explained that one of the problems that contributed to the accident was inadequate research of past accidents in other industries, as they only had focused only on researching the past accidents within the company and the other JR companies [75].

Many accident analyses are carried out in aerospace industries, and lessons learned can be relatively easily obtained for those systems. However, less work seems to be carried out in the rail sector. As JR West argues, the lessons learned should not be limited to their corporation, rather, we should examine the past accidents more broadly.

Thus, the list of the hazards, causes, and scenarios leading to the loss events should be beneficial for future system and organization designs. The list should include, for example, the overview of the accident and the recommendations such as the ones proposed in this thesis. The recommendations in this thesis can be a part of the list, but more lessons from other accident analysis should be added for that list.

(This page intentionally left blank)

Appendix A Supplement Information for WMATA CAST Analysis

A.1 Time Line of Incident, Enactment of Procedures, and Actions Involving Truck Circuits

Table A-1 shows the time line of the incident, enactment of procedures, and Actions involving the truck circuits. For actions, the Unsafe Control Actions are colored blue, and Mental Model Flaws are colored green.

They noticed that Loss-of-shunt should be detected properly during the maintenance activities and set the three-point-shunt test procedure. However, because of the ineffective circulation of the information, it was not well understood and properly implemented by the on-site ATC maintenance workers.

Also, software tool (loss-of-shunt software) was developed after the Rosslyn accident, but it was not used regularly. The management level controller (the communications superintendent for WMATA) believed that the maintenance workers were using the tool regularly because some of the on-site managers lied that those tools were used.

The track circuit B2-304, which caused the Loss in this accident, was not the only product which malfunctioned. The truck circuit C2-111 and B1-245 are the examples of malfunctioned track circuit due to parasitic oscillation. The B1-245 was believed to be repaired successfully but it was constantly not detecting trains. This is probably because (1) They never thought parasitic oscillation was a cause of the defect, and (2) They did not follow the procedure properly because they just didn’t want to follow a procedure or they actually did not notice the updated procedures.

Table A- 1 Time line of Incident, enactment of procedures, and actions involving truck circuits

Timeline (m/d/y)	**Incident, Manuals, Bulletin, Notices, and actions involving truck circuits**	
2/24/1982	PMI 11000 (Instructions)	・A written instructions for employees responsible for maintaining, testing, and inspecting components of the Metrorail ATC system. ・Requiring shut test in the transmitter end (1 position) ・The ATC engineers were using check list form PM-1, when performing verification under the PMI 11000. This form did only indicate the column for transmitter and/or receiver end, not for the middle of the track. ・Not specifically mentioned in the report, but it seems that this instruction was written as if the equipment were all GRS components. This might have made ATC mechanics and their supervisors think there are no official instructions in performing maintenance for the different manufactures' components.
3/25/2003	ATC System Integrity Maintenance Practices (Manuals)	・Requiring shunt test should be done in the transmitter end (1 position) ・Not specifically mentioned in the report, but it seems that this instructions were written as if the equipment were all GRS components. This might have made ATC mechanics and their supervisors think there are no official instructions in performing maintenance for the different manufactures' components.

6/7/2005	Rosslyn near-collision incident	・Track circuit C2-111 had been not detecting trains occupying it. ・ATC engineers reviewed the historical data and determined C2-111 did not detect the presence of a train in the middle of the circuit. ・The investigation revealed that false track circuit could pass a shunt test when it was placed at either end of the circuit, but did not detect the shunt when it was placed in the middle of the circuit ・They thought an electrical fault between the transmitter and receiver bond cables was the probable cause. However, **they never could figure out a definitive cause at this time.** They did not think parasitic oscillation was involved. ・WMATA developed the loss-of-shunt (software) tool as a result of this incident and following investigation. ・ATC engineers used a loss-of-shunt-tool on a weekly basis at first. However, about a year, they were not required to do it on a weekly basis anymore. Instead, they were recommended to be used once a month. ・ After the Fort Totten accident, **the communications superintendent** for WMATA stated that there was no record available which states that the loss-of-shunt tool was used monthly. On the contrary to this fact, he was informed by some ATC managers that the tool was used weekly. From a set of information like this, he incorrectly believed that the tool was used monthly basis. ・Also after the Fort Totten accident, the Rosslyn modules of C2-111 were tested and found to have parasitic oscillation between the transmitter module and the receiver module similar to that found at Fort Totten. ・Also after the Fort Totten accident, the historical data showed

		that from at least October 1988, C2-111 intermittently lost train detection and indicated "vacant" when trains were occupying the circuit. As C2-111 was always equipped with GRS impedance bonds and GRS track circuit modules, it is likely that the incompatibility is not likely the direct cause of the parasitic oscillation and false signals.
6/19/2005	Engineering bulleting and ATC safety notice	Transmitter end & in the middle of the track circuit (2 positions) ・Issued after Rosslyn incident. ・Shunt placement in the middle was added, based on the finding from the Rosslyn incident's investigation ・This represented a change from the existing procedures (PMI 11000)
10/6/2006	WMTA Metrorail engineering bulletin	・After the installation of a US&S impedance bond in a GRS ATP track circuit, shunt test should be performed at 3 positions (at each end & in the middle) ・If a track circuit does not pass a three-shunt verification process, the original impedance bond should be reinstalled. ・Intended to address concerns raised by some ATC technicians regarding the use of US&S bonds with GRS modules.
12/12/2007	Actions with B2-304	・Power level was raised from 55 to 70 % for B2-312 which shared the impedance bond with B2-304
12/18/2007	Actions with B1-245	・Installing the US&S's new receiver impedance bond for B1-245. ・The transmitter power level was increased ・The track circuit was reportedly adjusted and verified ・According to the recorded data, **the track circuit repeatedly lost detection** after the bond replacement.

12/24/2007		・A work order was opened for B1-245 as it was revealed that the circuit did not shunt a train ・The track circuit was reportedly adjusted and verified. ・According to the recorded data, **the track circuit repeatedly lost detection** after the adjustment
1/10/2008		・B1-245 was still not consistently detecting trains. ・ transmitter power level was changed but could not be adjusted correctly ・ATC technicians **removed track circuit B1-245 and notified the OCC and the MOC.**
1/11/2008		・B1-245's power level was changed again but **could not be adjusted correctly**
1/12/2008		・Removed the US&S's new receiver bond for B1-245 and reinstalled the original GRS's bond ・The track circuit was adjusted and verified. ・T**rack circuit continued to lose train detection after the reinstallation**
9/9/2008	Actions with B1-245	・ATC engineers reviewed the historical data of B1-245 and concluded that the GRS's transmitter bond was defective. ・They replaced the bond with another GRS bond. They adjusted and verified. **・ A review of historical data shows the track circuit continued not detecting trains.**
10/29/2008	T181 (yet to be approved when accident occurred)	・A written procedures for adjusting track circuits equipped with either GRS or US&S modules. ・After the adjustments, the track circuits were to be verified using the procedures written in PMI T111.

11/23/2008	PMI T111 (yet to be approved when accident occurred)	・Requiring shunt test at Transmitter end, Receiver end, & in the middle of the track (3 positions)
1/10/2009	Actions with B1-245	・The US&S's receiver bond was again installed into B1-245. The circuit was adjusted and verified. **・The historical data shows B1-245 continued not detecting trains.**
4/20/2009		・The US&S's transmitter bond was again installed into B1-245. The circuit was adjusted and verified. **・The historical data shows B1-245 continued not detecting trains.**
8/14/2009	Actions with B1-245	・The B1-245's GRS track circuit modules was replaced with US&S modules. ・The historical data shows **no further "not-detecting" events for B1-245**

A.2 Actions Involving B2-304 Prior to the Accident

The actions involving B2-304 prior to the accident are summarized chronologically in following Table A-2. The Unsafe Control Actions are colored blue, and Mental Model Flaws are colored green.

Table A- 2 Actions Involving B2-304 Prior to the Accident

Time Line	Actions involving B2-304	
	ATC mechanics	**Other Controllers**
6/16,17/2009	***Installation Team*** ・Installing the US&S's new transmitter impedance bond ・Increased transmitter power from 30 to 55% so as to solve bobbing problems. (Bobbing refers to the case where the train detection is transitioning from (1) vacant (2) and then to occupied, (3) and finally back to vacant again without any trains present.) ・Did 3 position verification and believed the track circuit functioned properly (according to her testimony) ・The post-accident testing revealed that **the B2-304 did not detect the trains' wheels** when placed at (1) middle of the circuit and (2) receiver end. These results are contrary to the testimony of the CIT crew leader. ・ The investigators **could not verify her statements to have performed 3-place-test** as the historical data was not reliable because of	***MOC (Part of OCC)*** ・ Acknowledged the report from the Installation team about bobbing of the track circuit. ・Opened the work order No. 7169867 for bobbing track circuit B2-304. ・ Did not issue the incident ticket which is generated for high-priority works ・(Although not directly related to this accident,) did not open the work order for B2-312 ***ATC shift supervisors & TSSM managers*** ・Because work order No.

	the frequent bobbing ・Based on the investigation, they seem to have not properly performed 3-position-shunt-test. ・She talked with her supervisor about the bobbing problems which she encountered during the adjustments, and was instructed to observe two train movements before departing. ・B2-304 and adjacent B2-312 began bobbing again when waiting for the trains and she did some minor actions to solve the problem which did not work ・Although two track circuits were still bobbing, the crew observed two trains were detected properly by the truck circuits. ・She called MOC and reported that the trains were observed properly but the two track circuits were still bobbing.	7169867 was not associated with an incident ticket, it was never included in any list that TSSM managers reviewed.
6/18/2009	***Preventative Maintenance Team*** ・Performed routine, scheduled preventative maintenance for B2-304 ・Conducted verification tests on B2-304 ・Used PMI 11000, and performed shunt test on only 1 position ・They verified that B2-304 performed properly because the track circuit detected the shunt ・They believed that B2-304 was not in unsafe condition. ・They found the bobbing but thought it was ok because the measurements and historical data	

	were consistent and seemed to be in safe condition ・They did not report the bobbing to the MOC because the problem cleared itself during trouble shooting. ・Did not aware of the bulletin and notices which require shunt test to be performed in more than 2 positions ・Not aware of the open work order No. 7169867	

A.3 Causal Loop Diagrams for the Conceptual Idea of the Migration to the High-Risk State

In the section 3.10, the dynamics and the migration to the high-risk state of the WMATA Metrorail system was explained. In this section, the concepts of (1) Degradation of safety culture, (2) Degradation of Infrastructure, (3) Degradation of Safety, and (4) the multiplier effect of three loops are presented in the form of Causal Loop Diagram, which is one of the System Dynamics modeling technique [76] which is represented by the concepts such as Delays, or Stocks and Flows.

The goal here in this thesis to use System Dynamics method is not making mathematically correct model, but to capture the big picture of the system's dynamical functions. Usually, it is beneficial to have the consistent units and dimensional consistency even when the model is purely conceptual like in this case. However, the model explained in this thesis would not necessarily follow this basic because some of the variables were difficult to be given quantitative concepts and having been failed to do so seemed not so harmful for understanding the System's Structure and Dynamics.

Besides, note that the conceptual ideas represented following were formulated through the CAST-based analysis, and the System Dynamics models were purely used for stimulating the understanding of what this thesis had in mind in the explanations provided in the section 3.9. In addition, note that these concepts are very subjective and possibly other persons would have different ideas of variables, relationships between variables, delays, stock and flows, etc.

A.3.1 Degradation of Safety Culture

The conceptual representation with Causal Loop Diagram with Delays and Stock & Flow is depicted in the following figure A-1. See the section 3.10.1 for the explanation of the idea of the degradation of safety culture. The structure explained here can be summarized as the reinforcing feedback structure labeled as "R1: Degradation of Safety Culture".

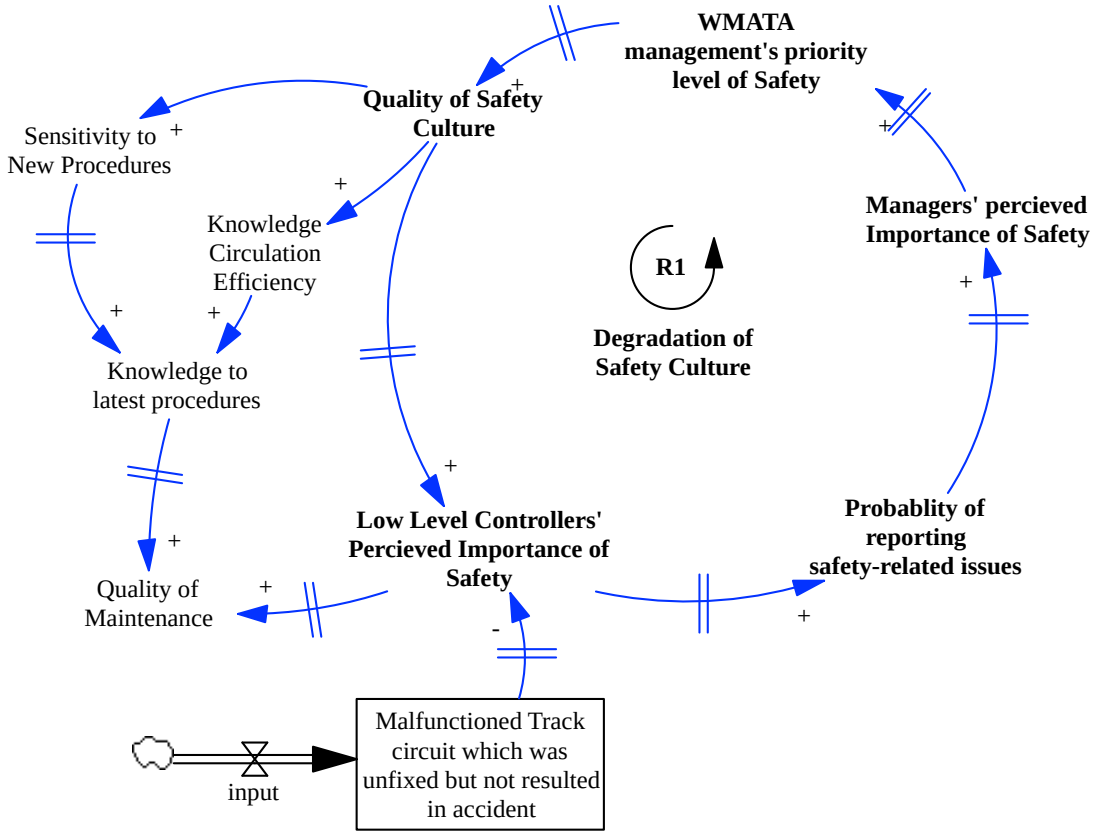


Figure A- 1 Conceptual Representation of Degradation of Safety Culture in WMATA.

A.3.2 Degradation of Infrastructure

The conceptual modeling for this mechanism is provided in the following figure A-2. See the section 3.10.2 for the explanation of the idea of the degradation of Infrastructure. The structure explained here can be summarized as the reinforcing feedback structure labeled as “R2: Degradation of Infrastructure”.

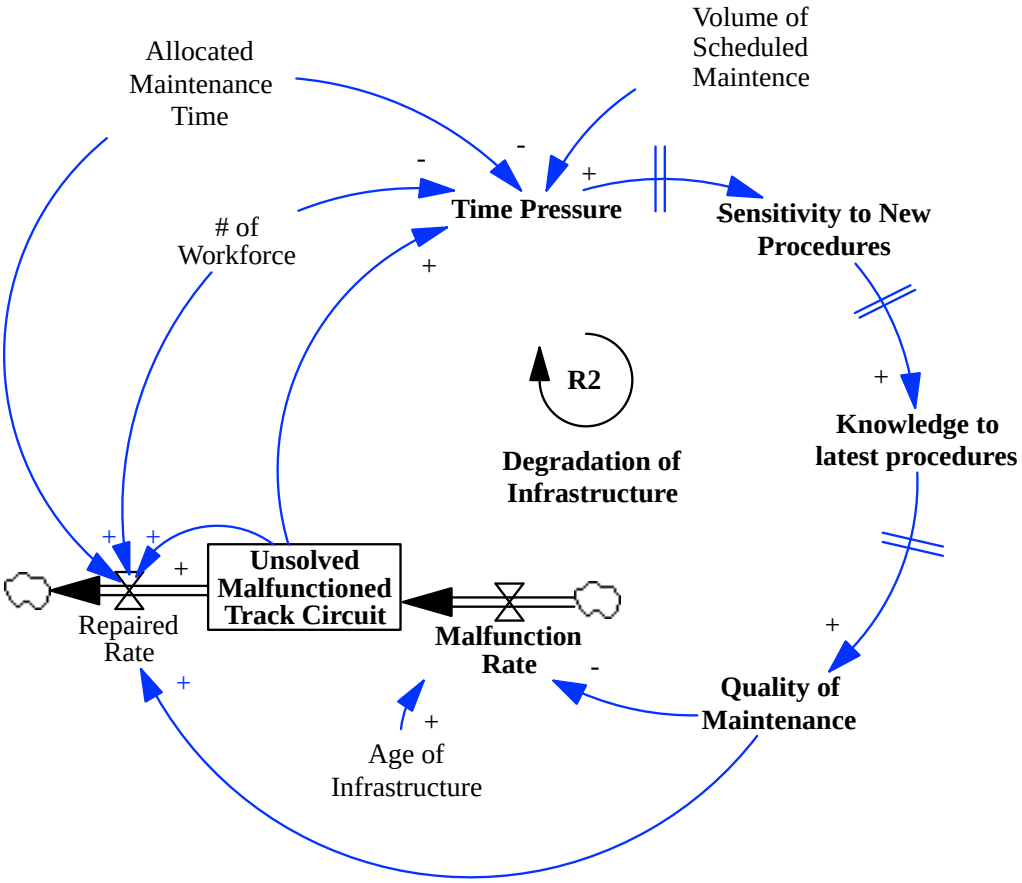


Figure A- 2 Conceptual Representation of Degradation of Infrastructure in WMATA.

A.3.3 Degradation of Safety

The conceptual Causal Loop Diagram with Delays and Stock & Flow is depicted in the following figure A-3. See the section 3.10.3 for the explanation of the idea of the degradation of safety. The structure explained here can be summarized as the reinforcing feedback structure labeled as “R3: Degradation of Safety”.

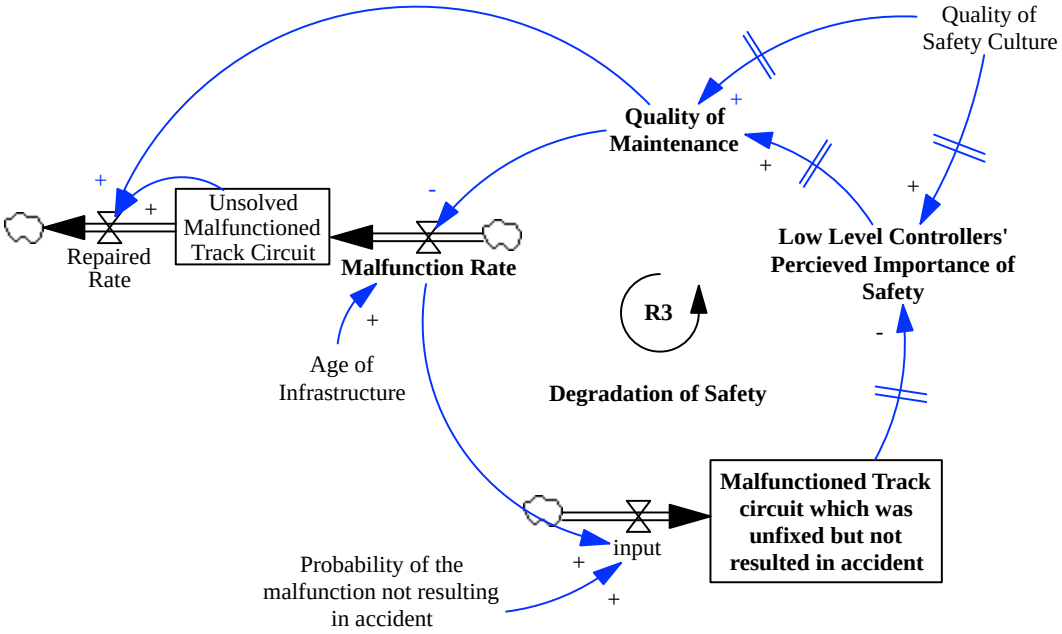


Figure A- 3 Conceptual Representation of Degradation of Safety in WMATA.

A.3.4 Combining the Loops together: Multiplier Effects

Abovementioned three reinforcing structures are combined and represented in the following figure A-4. These three reinforcing loops were mutually connected and had multiplier effect. See the section 3.10.4 for the explanation of this idea.

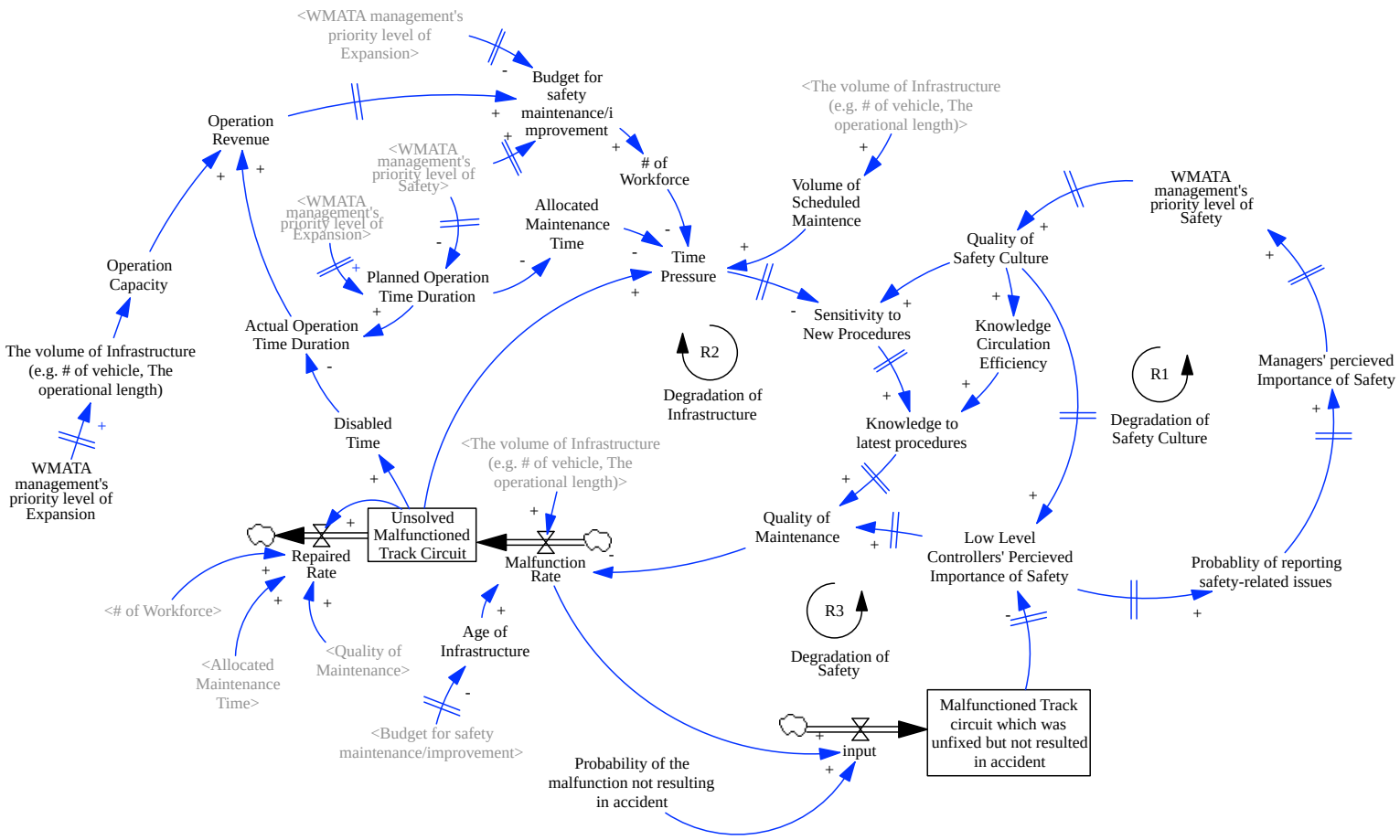


Figure A- 4 Conceptual Representation of Migration to a High-Risk State in WMATA.

Appendix B Supplement Information for Amtrak CAST Analysis

B.1 Safety Culture of Amtrak [56], [77], [78]

The weak safety culture within Amtrak management was likely behind this accident. The lack of safety culture was articulated in the other accident's report. That accident happened on Apr 2016 at NEC. In this accident, southbound Amtrak train 89 struck a backhoe with a worker inside, resulting in 2 workers killed and 39 others were injured, property damages were estimated to be $2.5 million.

In this 2016 accident, no work zone protection was added which did not make ATC system ensure that the train would automatically slow down.

NTSB concluded the problems were (not all are listed here):

1. Systematic problem with Amtrak's safety culture
2. No viable reporting system in place to collect safety critical information
3. Disengagement by a supervisor encouraged lax safety habits
4. 29 active failures and latent conditions
5. Safety was consistently a low priority in the decision-making process of the employees involved
6. Amtrak management did not proactively identify and mitigate unsafe conditions
7. Amtrak's rules and supervisor expectations did not adequately emphasize safety
8. Labor-management relationship was so adversarial that safety programs became contentious at the bargaining table, with the unions finally refusing to participate
9. Lack of consistent knowledge and vision for safety across Amtrak's management which created a culture that facilitated and enabled unsafe work practices by employees
10. No effective safety management system program
11. FRA's lack of safety oversight to require signal protection

From these findings, one can conclude that the accident in 2016 was just a symptom of a lax safety culture within Amtrak (and even in FRA and government).

As safety (culture) is a systematic characteristic (property), one can maintain that

the derailment in 2015 was also the symptom of lax safety culture within Amtrak and its safety oversight authorities. The ATC system was left to be allowing single point failures, likely because the front-line employees did not report those problems to the upper-level management or they were reported the problem but they decided not to mitigate likely because they prioritized saving cost.

B.2 "Lax" Design Requirements for PTC

The PTC system which Amtrak would implement still does not eliminate the train-to-train collision hazard, that is, the PTC would automatically stop trains only ahead of the interlockings, and it is incapable of doing so ahead of the "intermediate signals" (See Figure B-1).

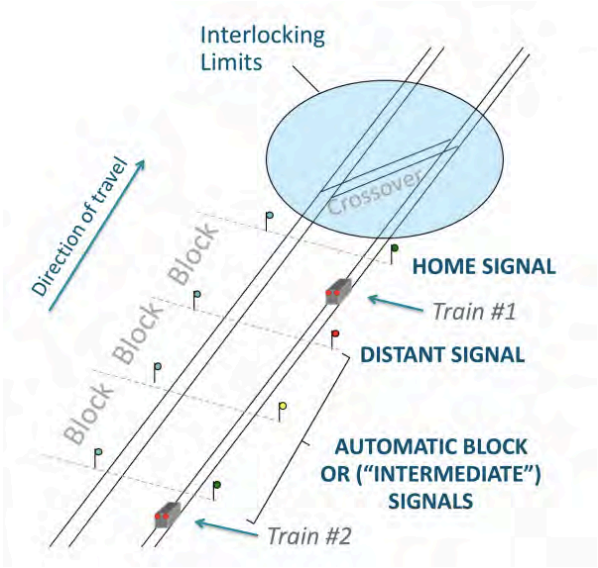


Figure B- 1 PTC stop the train only ahead of the interlockings.

(Adapted from Amtrak [45])

This means that if the train operator does not appropriately activate brake ahead of the red signal, the consequence is the train-to-train collision. One might argue that the train speed would be reduced into 20mph, but there seems to be no hazard analysis about why it is not unsafe. (The author could not find the documentation about to what speed the train would be

automatically decelerated, thus concluded that it would be around 20 mph which is inferred from current ATC's cab signal indication (see "Restricting" in Table 4-2).

There was no documentation why Amtrak management and governmental organizations concluded that this would meet the PTC requirement of "avoiding train-to-train collision," but it could be argued that all of them lack the policy of "eliminating single point failures."

This thesis argues that PTC should be the system which eliminates the single point failures, thus Amtrak and FRA's safety policies are problematic.

References

[1] D. Wakabayashi, “Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam,” *The New York Times*, 30-Jul-2018. [Online]. Available: https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html. [Accessed: 06-Mar-2019].

[2] NTSB, “PRELIMINARY REPORT HIGHWAY (HWY18MH010),” 24-May-2018. [Online]. Available: https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf. [Accessed: 06-Mar-2019].

[3] Alan Levin, “Lion Air Crash Demonstrates Unintended Consequences of Cockpit Automation,” *Insurance Journal*, 30-Nov-2018. [Online]. Available: https://www.insurancejournal.com/news/international/2018/11/30/510682.htm. [Accessed: 02-Mar-2019].

[4] Nick Ismail, “AI: the new driving force in the automotive industry,” *Information Age*, 15-Sep-2017. [Online]. Available: https://www.information-age.com/ai-new-driving-force-automotive-industry-123468560/. [Accessed: 06-Mar-2019].

[5] “Automated Vehicles for Safety,” *NHTSA*, 07-Sep-2017. [Online]. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety. [Accessed: 06-Mar-2019].

[6] N. G. Leveson, *Engineering a Safer World - Systems Thinking Applied to Safety*. MIT Press, 2011.

[7] R. Parasuraman, T.B. Sheridan, and C.D. Wickens, “A model for types and levels of human interaction with automation,” in *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 2000, pp. 286–297.

[8] “Excessive speed named as cause of deadly Taiwan train derailment,” *The Japan Times Online*, Oct-2018. [Online]. Available: https://www.japantimes.co.jp/news/2018/10/23/asia-pacific/excessive-speed-named-cause-deadly-taiwan-train-derailment/. [Accessed: 02-Mar-2019].

[9] Y. Tanaka, “Taiwan derailments 25 times in last 2 years,” *The Sankei News*, 24-Oct-2018. [Online]. Available: https://www.sankei.com/world/news/181024/wor1810240030-n1.html. [Accessed: 31-Jan-2019].

[10] “Analyzing the root causes of Spain’s high-speed derailment,” *Railtechnologymagazin.com*, 29-Feb-2016. [Online]. Available: http://www.railtechnologymagazine.com/Comment/analysing-the-root-causes-of-spains-high-speed-derailment. [Accessed: 02-Mar-2019].

[11] Aircraft and Railway Accidents Investigation Commission, “RA2007-3-1 Railway Accident Report - JR West Fukuchiyama Line Derailment (Japanese),” 28-Jun-2007. [Online]. Available: http://www.mlit.go.jp/jtsb/railway/fukuchiyama/RA07-3-1-1.pdf. [Accessed: 02-Mar-2019].

[12] “Memorial service held for 107 victims of 2005 fatal train derailment in Hyogo,” *Japan Today*, 25-Apr-2018. [Online]. Available: https://japantoday.com/category/national/memorial-service-held-for-107-victims-of-2005-fatal-train-derailment-in-hyogo. [Accessed: 02-Mar-2019].

[13] NTSB, “NTSB/PAR-10/02 NTSB Railroad Accident Report - Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station Washington, D.C. -,” 27-Jul-2010. [Online]. Available: https://www.ntsb.gov/investigations/accidentreports/reports/rar1002.pdf. [Accessed: 25-Jan-2019].

[14] International Union of Railways (UIC)), “High Speed Rail Brochure - 2018,” 11-Jun-2018. [Online]. Available: https://uic.org/IMG/pdf/uic_high_speed_2018_ph08_web.pdf. [Accessed: 03-Mar-2019].

[15] Central Japan Railway Company, “Annual Report 2018,” 2018. [Online]. Available: https://global.jr-central.co.jp/en/company/ir/annualreport/index.html. [Accessed: 03-Mar-2019].

[16] N. G. Leveson, “Lecture Notes | System Safety | Aeronautics and Astronautics | MIT OpenCourseWare.” [Online]. Available: https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-863j-system-safety-spring-2016/lecture-notes/. [Accessed: 22-Feb-2019].

[17] N. G. Leveson and J. P. Thomas, “STPA Handbook,” Mar. 2018.

[18] N. G. Leveson, “Engineering a Safer and More Secure World.”

[19] N. G. Leveson, presented at the MIT Lecture 16.863 System Safety Concept, Boston, MA, 2016.

[20] S. Kawakami, “Application of a systems-theoretic approach to risk analysis of

high-speed rail project management in the US," Thesis, Massachusetts Institute of Technology, 2014.

[21] US congress, "Congresses' consent legislation," 06-Nov-1966. [Online]. Available: http://uscode.house.gov/statutes/pl/89/774.pdf. [Accessed: 11-Mar-2019].

[22] WMATA, "Bylaws," 2018. [Online]. Available: https://www.wmata.com/about/board/upload/WMATA-Board-Bylaws-Adopted-6-28-2018.pdf. [Accessed: 25-Jan-2019].

[23] WMATA, "Compact," Aug-2009. [Online]. Available: https://www.wmata.com/about/board/upload/Compact_Annotated_2009_final.pdf. [Accessed: 25-Jan-2019].

[24] WMATA, "Metro Snapshot," 2019. [Online]. Available: https://www.wmata.com/about/upload/Metro-Snapshot-April-2018.pdf. [Accessed: 11-Mar-2019].

[25] B. O'Connor, "Loss of Detection: D.C. Metro Railway Collision," Aug-2011. [Online]. Available: https://sma.nasa.gov/docs/default-source/safety-messages/safetymessage-2011-08-01-dcmetrorailwaycollision-vits.pdf?sfvrsn=57ae1ef8_4. [Accessed: 11-Mar-2019].

[26] D. C. VOCK, "Fixing WMATA, the Nation's Second Busiest Transit System, From Every Direction," *Governing*, Nov-2016. [Online]. Available: http://www.governing.com/topics/transportation-infrastructure/gov-wmata-transit-problems.html.

[27] N. Fandos, "House Members Refuse Washington Subway System's Plea for More Funds," *NewYorkTimes*, 13-Apr-2016. [Online]. Available: https://www.nytimes.com/2016/04/14/us/house-members-refuse-washington-subway-systems-plea-for-more-funds.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer. [Accessed: 11-Mar-2019].

[28] C. Horton, "Train's Driver Disabled Speed Controls Before Taiwan Crash, Officials Say," *The New York Times*, 23-Oct-2018. [Online]. Available: https://www.nytimes.com/2018/10/23/world/asia/taiwan-train-crash-conductor-investigated.html. [Accessed: 31-Jan-2019].

[29] E. Mundahl, "As D.C.'s Metro Bleeds Cash, Are Other Transportation Options Performing Better?," *InsideSources*, 27-Feb-2017. [Online]. Available:

https://www.insidesources.com/more-profitable-than-wmata/. [Accessed: 02-Feb-2019].

[30] J. D. Sterman, “Sustaining Sustainability: Creating a Systems Science in a Fragmented Academy and Polarized World,” in *Sustainability Science: The Emerging Paradigm and the Urban Environment*, M. P. Weinstein and R. E. Turner, Eds. New York, NY: Springer New York, 2012, pp. 21–58.

[31] WMATA, “SafeTrack | WMATA,” *WMATA Homepage*. [Online]. Available: https://www.wmata.com/service/SafeTrack.cfm. [Accessed: 02-Feb-2019].

[32] F. Siddiqui, “When it comes to reversing the ridership slide, Metro’s leaders don’t have a plan,” *Washington Post*, 30-Sep-2018. [Online]. Available: https://www.washingtonpost.com/local/trafficandcommuting/when-it-comes-to-reversing-the-ridership-slide-metros-leaders-dont-have-a-plan/2018/09/30/bf299e7c-bcf5-11e8-b7d2-0773aa1e33da_story.html. [Accessed: 02-Feb-2019].

[33] N. G. Leveson, M. Stringfellow, and J. Thomas, “STAMP-Based Analysis of SBS Tank 731 Overflow Accident.”

[34] NTSB, “Derailment of Amtrak Passenger Train 188 Philadelphia, Pennsylvania May 12, 2015,” 17-May-2016. .

[35] Amtrak, “Amtrak (ATK) PTC Implementation Plan (PTCIP) Revision 4.0,” 18-Nov-2016. [Online]. Available: https://www.regulations.gov/document?D=FRA-2010-0029-0076. [Accessed: 10-Feb-2019].

[36] Amtrak, “Amtrak Company Profile - Fiscal Year 2017,” 2018. [Online]. Available: https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/nationalfactsheets/Amtrak-Company-Profile-FY2017-0318.pdf.

[37] Amtrak, “Amtrak-Audited-Consolidated-Financial-Statements-FY2018.pdf,” 2018. [Online]. Available: https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/financial/Amtrak-Audited-Consolidated-Financial-Statements-FY2018.pdf. [Accessed: 12-Feb-2019].

[38] Ernst & Young LLP, “Report of Independent Auditors,” Jan. 2019.

[39] Harvard Law Review, “Department of Transportation v. Association of American Railroads,” 10-Nov-2015. [Online]. Available: https://harvardlawreview.org/2015/11/department-of-transportation-v-association-

of-american-railroads/. [Accessed: 10-Feb-2019].

[40] RUSSELL G. QUIMBY, “Reliable Amtrak service can turn deadly — when underfunded | TheHill,” *The Hill*, 02-Sep-2018. [Online]. Available: https://thehill.com/opinion/finance/373166-reliable-amtrak-service-can-turn-deadly-when-underfunded. [Accessed: 18-Feb-2019].

[41] Amtrak, “General and Legislative Annual Report & Fiscal Year 2019 Grant Request,” 15-Feb-2018. [Online]. Available: https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/reports/Amtrak-General-Legislative-Annual-Report-FY2019-Grant-Request.pdf. [Accessed: 11-Mar-2019].

[42] Amtrak, “Amtrak Reports & Documents.” [Online]. Available: https://www.amtrak.com/reports-documents. [Accessed: 12-Feb-2019].

[43] Amtrak, “Amtrak Sets Revenue and Earnings Records Delivers Best Operating Performance in Company History,” *Amtrak Media*, 16-Nov-2018. [Online]. Available: https://media.amtrak.com/2018/11/amtrak-sets-revenue-and-earnings-records-delivers-best-operating-performance-in-company-history/. [Accessed: 12-Feb-2019].

[44] Amtrak, “How It Works: Railroad Signals in the Northeast Corridor,” *Amtrak*, 19-May-2015. [Online]. Available: http://blog.amtrak.com/2015/05/works-railroad-signals-northeast-corridor/. [Accessed: 07-Feb-2019].

[45] Amtrak, “Positive Train Control (PTC),” *Amtrak Media*. [Online]. Available: https://media.amtrak.com/positive-train-control/. [Accessed: 13-Feb-2019].

[46] NTSB, “(Special Investigation Report) End-of-Track Collisions at Terminal Stations Hoboken, New Jersey, September 29, 2016 and Atlantic Terminal, Brooklyn, New York, January 4, 2017,” 06-Feb-2018. .

[47] D. Z. Morris, “The century-old tech that ensures train safety,” *Fortune*, 24-Jul-2015. [Online]. Available: http://fortune.com/2015/07/24/automatic-train-control/. [Accessed: 13-Feb-2019].

[48] Congressional Research Service, “Positive Train Control (PTC): Overview and Policy Issues,” Sep. 2018.

[49] Amtrak Office of Inspector General, “RAILROAD SAFETY: Amtrak Has Made Progress in Implementing Positive Train Control, but Significant Challenges Remain,” 20-Dec-2012. [Online]. Available:

https://www.amtrakoig.gov/sites/default/files/reports/amtrak_oig-e-2013-003.pdf. [Accessed: 12-Feb-2019].

[50] NTSB, “NATIONAL TRANSPORTATION SAFETY BOARD FY 2018–2022 STRATEGIC PLAN,” Dec-2017. [Online]. Available: https://www.ntsb.gov/about/reports/Documents/FY2018-2022strategicPlan.pdf. [Accessed: 17-Feb-2019].

[51] Holly Yan, Madison Park, Jon Ostrower, and Steve Almasy, “Amtrak derailment: Two victims identified as rail advocates - CNN,” *CNN*, 20-Dec-2017. [Online]. Available: https://edition.cnn.com/2017/12/19/us/amtrak-derailment-washington/index.html. [Accessed: 16-Feb-2019].

[52] D. Z. Morris, “Why Didn’t a Planned Safety System Stop Sunday’s Amtrak Crash? | Fortune,” *Fortune*, 04-Feb-2018. [Online]. Available: http://fortune.com/2018/02/04/amtrak-safety-congress-funding/. [Accessed: 16-Feb-2019].

[53] D. Z. Morris, “How lack of wireless spectrum delayed implementation of Amtrak’s PTC system,” *Fortune*, 25-May-2015. [Online]. Available: http://fortune.com/2015/05/25/amtrak-ptc/. [Accessed: 16-Feb-2019].

[54] K. Johnson, R. Pérez-Peña, and N. Chokshi, “Multiple Deaths in Amtrak Train Derailment in Washington,” *The New York Times*, 20-Jan-2018. [Online]. Available: https://www.nytimes.com/2017/12/18/us/amtrak-derailment-washington.html. [Accessed: 09-Feb-2019].

[55] NTSB, “Collision of Metrolink Train 111 With Union Pacific Train LOF65-12 Chatsworth, California September 12, 2008,” 21-Jan-2010. [Online]. Available: https://www.ntsb.gov/investigations/AccidentReports/Reports/RAR1001.pdf. [Accessed: 15-Feb-2019].

[56] NTSB, “Amtrak Train Collision with Maintenance-of-Way Equipment, Chester, Pennsylvania, April 3, 2016,” 14-Nov-2017. [Online]. Available: https://www.ntsb.gov/investigations/AccidentReports/Reports/RAR1702.pdf.

[57] Jens Rasmussen, “Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models,” presented at the IEEE Transactions on Systems, Man, and Cybernetics, 1983, vol. smc-13, No.3, pp. 257–266.

[58] Nippon Export and Investment Insurance, “e-NEXI March 2011,” *NEXI Web*

Magazine, Mar-2011. [Online]. Available: https://www.nexi.go.jp/webmagazine/mt_file/e-nexi_2011_03.pdf. [Accessed: 24-Feb-2019].

[59] "Ranking for total track length of railroad around the world." [Online]. Available: http://top10.sakura.ne.jp/IBRD-IS-RRS-TOTL-KM.html#map. [Accessed: 23-Feb-2019].

[60] Amtrak, "Amtrak-Monthly-Performance-Report-September-2017-Preliminary-Unaudited.pdf," 27-Dec-2017. [Online]. Available: https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/monthlyperformancereports/2017/Amtrak-Monthly-Performance-Report-September-2017-Preliminary-Unaudited.pdf. [Accessed: 17-Feb-2019].

[61] Amtrak, "Amtrak-Audited-Consolidated-Financial-Statements-FY2017.pdf," 2017. [Online]. Available: https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/financial/Amtrak-Audited-Consolidated-Financial-Statements-FY2017.pdf. [Accessed: 20-Feb-2019].

[62] E. G. Fitzsimmons, "Amtrak at a Junction: Invest in Improvements, or Risk Worsening Problems," *The New York Times*, 22-Dec-2017. [Online]. Available: https://www.nytimes.com/2017/04/24/nyregion/amtrak-infrastructure-crisis.html. [Accessed: 20-Feb-2019].

[63] MLIT Japan (Ministry of Land, Infrastructure, Transport and Tourism), "Information about rail transportation's safety," Jul-2018. [Online]. Available: http://www.mlit.go.jp/common/001246059.pdf. [Accessed: 19-Feb-2019].

[64] "Dollar (USD) to Japanese yen (JPY) Currency Converter," *currency-calc.com*. [Online]. Available: https://www.currency-calc.com/USD_JPY. [Accessed: 20-Feb-2019].

[65] "Travel mode shares in the U.S.," *The Transport Politic*, 24-Aug-2016. [Online]. Available: https://www.thetransportpolitic.com/databook/travel-mode-shares-in-the-u-s/. [Accessed: 25-Feb-2019].

[66] MLIT Japan (Ministry of Land, Infrastructure, Transport and Tourism), "Transportation-related statistics (Koutsu kanren toukei shiryoushyu)." [Online]. Available: http://www.mlit.go.jp/statistics/kotsusiryo.html. [Accessed: 25-Feb-2019].

[67] D. Leonhardt, “Amtrak Crash and America’s Declining Construction Spending,” *The New York Times*, 21-Dec-2017. [Online]. Available: https://www.nytimes.com/2015/05/14/upshot/amtrak-crash-and-americas-declining-construction-spending.html. [Accessed: 25-Feb-2019].

[68] KIRSTEN KOROSEC, “Amtrak Funding Slashed In Half Under Trump Spending Plan,” *Fortune*, 13-Feb-2018. [Online]. Available: http://fortune.com/2018/02/12/amtrak-funding-cut-trump-spending-plan/. [Accessed: 25-Feb-2019].

[69] Bart Jansen, “Amtrak gets nearly $2 billion in federal spending bill, despite Trump criticism and accidents,” *USA TODAY*, 22-Mar-2018. [Online]. Available: https://www.usatoday.com/story/news/2018/03/21/amtrak-gets-nearly-2-billion-federal-spending/447301002/. [Accessed: 25-Feb-2019].

[70] R. Neate and J. Walters, “Congress votes to cut Amtrak’s funding hours after fatal train crash,” *The Guardian*, 13-May-2015. [Online]. Available: https://www.theguardian.com/world/2015/may/13/amtrak-funding-cuts-congress-train-crash. [Accessed: 25-Feb-2019].

[71] USDOT, “Age and Availability of Amtrak Locomotive and Car Fleets | Bureau of Transportation Statistics.” [Online]. Available: https://www.bts.gov/content/age-and-availability-amtrak-locomotive-and-car-fleets. [Accessed: 25-Feb-2019].

[72] S. D. Ota, “Assuring safety in high-speed magnetically levitated (maglev) systems : the need for a system safety approach,” Thesis, Massachusetts Institute of Technology, 2008.

[73] JR West, “Overview of Accident — JR-West.” [Online]. Available: https://www.westjr.co.jp/global/en/fukuchiyama/outline/. [Accessed: 16-Mar-2019].

[74] “Should be Remembered- Thirteen years past since Fukuchiyama Derailment (in Japanese),” *The Sankei News*, 25-Apr-2018. [Online]. Available: https://www.sankei.com/affairs/news/180425/afr1804250007-n1.html. [Accessed: 16-Mar-2019].

[75] JR West, “Review of the present condition about safety (in Japanese).” [Online]. Available: https://www.westjr.co.jp/safety/fukuchiyama/plan_improvement/pdf/keikaku_01.pdf.

[76] John D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a*

Complex World. McGraw-Hill, Inc., 2000.

[77] NTSB, “Ignored Safety Procedures, Fractured Safety Program Led to Fatal Amtrak Derailment,” 14-Nov-2017. [Online]. Available: https://www.ntsb.gov/news/press-releases/Pages/pr20171114.aspx. [Accessed: 16-Feb-2019].

[78] NTSB, “NATIONAL TRANSPORTATION SAFETY BOARD Public Meeting of November 14, 2017,” 2017. [Online]. Available: https://www-ntsb-gov.libproxy.mit.edu/news/events/Documents/2017-DCA16FR007-BMG-abstract.pdf.